Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

17.028

Botschaft zum Informationssicherheitsgesetz

vom 22. Februar 2017

Sehr geehrter Herr Nationalratspräsident
Sehr geehrter Herr Ständeratspräsident
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf eines Informationssicherheitsgesetzes.

Wir versichern Sie, sehr geehrter Herr Nationalratspräsident, sehr geehrter Herr Ständeratspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

22. Februar 2017

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Doris Leuthard
Der Bundeskanzler: Walter Thurnherr

Übersicht

Diese Vorlage schafft – basierend auf international anerkannten Standards – einen einheitlichen formell-gesetzlichen Rahmen für die Informationssicherheit beim Bund. Sie legt den Fokus auf die kritischsten Informationen und Systeme sowie auf die Standardisierung der Massnahmen. Somit soll die Informationssicherheit beim Bund nachhaltig und wirtschaftlich verbessert werden.

Ausgangslage

Mehrere Angriffe auf Informationssysteme des Bundes haben aufgezeigt, dass der Schutz von Informationen beim Bund Lücken aufweist. Diese Lücken sind auch auf unzeitgemässe Rechtsgrundlagen zurückzuführen. Die bestehenden formell-gesetzlichen Grundlagen für die Informationssicherheit finden sich heute verstreut in einer Vielzahl von Erlassen. Die verschiedenen Vorschriften sind sektoriell ausgelegt, kaum aufeinander abgestimmt und weisen wesentliche Lücken und Widersprüche auf. In der Folge betreibt der Bund heute sowohl rechtlich als auch organisatorisch parallele Strukturen für Teilbereiche der Informationssicherheit. Mit der Entwicklung zu einer Informationsgesellschaft sind die entsprechenden Bedrohungen komplexer und dynamischer geworden. Ihnen muss professionell, vernetzt und integral begegnet werden. Die Praxis hat gezeigt, dass die sektorielle Ausrichtung beim Bund nicht mehr geeignet und effizient ist. Die Massahmen der Informationssicherheit müssen auf die Bedürfnisse der Informationsgesellschaft abgestimmt, möglichst risikogerecht eingesetzt und behördenübergreifend koordiniert werden. Deshalb sollen diese Massnahmen in eine einzige moderne Regelung zusammengeführt werden. Dies entspricht auch den internationalen Standards, welche die Informationssicherheit nach einem integralen Ansatz regeln.

Der Bundesrat beauftragte das VBS, formell-gesetzliche Grundlagen für die Informationssicherheit des Bundes auszuarbeiten. Er verlangte dabei, dass für alle Bundesbehörden minimale Sicherheitsstandards gelten. Im Verlaufe der Arbeiten am Entwurf beschloss der Bundesrat zahlreiche Massnahmen, die in der Vorlage berücksichtigt werden mussten. Die überwiegend positiven Ergebnisse des Vernehmlassungsverfahrens haben bestätigt, dass im Bereich der Informationssicherheit Handlungsbedarf besteht und dass die Vorlage eine geeignete Lösung dafür darstellt.

Inhalt der Vorlage

Der Bundesrat verfolgt mit dieser Vorlage zwei ambitiöse Ziele. Zum einen will er die wichtigsten Rechtsgrundlagen für die Sicherheit von Informationen und Informatikmitteln des Bundes in einen einzigen Erlass zusammenführen (Einheitserlass). Dabei sollen Lücken des geltenden Rechts geschlossen sowie zahlreiche Anliegen der parlamentarischen Aufsichtsbehörden berücksichtigt werden. Zum anderen soll die Regelung für alle Behörden und Organisationen des Bundes gelten. Damit soll der Bund ein möglichst einheitliches Sicherheitsniveau erreichen. Gleichzeitig ist die Regelung aber auch in zweifacher Hinsicht sehr bescheiden. Erstens basiert die Vorlage auf anerkannten, in der Praxis erprobten internationalen Standards. Zwei-

tens legt sie keine detaillierten Massnahmen zur Gewährleistung der Informationssicherheit fest, sondern schafft lediglich einen formell-gesetzlichen Rahmen, auf dessen Grundlage die jeweiligen Bundesbehörden auf Verordnungs- und Weisungsebene die Informationssicherheit konkretisieren werden.

Das Gesetz regelt insbesondere das Risikomanagement, die Klassifizierung von Informationen, die Sicherheit beim Einsatz von Informatikmitteln, die personellen Massnahmen sowie den physischen Schutz von Informationen und Informatikmitteln. Um ein möglichst einheitliches Sicherheitsniveau zu erreichen und um die Kosten der Informationssicherheit zu senken, sollen die Anforderungen und Massnahmen standardisiert werden. Das Öffentlichkeitsprinzip in der Verwaltung soll weiterhin uneingeschränkt gelten, weshalb der Entwurf den Vorrang des Öffentlichkeitsgesetzes ausdrücklich vorsieht.

Die Regelung über die Personensicherheitsprüfungen wird vom Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR 120*) in dieses Gesetz übertragen. Gleichzeitig wird sie an die heutigen Bedürfnisse der Informationssicherheit angepasst. Der Bundesrat will den Einsatz der Personensicherheitsprüfung auf das Mindestmass reduzieren, das zur Identifizierung von erheblichen Risiken erforderlich ist. Inskünftig sollen deutlich weniger Prüfungen durchgeführt werden.*

Zur Gewährleistung der Informationssicherheit bei der Vergabe von sicherheitsempfindlichen Aufträgen an Dritte – einschliesslich der kritischen IKT-Beschaffungen des Bundes – will der Bundesrat den Geltungsbereich des militärischen Betriebssicherheitsverfahrens auf zivile Beschaffungen erweitern. Er will dieses neue Instrument gezielt und unbürokratisch einsetzen. Er will auch eine Grundlage für die Abgabe von Sicherheitserklärungen zugunsten von Schweizer Unternehmen schaffen, die sich für ausländische Aufträge bewerben und hierfür eine nationale Sicherheitserklärung benötigen.

Zur Unterstützung der Betreiberinnen von kritischen Infrastrukturen im Bereich der technischen Informationssicherheit müssen die zuständigen Organe des Bundes Adressierungselemente im Fernmeldebereich bearbeiten. Adressierungselemente können unter Umständen als besonders schützenswerte Personendaten betrachtet werden. Der Entwurf schafft die Grundlage für deren Bearbeitung und Austausch.

Das Gesetz richtet sich primär an die Bundesbehörden. Der Bundesrat will jedoch auch die Zusammenarbeit mit den Kantonen verbessern. Die Kantone sollen für eine gleichwertige Informationssicherheit sorgen, wenn sie klassifizierte Informationen des Bundes bearbeiten oder auf seine Informatikmittel zugreifen. Zur Verstärkung der Zusammenarbeit sollen die Kantone Einsitz im vorgesehenen Koordinationsorgan des Bundes nehmen und an der Standardisierung der Massnahmen mitwirken.

Die Umsetzungskosten hängen weitgehend vom Sicherheitsniveau, das die Bundesbehörden erreichen wollen, und vom entsprechenden Ausführungsrecht ab. Der personelle Mehrbedarf zur Verbesserung der Informationssicherheit soll grösstenteils durch eine Reduktion des Personalaufwands für die Personensicherheitsprüfungen kompensiert werden. Insgesamt könnten nach heutiger Einschätzung mittelfristig zwischen vier und elf zusätzliche Stellen erforderlich sein.

Inhaltsverzeichnis

Botschaft

1 Grundzüge der Vorlage

1.1 Ausgangslage

1.1.1 Entwicklung zu einer Informationsgesellschaft

Die Welt erlebt seit einigen Jahrzehnten einen fundamentalen gesellschaftlichen Wandel, der durch die sich noch laufend beschleunigenden Entwicklungen der Informatik gefördert wird. Von den neuen Möglichkeiten, jederzeit und überall auf Informationen zugreifen und diese austauschen zu können, sind alle Bereiche der Gesellschaft betroffen: Kultur, Wirtschaft, Bildung und Forschung, Gesundheit, Verkehr und Energie, Verteidigung usw. Diese Entwicklungen sind zugleich unvermeidliche Begleiterscheinung und unentbehrliche Bedingung für die laufende Globalisierung. Alle Gesellschaften werden vernetzter, mobiler und mehrheitlich transparenter als je zuvor. Unsere Lebensweise hat sich innert – historisch betrachtet – kürzester Zeit grundlegend verändert.

Der Einsatz der Informatik eröffnet der Schweiz bei ihrer Entwicklung zu einer Informationsgesellschaft vielfältige Chancen. Mit den neuen technischen Möglichkeiten und Vernetzungen sind aber auch Risiken verbunden, die nicht ignoriert werden dürfen. Informationen kann ein hoher Wert zukommen. Der Verlust, der Diebstahl, die Preisgabe und der Missbrauch von Informationen oder die Störung der Mittel zu deren Bearbeitung (Informatikmittel) können wesentliche öffentliche Interessen oder die Rechte Dritter schwerwiegend beeinträchtigen, erhebliche finanzielle Folgen nach sich ziehen und sogar die Erfüllung kritischer gesetzlicher Aufgaben des Bundes gefährden.

Strategie für eine digitale Schweiz

Der Bundesrat ist sich der grundlegenden Bedeutung der Informatik für den Wirtschaftsstandort und den Lebensraum Schweiz bewusst. Bereits 1998[1] hat er eine Strategie für eine Informationsgesellschaft in der Schweiz verabschiedet, die 2006[2] und 2012[3] aktualisiert wurde. Am 20. April 2016[4] hat der Bundesrat die Strategie «Digitale Schweiz» verabschiedet, mit der die Strategie von 2012 abgelöst wurde. Im Zentrum der neuen Strategie steht die konsequente Nutzung der Chancen der Digitalisierung, damit sich die Schweiz als attraktiver Lebensraum und innovativer, zukunftsorientierter Wirtschafts- und Forschungsstandort behaupten kann. Um dieses Ziel zu erreichen, gibt die Strategie die Leitlinien für das staatliche Handeln vor. Sie zeigt auf, wie Behörden, Wirtschaft, Wissenschaft und Forschung sowie die Zivilgesellschaft zusammenarbeiten sollen, damit die mit der Digitalisierung einhergehenden Transformationsprozesse zum Nutzen der Schweiz gestaltet werden können.

1 BBl **1998** III 2387
2 BBl **2006** 1877
3 BBl **2012** 3765
4 BBl **2016** 3985

Der Bundesrat gab im Zusammenhang mit diesem gesellschaftlichen Wandel zahlreiche Projekte in Auftrag (z. B. E-Government, E-Justice, E-Health, elektronische Geschäftsverwaltung usw.). Zudem erteilte er dem EJPD mehrere Aufträge zur Sicherstellung der nötigen Rechtsgrundlagen. Aus diesen Projekten ergibt sich eine laufend komplexer und dynamischer werdende Vernetzung des Informationsaustauschs und der Systeme von Bürgerinnen, Bürgern und Behörden einerseits sowie von Behörden untereinander andererseits.

E-Government-Strategie Schweiz

Am 24. Januar 2007[5] verabschiedete der Bundesrat die E-Government-Strategie Schweiz. Diese nationale Strategie wurde unter Federführung des ISB in enger Zusammenarbeit mit den Kantonen und Gemeinden entwickelt. Sie bildet die Basis für Bund, Kantone und Gemeinden, ihre Bestrebungen auf gemeinsame Ziele auszurichten, und legt Grundsätze, Vorgehen sowie Instrumente zu deren Umsetzung fest. Sie verfolgt drei strategische Ziele:

- Die Bevölkerung kann die wichtigen – häufigen oder mit grossem Aufwand verbundenen – Geschäfte mit den Behörden elektronisch abwickeln.
- Die Wirtschaft wickelt den Verkehr mit den Behörden elektronisch ab.
- Die Behörden haben ihre Geschäftsprozesse modernisiert und verkehren untereinander elektronisch.

Die weiterentwickelte «E-Government-Strategie Schweiz» wurde Ende 2015 verabschiedet.[6]

Öffentlichkeitsprinzip der Bundesverwaltung

Der Bundesrat erkannte in seiner BGÖ-Botschaft, dass der damals in der Verwaltung geltende Geheimhaltungsgrundsatz den Anforderungen einer effektiven, demokratischen Kontrolle der Verwaltungstätigkeit durch die Bürgerinnen und Bürger nicht mehr gerecht wurde. Ende 2004 wurde in der Folge das Öffentlichkeitsgesetz verabschiedet. Es berechtigt jede Person, ohne besonderen Nachweis von Interessen amtliche Dokumente einzusehen und von den Verwaltungseinheiten Auskünfte über den Inhalt amtlicher Dokumente zu erhalten. Der Grundsatz der Öffentlichkeit hat eine Tragweite, die über den rein rechtlichen Rahmen hinausgeht. Er bedeutet, dass der Staat seine Informationen im Auftrag und im Namen des schweizerischen Volkes bearbeitet. Dieses ist jederzeit berechtigt, seine Kontrolle auszuüben. Ausnahmen vom Öffentlichkeitsprinzip sind zwar möglich, werden im Gesetz aber abschliessend aufgezählt. Wird der Zugang zu einem Dokument zum Schutz von überwiegenden öffentlichen oder privaten Interessen ausnahmsweise eingeschränkt, aufgeschoben oder verweigert, muss das entsprechende Dokument in der Folge gemäss seinem tatsächlichen Schutzbedarf geschützt werden.

5 Die Strategie ist im Internet unter folgender Adresse abrufbar: www.egovernment.ch > Umsetzung > E-Government Schweiz 2008–2015.

6 Die Strategie ist im Internet unter folgender Adresse abrufbar: www.egovernment.ch > Umsetzung > E-Government-Strategie Schweiz.

Open-Government-Data-Strategie Schweiz

OGD ist ein Konzept, das auf die Zugänglichkeit und Wiederverwendung von Daten zielt, die im Rahmen der Verwaltungstätigkeit produziert werden. Die Veröffentlichung und freie Sekundärnutzung von Behördendaten kann wirtschaftlichen, politischen und verwaltungsinternen Nutzen stiften. Eine Abwägung von Chancen und Risiken von OGD zeigt, dass ein attraktives Potenzial für eine transparente, effiziente Verwaltungsführung und die wirtschaftliche Wertschöpfung besteht. Der Bundesrat hat deshalb am 16. April 2014[7] die Open-Government-Data-Strategie Schweiz 2014–2018 verabschiedet. Darin legt er seine Vision und seine strategischen Ziele fest. Schliesslich werden für die Umsetzung Grundsätze und konkrete Massnahmen definiert. Die Veröffentlichung von Daten im Sinne von OGD kommt nur für jene Daten in Frage, die im Besitz der Bundesbehörden sind und deren Wiederverwendung nicht aus datenschutz-, urheber- oder informationsschutzrechtlichen Gründen unzulässig ist. Zudem müssen die Behörden dafür sorgen, dass die zugänglich gemachten Daten integer (richtig) und nachvollziehbar sind. Sie müssen die entsprechenden rechtlichen, organisatorischen und technischen Massnahmen festlegen und umsetzen.

1.1.2 Risiken der Informationsgesellschaft

Der Bundesrat will das Risiko reduzieren, dass der gesellschaftliche Wandel zu Nachteilen für die Bevölkerung und die Wirtschaft oder zur Verletzung von Persönlichkeitsrechten führt. Es bestehen insbesondere Risiken, die nicht primär die Auswirkungen des gesellschaftlichen Wandels (z. B. sogenannte *digitale Gräben*), sondern die Informationen selbst sowie die vernetzte Informations- und Kommunikationsinfrastruktur betreffen. Der wahre Wert von Informationen wird bedauerlicherweise oft erst nach einem Vorfall und beim Eintreten negativer Auswirkungen erkannt. Sowohl für öffentliche Stellen als auch für Unternehmen und Privatpersonen kann der Verlust, der Diebstahl, die unberechtigte Preisgabe oder der Missbrauch von Informationen äusserst unliebsame Folgen zeitigen. Auch die Informations- und Kommunikationsinfrastruktur sowie die einzelnen Informatikmittel, die Behörden und Unternehmen zur Unterstützung ihrer Geschäftsprozesse einsetzen, sind verwundbar. So kann der Ausfall eines Informatiksystems je nachdem, wie heikel die damit bearbeiteten Geschäfte sind, erhebliche finanzielle Folgen nach sich ziehen. Wenn ein solcher Ausfall die Betreiberin einer kritischen Infrastruktur betrifft, die Dienste erbringt, die für das Funktionieren der Gesellschaft, der Wirtschaft oder des Bundes unerlässlich sind, kann dies schlimmstenfalls katastrophale Auswirkungen, einschliesslich des Verlusts von Menschenleben, zur Folge haben.

Gefahren für Informationen und Informatikmittel

Die Medien berichten fast täglich über Spionage, Angriffe, Ausfälle von Informatikdiensten und sonstige Ereignisse im Bereich der Informationssicherheit. Diese Gefahren werden auch in der NCS beschrieben. Für eine realistische Wahrnehmung in diesem Bereich sind drei Punkte zu beachten.

7 BBl **2014** 3493

Die Gefahren müssen ernst genommen werden. Fachleute haben zwar oft die Tendenz, die Gefahren und ihre potenziellen Auswirkungen zu dramatisieren. Umgekehrt dürfen die Risiken aber auch nicht unterschätzt werden. Die Geldmittel und das technische Knowhow, die von der organisierten Kriminalität eingesetzt werden, um Online-Kundendaten (insbesondere Bank- und Kreditdaten) zu stehlen oder Privatpersonen zu erpressen, mögen gross sein. Sie sind jedoch unbedeutend im Vergleich zu den finanziellen und personellen Mitteln, die von bestimmten staatlichen Akteuren eingesetzt werden, um politische, diplomatische, wissenschaftliche und wirtschaftliche Spionage zu betreiben. Gewisse Staaten verfolgen als prioritäre Massnahme gezielt Wirtschafts- und Industriespionage zur Industrialisierung und Weiterentwicklung ihrer Wirtschaft oder zur Modernisierung ihrer Streitkräfte.

Ernstzunehmende Gefahren bestehen überdies nicht nur in Bezug auf den Schutz der Vertraulichkeit von Informationen. Auch die Verfügbarkeit von öffentlichen und privaten Infrastrukturen und Diensten ist wegen deren Abhängigkeit von der Informatik gefährdet. Sabotageangriffe wie der im Juni 2010 entdeckte Angriff auf iranische Urananreicherungsanlagen mittels des Schadprogramms *Stuxnet* mögen die meist zitierten Gefährdungsannahmen darstellen. Betriebsstörungen wegen technischen Versagens, Fehlmanipulationen oder Elementarereignissen wie einem Stromausfall oder Brand kommen deutlich öfter vor und können ebenso gravierende Auswirkungen zur Folge haben.

Schliesslich dürfen die gross angelegte Überwachung des Internetverkehrs, insbesondere durch die Kompromittierung von breit benutzten Informatikdiensten und die systematische Korruption von Verschlüsselungsstandards nicht vergessen werden. Wir wissen heute, dass die Grundannahmen zur Integrität des Internets und der Basisdienste nicht zutreffen: Es kann nicht davon ausgegangen werden, dass die Informationen sicher bearbeitet werden.

Es findet ein digitales Wettrüsten statt. Die meisten entwickelten Länder sind sich ihrer Abhängigkeit von der Informatik und der damit verbundenen Bedrohungen bewusst. Sie setzen entsprechende Schutzvorkehrungen um. Bei weitem nicht alle Staaten verfolgen aber bloss *defensive* Strategien. Viele sind daran, auch *offensive* militärische und nachrichtendienstliche Fähigkeiten aufzubauen. Auch in der Schweiz werden nun Stimmen laut, die den Ausbau solcher offensiver Fähigkeiten fordern. Im Gegensatz zum klassischen Wettrüsten nehmen aber nicht nur staatliche oder staatlich finanzierte Akteure daran teil. Da die Entwicklung neuer technischer Schutz- oder Schadprogramme nicht immer besonders kompliziert und kostspielig ist oder grössere Infrastrukturen verlangt, arbeiten zahlreiche Informatiker, Mathematikerinnen und andere technologisch versierte Personen unermüdlich daran. Angesichts der eingesetzten Mittel und der Heterogenität der Akteure scheint das digitale Wettrüsten erst begonnen zu haben. Diese Dynamik einzudämmen wird eine riesige Herausforderung sein, auf die es zurzeit keine Antwort gibt. Fest steht nur, dass kein Land sie allein bewältigen kann.

Die enge Fokussierung auf den Bereich «Cyber» ist gefährlich. Durch die Digitalisierung der Informationsbearbeitung und die Vernetzung der Systeme zur Informationsbearbeitung, insbesondere über das Internet, sind neue Bedrohungsarten entstanden. Es ist deshalb verständlich, dass momentan der Schutz vor diesen neuen Bedrohungen im Zentrum der Aufmerksamkeit und des Handelns steht. Dies darf

aber nicht dazu führen, dass der Schutz von Informationen und Informatikmitteln auf den Schutz vor Cyber-Angriffen reduziert wird. Wesentliche Gefahren haben nämlich wenig oder nur indirekt mit dem Internet oder elektronischen Schadprogrammen zu tun. Spionage wird beispielweise immer noch mit *alten* Methoden ausgeübt. Zwar ist der Einsatz elektronischer Spionagemittel verhältnismässig günstig und weniger riskant als der Einsatz von eigentlichen Spionen. Die menschliche Komponente ist jedoch für die Beschaffung qualitativ hochwertiger Informationen weiterhin unentbehrlich. Informationen werden auch heute noch mündlich ausgetauscht oder auf Papier bearbeitet. Die Risiken, die damit verbunden sind, dürfen bei den Bestrebungen zur Schaffung von Informationssicherheit nicht ignoriert werden.

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

Der Bundesrat will in Zusammenarbeit mit Behörden, Wirtschaft und den KI-Betreiberinnen die Cyber-Risiken, denen diese täglich ausgesetzt sind, minimieren. Die NCS identifiziert Cyber-Risiken als Ausprägung bestehender Prozesse und Verantwortlichkeiten. Entsprechend sollen sie in bereits bestehenden Risikomanagementprozessen berücksichtigt werden.

Der Bundesrat verfolgt folgende Ziele:

- frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich;
- Erhöhung der Widerstandsfähigkeit der KI;
- wirksame Reduktion der Cyber-Risiken.

Zu diesem Zweck will er die Zusammenarbeit zwischen Behörden und Wirtschaft im Cyber-Bereich vertiefen und das bereits gelegte Fundament festigen. Die bestehende Kooperation des ISB mit dem NDB in der MELANI, die diese Aufgabe in Form von öffentlich-privaten Partnerschaften schon bis anhin wahrgenommen hat, wurde gestärkt. Der Bundesrat erteilte den Departementen überdies den Auftrag, in ihrem Zuständigkeitsbereich sowie im Dialog mit den kantonalen Behörden und der Wirtschaft die Umsetzung verschiedener Massnahmen an die Hand zu nehmen. Diese reichen von Risikoanalysen zu kritischen Informatikinfrastrukturen bis hin zur stärkeren Einbringung der Schweizer Interessen auf internationaler Ebene. Für die Koordination der Umsetzung der NCS wurde im EFD eine Koordinationsstelle geschaffen. Der Bundesrat setzt somit auf bestehende Strukturen und verzichtet auf ein zentrales nationales Steuerungs- und Koordinationsorgan, wie es derzeit in anderen Ländern aufgebaut wird.

Die Strategie wird im Laufe des Jahres 2017 aktualisiert.

Risiken für die Bundesbehörden

Die Bundesbehörden sind den in der NCS aufgeführten Gefahren ebenfalls ausgesetzt. Sie betreiben nämlich auch Informations- und Kommunikationsinfrastrukturen, deren Störung, Ausfall oder Zerstörung die Erfüllung kritischer gesetzlicher Aufgaben gefährden und somit gravierende Auswirkungen auf die Gesellschaft, die Wirtschaft oder den Staat haben kann.

Der Bund bearbeitet zur Erfüllung seiner Aufgaben zudem täglich grosse Mengen von Informationen. Unter diesen Informationen befinden sich auch solche, die für die innere oder äussere Sicherheit, die internationalen Beziehungen oder die wirtschaftspolitischen Interessen der Schweiz besonders wichtig sind und deshalb mittels Klassifizierung geschützt werden müssen. Klassifizierte Informationen sind aber nicht die einzigen Informationen, die einen erhöhten Schutzbedarf aufweisen. Spionage zielte zwar in der Vergangenheit hauptsächlich auf die Beschaffung von militärischen und aussenpolitischen Informationen. Sie ist heute aber vermehrt wirtschaftsorientiert. Im harten globalen Wettbewerb schafft sich derjenige einen entscheidenden Vorteil, der sich das Wissen (Forschungs- und Entwicklungsergebnisse, Knowhow) seiner Konkurrenten verschaffen kann. Entsprechend hat Spionage in der Wirtschaft und in der Industrie, insbesondere im hochtechnologischen Bereich, seit einigen Jahren zugenommen. Gerade in diesem Zusammenhang stellt die Bundesverwaltung ein hochsensibles Nervenzentrum dar: Sie reguliert die Privatwirtschaft; sie prüft bestimmte Produkte und entscheidet über deren Zulassung; sie kontrolliert gewisse Unternehmen; sie beschafft selber hochwertige Produkte und Dienstleistungen usw. Die Bundesverwaltung steht dabei in einem ständigen Dialog mit ihren öffentlichen und privaten Partnern im In- und im Ausland. Bei diesen Tätigkeiten bearbeitet sie sehr viele Informationen, die Geschäfts- und Fabrikationsgeheimnisse Dritter beinhalten. Sie kann in der Folge ins Visier derjenigen geraten, die solche Informationen beschaffen wollen. Dritte, die ihre Informationen aufgrund einer gesetzlichen Pflicht oder eines Vertrags den Bundesbehörden anvertrauen, erwarten zu Recht, dass diese auch dort zuverlässig geschützt werden.

Der Bund bearbeitet überdies in grossem Umfang Personendaten. Diese dürfen nach den Vorschriften der Datenschutzgesetzgebung nur rechtmässig, zweckkonform sowie in verhältnismässigem Rahmen bearbeitet werden. Sie müssen sowohl mit organisatorischen als auch mit technischen Massnahmen geschützt werden. Bei einem Datenmissbrauch können die Persönlichkeitsrechte der Personen, deren Daten bearbeitet werden, schwerwiegend verletzt werden. Gewisse Personendaten sind ebenso gefragt wie Technologieinformationen der Industrie. Es gibt einen blühenden Markt für die Beschaffung und die Bekanntgabe personenbezogener Daten.

Diese Risiken für den Bund sind nicht abstrakte, unwahrscheinliche Hypothesen. So wurde Anfang 2016 beim bundesnahen Rüstungsunternehmen RUAG ein Schadprogramm entdeckt, das Spionageaktivitäten ausführte. Das Schadprogramm blieb lange im Netzwerk der RUAG verborgen. Auf ähnliche Weise wurde in den Jahren zuvor das EDA angegriffen. Nicht vergessen werden dürfen die Bedrohungen durch Mitarbeitende des Bundes. So wurde im Mai 2012 beim NDB ein schwerwiegender Datendiebstahl entdeckt. Ein Mitarbeiter des NDB speicherte grosse Mengen sensibler Informationen, die ihm mit seinen Berechtigungen zugänglich waren, auf entfernbare Datenträger und schmuggelte sie aus den Räumlichkeiten des Dienstes. Vor seiner Verhaftung traf der Mitarbeiter erste Vorkehrungen, um die entwendeten Daten zu verkaufen.

Häufig werden auch weniger gravierende Vorkommnisse festgestellt. Diese Ereignisse reichen von Diebstahl oder Verlust von Laptops, Smartphones oder klassifizierten Informationsträgern über unberechtigte, meistens politisch motivierte Preisgabe von vertraulichen Informationen bis zu Betriebsstörungen wegen Server-

Ausfällen, Netzwerk-Überlastungen oder fehlerhaften Software-Konfigurationen. Da die Mehrheit solcher Vorfälle entweder nicht systematisch erfasst oder zumindest nicht zur Bewertung an die Fachorgane weitergeleitet wird, ist es schwierig, den Gesamtschaden für den Bund einzuschätzen. Bei schweren oder wiederholten Vorfällen, kann das Vertrauen in die Bundesbehörden ernsthaft gestört werden. Dies kann sogar so weit gehen, dass dem Bund Informationen vorenthalten werden, solange er deren zuverlässigen Schutz nicht nachweislich gewährleistet.

1.1.3 Notwendigkeit eines neuen Bundesgesetzes

Es stellt sich die Frage, inwiefern ein Gesetz im formellen Sinne für die Informationssicherheit der Bundesbehörden erforderlich ist. Nachfolgend werden die drei wichtigsten Gründe dafür zusammengefasst. Der detaillierte Regelungsbedarf sowie die vorgeschlagenen Lösungen werden unter Ziffer 1.2 erläutert.

Elektronisierung des Informationsaustauschs und Vernetzung der Informatik

Die Bundesbehörden tauschen zur Erfüllung ihrer verfassungsmässigen und gesetzlichen Aufgaben Informationen untereinander und mit Dritten aus. Dieser Informationsaustausch findet vermehrt und verstärkt elektronisch statt. Gleichzeitig nimmt die Vernetzung der Informatiksysteme der Bundesbehörden untereinander laufend zu. Damit steht fest, dass die Systeme der verschiedenen Bundesbehörden immer mehr gemeinsame Schnittstellen aufweisen. Dadurch erhöht sich das Risiko, dass sich Bedrohungen sowie Angriffe gegen eine Behörde auf die Zuständigkeitsbereiche anderer beteiligter Behörden ausbreiten. Werden Informationen auch ausserhalb der Organisation bearbeitet, so genügt der Schutz des eigenen Zuständigkeitsbereichs allein nicht mehr, weil die Schutzmassnahmen auch ausserhalb des eigenen Perimeters Wirkung erzielen müssen: Die Schutzmassnahmen müssen an die Information selbst verknüpft werden. Es ist deshalb unentbehrlich, dass die jeweiligen Behörden verpflichtet werden, ihre organisatorischen, personellen, technischen und physischen Sicherheitsmassnahmen zum Schutz von Informationen und Informatikmitteln aufeinander abstimmen und dass Dritte, die Informationen des Bundes bearbeiten, die Sicherheitsvorgaben des Bundes erfüllen.

Die bestehenden formell-gesetzlichen Grundlagen für die Informationssicherheit finden sich jedoch heute – meistens ohne ausdrückliche Erwähnung – verstreut in einer Vielzahl von Erlassen (z. B. RVOG, ParlG, MG, StGB, BWIS, BPG, BÖB, BGA, DSG, BGÖ), die nur für bestimmte Behörden gelten, zum Beispiel:

- Obschon die Klassifizierung von Informationen für die Durchführung von PSP massgebend ist (vgl. Art. 19 Abs. 1 BWIS), werden die entsprechenden Klassifizierungskriterien in einem Erlass (ISchV) festgelegt, der für die Bundesverwaltung und die Armee gilt, nicht aber für die anderen Bundesbehörden. Diese sind heute grundsätzlich frei, ihre eigenen Klassifizierungsstufen festzulegen. In der Folge stimmen weder die Kriterien noch die Schutzmassnahmen zwischen den Bundesbehörden überein.
- Die formell-gesetzliche Regelung der Sicherheit beim Einsatz von Informatikmitteln ist fast ausschliesslich nach dem Grundsatz des Perimeterschutzes

konzipiert (RVOG für die Bundesverwaltung; ParlG für das Parlament usw.).

- Die PSP können grundsätzlich nur bei Angestellten der Bundesverwaltung, Angehörigen der Armee und Dritten, die an klassifizierten Projekte des Bundes mitwirken, durchgeführt werden. In wenigen Fällen können auch kantonale Angestellte geprüft werden. Fraglich ist, ob Angestellte der anderen Bundesbehörden vom Geltungsbereich des BWIS überhaupt erfasst sind.
- Das Geheimschutzverfahren kann zurzeit aufgrund seines Geltungsbereichs nur für militärisch klassifizierte Beschaffungen durchgeführt werden. Bei kritischen Beschaffungen von zivilen Behörden darf es nicht angewendet werden.

Der Geltungsbereich der bestehenden Instrumente der Informationssicherheit muss alle Personen und Organisationen erfassen können, die vom Bund mit der Bearbeitung seiner Informationen oder mit dem Zugriff auf seine Informatiksysteme und -netze betraut werden. Nur so kann die erforderliche Sicherheit und das gegenseitige Vertrauen gewährleistet werden.

Ineffizienz der heutigen Regelungen

Neben Lücken beim Geltungsbereich weisen die bestehenden Rechtsgrundlagen zur Informationssicherheit weitere wesentliche materielle Lücken und Schwachstellen auf. So sind die meistens Instrumente sektoriell ausgelegt, ihre materiellen Regelungen kaum aufeinander abgestimmt und oft nicht auf die praktischen Bedürfnisse einer Informationsgesellschaft ausgerichtet, zum Beispiel:

- Datenschutz, Schutz von klassifizierten Informationen, Informatiksicherheit, PSP, Geheimschutzverfahren, Risikomanagement und physische Sicherheit werden alle in separaten Erlassen geregelt. In der Folge betreibt der Bund für jeden dieser Teilbereiche der Informationssicherheit parallele Organisationstrukturen. Der interdisziplinäre Koordinationsaufwand ist erheblich, eine gesamtheitliche Wirkungs- und Wirtschaftlichkeitsbetrachtung kaum möglich. Auch die Koordination von politischen Geschäften mit Bezügen zur Informationssicherheit sowie die Zusammenarbeit mit den Kantonen und den internationalen Partnern werden erheblich erschwert.
- Bei der sicheren Bearbeitung von Informationen legt die Gesetzgebung meistens das Schwergewicht auf den Schutz der Vertraulichkeit. Obschon die Auswirkungen beim Verlust der Verfügbarkeit von Informationen oder Informationssystemen deutlich schwerwiegender sein können als bei einem Verlust der Vertraulichkeit, kann heute bei Personen oder Firmen, die beim Bund oder für den Bund kritische Informatikmittel betreiben, keine PSP oder kein Geheimschutzverfahren durchgeführt werden.
- Einige Erlasse verlangen, dass Informationen (und Daten) nach dem Stand der Technik geschützt werden (vgl. z. B. Art. 8 Abs. 2 Bst. d DSG, Art. 3 Bst. k ISchV). Wer diesen Stand der Technik umschreibt, wird aber nicht festgelegt.

Mit der Entwicklung zu einer Informationsgesellschaft sind die entsprechenden Bedrohungen komplexer und dynamischer geworden. Ihnen muss professionell, vernetzt und integral begegnet werden. Die Praxis hat gezeigt, dass die sektorielle Ausrichtung beim Bund nicht mehr geeignet und effizient ist. Deshalb sollen alle wichtigsten Massnahmen der Informationssicherheit in eine einzige, moderne Regelung zusammengeführt und gesamtheitlich gesteuert werden. Dies entspricht auch dem integralen Ansatz der internationalen Standards zur Informationssicherheit.

Einschränkungen verfassungsmässiger Rechte und Bearbeitung von besonders schützenswerten Personendaten

Nach Artikel 36 Absatz 1 zweiter Satz sowie Artikel 164 Absatz 1 Buchstabe b BV gehören die grundlegenden Bestimmungen über die Einschränkungen verfassungsmässiger Rechte in ein Gesetz im formellen Sinne. Der Detaillierungsgrad der entsprechenden Regelung hängt von der Schwere des Eingriffs ab. Ferner dürfen Bundesorgane nach Artikel 17 Absatz 2 DSG besonders schützenswerte Personendaten sowie Persönlichkeitsprofile nur bearbeiten, wenn ein Gesetz dies ausdrücklich vorsieht. Formell-gesetzliche Grundlagen sind nötig für:

- den Einsatz von Informationssystemen zur zentralen Kontrolle von Identitäten, weil damit besonders schützenswerte Personendaten bearbeitet werden;
- die PSP, weil die Durchführung einer PSP mit einem erheblichen Eingriff in die Grundrechte von Privatpersonen verbunden ist;
- das BSV, weil die Durchführung eines BSV mit einem erheblichen Eingriff in die Grundrechte von Privatpersonen sowie juristischen Personen verbunden ist;
- die Unterstützung der KI-Betreiberinnen durch den Bund, weil dabei besonders schützenswerte Personendaten bearbeitet werden können;
- die Klassifizierung von Informationen, die Sicherheitseinstufung von Informatikmitteln sowie die Bezeichnung von Sicherheitszonen, weil sie Voraussetzungen für die Durchführung von PSP und BSV sind und entsprechend für die Einschränkung der verfassungsmässigen Rechte massgebend sind.

1.1.4 Aufträge des Bundesrats

Aufgrund dieser Entwicklungen und neuen Risiken hat der Bundesrat zahlreiche Aufträge erteilt, um die Informationssicherheit des Bundes zu verbessern. Nachfolgend werden nur diejenigen Aufträge aufgeführt, die für die Ausarbeitung der Gesetzesvorlage massgebend waren oder einen wesentlichen Einfluss darauf hatten. Anschliessend werden die Empfehlungen der parlamentarischen Aufsichtsorgane aufgeführt, die ebenfalls berücksichtigt wurden.

Verabschiedung der Informationsschutzverordnung und Prüfauftrag

Mitte 2007 verabschiedete der Bundesrat die neue IschV. Diese ersetzte die beiden bisherigen Verordnungen aus dem zivilen und dem militärischen Bereich und verzichtete auf die ohnehin kaum mehr mögliche Unterscheidung zwischen zivilen und

militärischen Informationen. Mit den darin geregelten Klassifizierungs- und Bearbeitungsvorschriften wurde zudem erstmals ein einheitliches Schutzniveau innerhalb der Bundesverwaltung festgelegt. Die IschV wurde als Übergangserlass konzipiert und ihre Geltungsdauer entsprechend befristet. Gleichzeitig mit ihrer Verabschiedung beauftragte der Bundesrat das VBS, ihm bis Ende 2009 einen Bericht über den Vollzug, die Wirksamkeit und die Wirtschaftlichkeit der IschV zu erstatten und Antrag zur Schaffung formell-gesetzlicher Grundlagen zu stellen.

Bundesratsbeschluss über Massnahmen zur Erhöhung der Informationssicherheit in der Bundesverwaltung

Der Bundesrat beschloss in der Folge des Angriffs auf die Systeme des EDA am 16. Dezember 2009 und am 4. Juni 2010 Massnahmen zur Erhöhung der Informationssicherheit in der Bundesverwaltung. Er legte dabei eine Reihe von organisatorischen und technischen Massnahmen fest, die kurz- und mittelfristig den Schutz der Informationen bei deren Bearbeitung mit Informatikmitteln der Bundesverwaltung verbessern sollen. Der Bundesrat beantragte zudem der EFK, den Stand der Umsetzung dieser Massnahmen zu überprüfen. Der erste Revisionsbericht der EFK wurde dem Bundesrat am 2. Dezember 2011[8] vorgelegt. Dieser Bericht gibt trotz eingeschränktem Prüfumfang einen guten Einblick in den Handlungsbedarf, der beim Einsatz der Informatik besteht.

Bundesratsauftrag zur Schaffung formell-gesetzlicher Grundlagen für den Informationsschutz bzw. die Informationssicherheit

Der vom Bundesrat bei der Verabschiedung der ISchV verlangte Bericht über die Wirksamkeit zeigte auf, dass die von der ISchV vorgesehene Übergangsfrist bis Ende 2009 für Anpassungen zur Gewährleistung des technischen Informationsschutzes mehrheitlich nicht eingehalten wurde. Damit bestanden erhebliche Lücken beim elektronischen Schutz von klassifizierten Informationen. Nach Kenntnisnahme des Berichts des VBS sowie in Anbetracht der Lehren aus dem Hacker-Angriff gegen das EDA erteilte der Bundesrat am 12. Mai 2010 dem VBS den Auftrag, formell-gesetzliche Grundlagen für den Informationsschutz auszuarbeiten. Die neue Regelung sollte insbesondere:

- den Geltungsbereich der Sicherheitsvorschriften auf alle Personen ausweiten, die vom Bund mit der Bearbeitung geschützter Informationen betraut werden;
- einheitliche formell-gesetzliche Grundlagen für die Durchführung von Geheimschutzverfahren im militärischen und zivilen Bereich schaffen;
- eine einheitliche Vertragsschlusskompetenz des Bundesrats für internationale Vereinbarungen im Bereich des Informationsschutzes schaffen.

Der Bundesrat beauftragte ferner das VBS, zu prüfen, ob und inwieweit weitere materielle Probleme im Bereich des Informationsschutzes einer formell-gesetzlichen Regelung zuzuführen sind sowie ob die Zuständigkeiten und Verantwortlichkeiten im Bereich der Informationssicherheit den heutigen Anforderungen genügen.

8 www.efk.admin.ch > Publikationen > Querschnittsprüfungen > Querschnittsprüfung > IT-Sicherheit in der Bundesverwaltung

Ergänzung des Bundesratsauftrags vom 12. Mai 2010

Am 14. Januar 2011 setzte der Departemensvorsteher des VBS eine Expertengruppe unter der Leitung von Prof. Dr. iur. Markus Müller, Ordinarius für Staats- und Verwaltungsrecht an der Universität Bern, ein. Der Departemensvorsteher des VBS erteilte ihr den Auftrag, ein Normkonzept und darauf gestützt einen Gesetzesentwurf auszuarbeiten. Die Expertengruppe unterbreitete ihr Normkonzept dem Departemensvorsteher des VBS am 29. Juni 2011. Dieser unterrichtete den Bundesrat über die Erkenntnisse der Expertengruppe. Der Bundesrat dehnte daraufhin mit Beschluss vom 30. November 2011 den künftigen Regelungsbereich vom engen Schutz klassifizierter Informationen auf eine umfassende Informationssicherheit aus. Er stellte zudem fest, dass aufgrund des stets zunehmenden elektronischen Austauschs von Informationen mit den anderen Behörden sowie der ebenfalls zunehmenden Vernetzung der Informatiksysteme eine wirksame Informationssicherheit nur noch dann erreicht werden kann, wenn für alle Bundesbehörden einheitliche minimale Sicherheitsstandards gelten. Er beschloss deshalb, dass der auszuarbeitende Entwurf für alle Behörden und Organisationen des Bundes gelten soll, wobei die detaillierten und bereichsspezifischen Ausführungsbestimmungen weiterhin in der Kompetenz der jeweiligen Bundesbehörden liegen sollen. Er beauftragte schliesslich das VBS, die Gesetzgebungsarbeiten mit den Aufträgen zur Erarbeitung der NCS sowie zur Strategie für eine Informationsgesellschaft in der Schweiz zu koordinieren.

Die Ausdehnung des Geltungs- und Regelungsbereichs sowie die geforderte Koordination mit den erwähnten Projekten führten zu einer Erweiterung der Expertengruppe. Vertreten waren nun: die BK, das EDA, das EJPD (GS, BJ, Fedpol), das VBS (GS, Armeestab), das EFD (GS, ISB, BIT), das UVEK (BAKOM), der EDÖB, die Parlamentsdienste, die eidgenössischen Gerichte und die Kantone (SIK). MELANI und der NDB wurden punktuell beigezogen.

Zusatzauftrag und Erweiterung zu einer IDAG

Nach Bekanntwerden eines Vorfalls im NDB erhielt die Expertengruppe am 24. Oktober 2012 vom Bundesrat den Zusatzauftrag, einen Bericht über die Gefahren und Lücken in der Informationssicherheit in der Bundesverwaltung zu erstellen sowie Vorschläge für Sofortmassnahmen zu unterbreiten. Die Expertengruppe wurde hierauf noch einmal erweitert. Sie bildete nun mit Vertreterinnen und Vertretern des EDI und des WBF eine IDAG. Die IDAG ISG überreichte ihren Bericht samt Empfehlungen am 29. Januar 2013 dem VBS. Daraufhin beschloss der Bundesrat am 15. März 2013, das Führungskader der Bundesverwaltung schulen zu lassen. Für die Durchführung der Ausbildungsmassnahmen ist das EPA federführend.

Bundesratsauftrag zur Harmonisierung und Straffung der PSP

Am 1. Februar 2012 beauftragte der Bundesrat das VBS, eine Harmonisierung und Straffung der zu überprüfenden Funktionen und der ihnen zugeordneten Prüfstufen sowie weitere Optimierungsmassnahmen mit Auswirkungen auf den Ressourcenbereich zu prüfen. Nach Kenntnisnahme des Berichts der hierfür eingesetzten IDAG PSP beauftragte der Bundesrat am 29. November 2013 unter anderem die IDAG ISG, bei ihren Arbeiten die Empfehlungen des Berichts zu berücksichtigen und, soweit angemessen, in den Gesetzesentwurf einzuarbeiten (s. Ziff. 1.2.5).

Verabschiedung der Verordnung über die Durchführung von BSV im Rahmen der europäischen Satellitennavigationsprogramme Galileo und EGNOS

Mit Beschluss vom 13. Dezember 2013[9] genehmigte der Bundesrat das Kooperationsabkommen mit der EU zur Teilnahme der Schweiz an den Satellitennavigationsprogrammen Galileo und EGNOS. Damit erhielten Schweizer Unternehmen einen gleichberechtigten Zugang zu den mit diesen Programmen zusammenhängenden Ausschreibungen. Mit dem Abkommen verpflichtete sich die Schweiz auch, die beiden Programme insbesondere gegen missbräuchliche Verwendung, Frequenzstörungen und feindliche Aktivitäten zu schützen. Sie muss dabei ein Sicherheitsniveau gewährleisten, das mit dem Sicherheitsniveau der EU vergleichbar ist. Schweizerische Firmen oder Forschungsinstitute, die sich an sicherheitsrelevanten Beschaffungen oder Forschungsaufträgen beteiligen wollen, benötigen dafür eine nationale BSE. Da zurzeit die Durchführung von entsprechenden BSV nur im militärischen Bereich – und zwar gestützt auf die veraltete Geheimschutzverordnung des EMD vom 29. August 1990[10] – zulässig ist, verabschiedete der Bundesrat am 6. Juni 2014 als Übergangslösung bis zum Inkrafttreten des ISG eine direkt auf die BV gestützte Verordnung[11], die es der zuständigen Fachstelle beim VBS ermöglicht, für Beschaffungen im Rahmen von Galileo und EGNOS BSE auszustellen.

Auftrag zur Schaffung einer gesetzlichen Grundlage für IAM Bund

Zur Erfüllung ihrer Aufgaben betreiben die Behörden und Organisationen des Bundes zahlreiche Informationssysteme. Für jedes dieser Systeme muss sichergestellt werden, dass die richtigen Personen und Anwendungen zum richtigen Zeitpunkt den richtigen Zugriff erhalten, was eine Identitäts- und Zugriffsverwaltung voraussetzt. Mit dem stets zunehmenden Umfang der Nutzung von Informationen über die Organisationsgrenzen hinweg können die Anforderungen an Schutz und Funktionalität nur noch mit übergreifend koordinierten Systemen effizient erfüllt werden. Mit IAM Bund ist geplant, die Authentifizierung von Benutzerinnen und Benutzern und die Überprüfung gewisser Attribute und Berechtigungen statt bei jeder einzelnen Fachanwendung separat neu für mehrere Fachanwendungen gemeinsam vorzunehmen. Gewisse Aspekte der zentralisierten Bearbeitung von Personendaten bedürfen aus Datenschutzgründen einer formell-gesetzlichen Grundlage. Da eine effiziente Verwaltung von Identitäten und Zugriffen für die Informationssicherheit entscheidend ist, beauftragte der Bundesrat am 14. Januar 2015 das VBS, zusammen mit dem EFD den Entwurf zum ISG mit einer Grundlage für Identitätsverwaltungs-Systeme zu ergänzen.

Empfehlungen der parlamentarischen Aufsichtsorgane

Die GPK und die GPDel befassen sich regelmässig mit Themen aus dem Bereich der Informationssicherheit. Sie haben in den jüngsten Jahren mehrere Verbesserungen empfohlen, die der Bundesrat bei der Ausarbeitung dieser Vorlage berücksichtigt hat.

9 SR **0.741.826.8**
10 SR **510.413**
11 SR **510.661**

- *Bericht der GPK-S vom 3. Dezember 2010*[12] *über das Verhalten der Bundesbehörden in der diplomatischen Krise zwischen der Schweiz und Libyen, Empfehlung 12:* Die GPK-S stellte im Rahmen ihrer Prüfung zur Krise zwischen der Schweiz und Libyen eine Reihe von Informationsschutzproblemen fest. In ihrem Bericht hielt sie fest, dass *«derartige Ereignisse belegen, dass in Sachen Informationsschutz und Schutz von technischen Geräten in der Bundesverwaltung ein grosser Handlungsbedarf besteht, weshalb es zwingend ist, dass eine rasche Abhilfe erfolgt»*. Sie empfahl dem Bundesrat, *«in seinem Kompetenzbereich die nötigen Massnahmen zu treffen, um inskünftig die Geheimhaltung auch auf höchster Stufe innerhalb der Bundesverwaltung gewährleisten zu können. Dabei ist auch den technischen Aspekten der den Mitarbeitenden abgegebenen Geräte eine gebührende Aufmerksamkeit zu schenken»*.
- *Bericht der GPK-N vom 12. April 2013*[13] *zur Nachkontrolle zur Inspektion über die Umstände der Ernennung von Roland Nef zum Chef der Armee*
  - *Empfehlung 1:* Die GPK-N forderte den Bundesrat auf, im Rahmen der Ausarbeitung des ISG eingehend zu prüfen, ob es zweckmässig ist, im formellen Gesetz zum einen zu definieren, was ein Sicherheitsrisiko im Sinne der PSP ist, und zum anderen festzuhalten, was das Endziel dieser Kontrollen ist.
  - *Empfehlung 5:* Die GPK-N forderte den Bundesrat auf, dafür zu sorgen, dass die Situation in Bezug auf Personen ohne Schweizer Staatsbürgerschaft rasch geklärt wird und die beiden Fachstellen PSP einheitlich und gestützt auf klare Rechtsgrundlagen verfahren.
- *Bericht der GPDel vom 30. August 2013 über die Informatiksicherheit beim NDB (Zusammenfassung):* Die GPDel beschloss am 15. Oktober 2012, eine formelle Inspektion zur Informatiksicherheit im NDB durchzuführen. Sie erstellte Anfang Juli 2013 einen umfassenden Bericht zuhanden des Bundesrats und publizierte einen Kurzbericht, der elf Empfehlungen enthält. Für den Entwurf sind insbesondere drei Empfehlungen wichtig:
  - *Empfehlung 5:* Die GPDel empfahl dem Bundesrat, mit einer Revision der PSPV dafür zu sorgen, dass für externe Mitarbeitende die gleichen Anforderungen an die Stufe der PSP gestellt werden wie für Angestellte des Bundes, welche die gleichen Aufgaben wahrnehmen. Die Verantwortung für die Einhaltung der Vorschriften durch externe Firmen und ihre Mitarbeitenden sei derjenigen Bundesstelle zu übertragen, für welche die Externen letztlich ihre Leistung erbringen. Anlässlich der Nachkontrolle zur Inspektion bat die GPDel den Bundesrat mit Schreiben vom 30. Juni 2014, dafür besorgt zu sein, dass im ISG die PSP für die externen Mitarbeitenden genau so präzise und umfassend geregelt wird wie für die internen Angestellten des Bundes (vgl. Jahresbericht 2014 der GPK/GPDel vom 30. Januar 2015[14], Ziff. 4.3.4).

12 BBl **2011** 4304
13 BBl **2013** 6241
14 BBl **2015** 5217

- *Empfehlung 6:* Die GPDel empfahl dem Bundesrat, in dieser Botschaft die Rollen, welche die PSP und die Personalführung in der Informationssicherheit spielen, ausführlich darzulegen und klar voneinander abzugrenzen. Gleichzeitig soll in einem separaten Bericht erläutert werden, wie viele personelle Ressourcen der Bund für die Durchführung der PSP einsetzen soll und welchen Beitrag an den Informationsschutz er damit leisten will.
- *Empfehlung 9:* Die GPDel empfahl dem Bundesrat, Vorschläge zu erarbeiten, um das Verfahren zur Überprüfung des Standes der Informatiksicherheit im Bund zu verbessern. Die Massnahmen sollen den Bundesrat befähigen, im Rahmen eines institutionalisierten Verfahrens Risiken der Informatiksicherheit rechtzeitig zu erkennen, die notwendigen risikomindernden Massnahmen zu beschliessen und ihre Umsetzung zu verfolgen.

– *Bericht der GPK-S vom 7. Oktober 2014*[15] *über externe Mitarbeitende der Bundesverwaltung:* In diesem Bericht beurteilte die GPK-S die Resultate und die Feststellungen einer durch die Parlamentarische Verwaltungskontrolle durchgeführten Evaluation über den Umfang, die Rechtmässigkeit, die Transparenz sowie die Zweckmässigkeit der Beiziehung externer Mitarbeitender in der Bundesverwaltung. Sie formulierte anschliessend sechs Empfehlungen zuhanden des Bundesrats. Mit ihrer Empfehlung 6 ersuchte die GPK-S den Bundesrat, den PSP von externen Mitarbeitenden mit Informatikaufgaben besondere Beachtung zu schenken, da diese Zugang zu Informationen oder Material haben, die «vertraulich» oder «geheim» klassifiziert sind. Auch ersuchte die GPK-S den Bundesrat, die Rechtsgrundlagen der PSP so zu ändern, dass das Ergebnis dieser Prüfungen vor Arbeitsantritt der betreffenden Mitarbeiterin oder des betreffenden Mitarbeiters bekannt sein muss.

1.2 Die beantragte Neuregelung

Mit der beantragten Neuregelung will der Bundesrat einen einheitlichen rechtlichen Rahmen zur Steuerung und Umsetzung der Informationssicherheit für alle Bundesbehörden schaffen. Alle Grundsätze und Massnahmen der Informationssicherheit sollen in einen einzigen Einheitserlass zusammengeführt werden, sodass die Umsetzung nach einem integralen Ansatz erfolgen kann und ein möglichst einheitliches behördenübergreifendes Sicherheitsniveau erreicht wird. Gleichzeitig sollen Lücken des geltenden Rechts behoben werden, damit die Bundesbehörden über zeitgemässe, auf die Bedürfnisse der Informationsgesellschaft ausgerichtete rechtliche Grundlagen verfügen. Ferner sollen die erforderlichen zentralen Befugnisse des Bundes zur Umsetzung der NCS formell-gesetzlich abgedeckt werden. Schliesslich soll die Fachorganisation der Informationssicherheit professioneller und effizienter werden.

15 BBl **2015** 3673

Nachfolgend werden der detaillierte Regelungsbedarf und die vorgeschlagenen Lösungen für die Kernpunkte der beantragten Neuregelung dargestellt.

1.2.1 Informationssicherheit

Informationen werden heute mehrheitlich in elektronischer Form bearbeitet. Ihr Schutz hängt deshalb immer mehr von den elektronischen Verfahren und Mitteln ab, mit welchen sie bearbeitet werden. Zurzeit sind beim elektronischen Schutz von Informationen aller Art wesentliche Sicherheitslücken vorhanden. Vor diesem Hintergrund muss aber festgehalten werden, dass die Aufgaben derjenigen Stellen, die für die Vorgaben der Informatiksicherheit oder für deren Umsetzung zuständig sind, innert kürzester Zeit wesentlich komplexer geworden sind. Gründe dafür sind die laufenden technologischen Innovationen, die damit verbundenen neuen Gefahren und Schwachstellen sowie die zu knappen finanziellen und personellen Ressourcen. Angesichts der Herausforderungen im technischen Bereich kündigte MELANI bereits 2008 in ihrem Halbjahresbericht an, dass eine Neuausrichtung notwendig sei:

> «Aktuelle gezielte IT-Angriffe lassen sich auch mit Hilfe technischer Sicherheitsvorkehrungen sowie einer gesunden Portion Menschenverstand nicht immer erfolgreich abwehren. Deshalb ist eine Neufokussierung nötig, welche den Schutz der Information ins Zentrum rückt und nicht nur den Schutz der Computer und Netzwerke berücksichtigt. […] Dies wird ein verstärktes Informations- und Datenmanagement, Informationsklassifizierung und dergleichen nach sich ziehen.»[16]

Diese Aussage ist für das Verständnis der beantragten Neuregelung zentral. Die technische Informatiksicherheit allein genügt nicht mehr. Bedeutend wichtiger für einen wirksamen Schutz der Informationen sind die organisatorischen Massnahmen. Organisatorische Mängel bestehen beim Bund insbesondere bei den Rechtsgrundlagen sowie beim Management der Informationssicherheit.

Mängel bestehen vorab bei den rechtlichen Rahmenbedingungen. Die heutigen Rechtsgrundlagen für den Schutz von Informationen sind sehr sektoriell ausgelegt, kaum aufeinander abgestimmt und oft lückenhaft. In der Folge betreibt der Bund heute sowohl rechtlich also auch organisatorisch parallele Systeme für den Datenschutz, den Schutz klassifizierter Informationen, die Informatiksicherheit, die physische Sicherheit und das Risikomanagement. Ferner ist heute die Durchführung von PSP und BSV ausschliesslich bei Personen und Unternehmen vorgesehen, die klassifizierte Informationen des Bundes bearbeiten, nicht aber bei Personen, die seine kritischen Informatikmittel verwalten oder betreiben. Darüber hinaus sind die Rechtsgrundlagen oft nicht auf die praktischen Bedürfnisse der elektronischen Bearbeitung von Informationen abgestimmt.

Dass Sicherheit Chefsache ist und ein effizientes Management der Informationssicherheit sich wirtschaftlich lohnt, wird in der Privatwirtschaft spätestens dann wahrgenommen, wenn ein Schadenfall eintritt und Schadenbegrenzung betrieben wird. Bei öffentlichen Verwaltungen wird Sicherheit aber häufig lediglich als Kos-

16 www.melani.admin.ch > Dokumentation > Lageberichte

tentreiber und Hindernis betrachtet. Grund dafür ist insbesondere die Tatsache, dass der öffentlichen Hand bei Vorfällen kein wettbewerblicher Schaden entstehen *kann*. Demzufolge wird in der Regel auch der Produktivitätsverlust, der beispielsweise durch den Ausfall von Informatikdiensten verursacht wird, weder eruiert noch mit den Kosten von risikomindernden Massnahmen abgewogen.

Beim Bund ist die Lage nicht anders. Die Informatiksicherheit wird oft als rein technische Angelegenheit betrachtet und nicht als Führungsaufgabe wahrgenommen. Demzufolge haben die Linienvorgesetzten in der Regel nur wenig Verständnis für ihre Rolle im Sicherheitsprozess und die geschäftsüblichen Führungstätigkeiten (z. B. Setzung von Zielen, Kontrolle der Umsetzung oder Prüfung der Wirksamkeit von Massnahmen) finden nur selten auf den Sicherheitsbereich Anwendung. Auch die Kosten der Sicherheit können nicht transparent dargelegt werden, was eine Beurteilung der Wirtschaftlichkeit der Massnahmen (Kosten-Nutzen-Analyse) verunmöglicht. Schliesslich werden bei Vorfällen oder Verstössen gegen die Vorschriften die Verantwortlichen nur selten zur Rechenschaft gezogen.

Informationen können aus verschiedenen Gründen schutzwürdig sein. Die organisatorischen und technischen Massnahmenpakete, die zur Umsetzung der jeweiligen Schutzbedürfnisse erforderlich sind, unterscheiden sich jedoch kaum. Wenn deren Umsetzung einheitlich geregelt, organisiert und geführt wird, können Synergien genutzt und gleichzeitig der Schutz verbessert werden. Dafür müssen die Rechtsgrundlagen zwingend auf die Bedürfnisse der Informationsgesellschaft abgestimmt werden und die Linienvorgesetzten ihre Aufgaben klarer wahrnehmen.

Der Bundesrat ist sich der zunehmenden gegenseitigen Abhängigkeiten zwischen dem technischen und organisatorischen Schutz von Informationen sowie den aufgeführten organisatorischen Mängeln bewusst. Er hat die Rechtsetzungsarbeiten am ISG entsprechend ausgerichtet: Das Ziel ist eine umfassende, die organisatorische und technische Seite berücksichtigende *Informationssicherheit.* Die Neuregelung hat sich nach *anerkannten internationalen Standards* zu richten. Diese *integrale Informationssicherheit* entspricht dem, was in der Privatwirtschaft und in vielen öffentlichen Verwaltungen weltweit bereits seit einigen Jahren als *règle de l'art* gilt. Sie wird durch einige internationale Standards, insbesondere durch die Normen ISO/IEC 27001 und 27002[17], formalisiert. Solche Standards haben wenig mit der Technik zu tun. Der Fokus wird fast ausschliesslich auf die Aufgaben des *Managements* zum Schutz seiner informationellen Werte sowie auf die entsprechenden organisatorischen Massnahmen gesetzt. Die Standards enthalten jedoch auch praxistaugliche und -erprobte *Best Practices* zur Umsetzung von personellen, technischen und baulichen Massnahmen. Sie werden regelmässig angepasst, um neuen, insbesondere auch empirischen Erkenntnissen aus Studien und Vorfällen Rechnung zu tragen. Sie umschreiben also den Stand der Wissenschaft.

Das ISG schafft einheitliche formell-gesetzliche Grundlagen für das Management der Informationssicherheit im Bund. Es basiert im Aufbau und Inhalt grösstenteils auf den erwähnten Normen und beabsichtigt deren massgeschneiderte Umsetzung. Dabei wird die Informationssicherheit *nach einem integralen Ansatz* betrachtet, d. h. möglichst alle Belange der Informationssicherheit werden zusammen gesteuert,

17 Der Text der Normen ist abrufbar unter www.iso.org > Store > Normes ISO.

umgesetzt, überprüft und verbessert. Die Vorlage fasst dementsprechend die wichtigsten organisatorischen Massnahmen für den Schutz aller Informationen und zur Gewährleistung der Sicherheit beim Einsatz von Informatikmitteln in einer einzigen Regelung zusammen.

1.2.2 Geltungsbereich und Zusammenarbeit mit den Kantonen

Sachlicher Geltungsbereich

Der sachliche Geltungsbereich ergibt sich grundsätzlich aus dem Begriff der Informationssicherheit. Im Zentrum des Schutzes stehen alle Informationen, für welche die Bundesbehörden zuständig sind. Es handelt sich hauptsächlich um Informationen, welche die Bundesbehörden selber erstellen. Erfasst werden aber auch Informationen, die sie von Dritten erhalten und für deren sichere und rechtmässige Bearbeitung sie deshalb zuständig sind. Weiter sind Informationen betroffen, mit deren Bearbeitung die Bundesbehörden Dritte beauftragen. Das Gesetz gilt für Informationen jeglicher Art, also beispielsweise nicht bloss für Informationen in Textform, sondern auch für graphische Darstellungen, und in beliebiger Form, das heisst nicht bloss für elektronische Informationen sondern beispielsweise auch für Informationen auf Papierdokumenten.

Vom Entwurf werden sämtliche Informatikmittel erfasst, die von den Bundesbehörden eingesetzt werden oder deren Betrieb sie in Auftrag geben. Richtig besehen müssen zwar die technischen Mittel zur Verarbeitung von Informationen nicht um ihrer selbst willen geschützt werden, sondern vielmehr selbst den Schutz der damit verarbeiteten Informationen und der damit unterstützten Geschäftsprozesse gewährleisten. Da die Praxis aber die Informatikmittel als *Schutzobjekte* betrachtet, werden diese im ISG auch ausdrücklich erfasst.

Institutioneller Geltungsbereich

Beim vorliegenden Erlass handelt es sich über weite Strecken um einen Organisationserlass. Das Gesetz soll aber von allen Bundesbehörden sowie den ihnen unterstellten Organisationen in ihrem jeweiligen Zuständigkeitsbereich angewendet werden, da nur auf diese Weise eine wirksame Informationssicherheit erzielt werden kann. Einheiten der dezentralen Bundesverwaltung sowie Organisationen des öffentlichen oder privaten Rechts, die Verwaltungsaufgaben erfüllen, sollen das Gesetz ganz oder teilweise anwenden müssen, sofern sie sicherheitsempfindliche Tätigkeiten des Bundes ausüben oder zur Erfüllung ihrer Aufgaben Informatikmittel des Bundes einsetzen oder darauf zugreifen müssen. Diese risikobasierte Lösung entspricht der Absicht des Bundesrats, den Geltungsbereich der Informationsschutzregelungen auf alle Personen zu erstrecken, die vom Bund mit der Bearbeitung geschützter Informationen betraut werden.

Die Gründe, weshalb alle Bundesbehörden einschliesslich der gesetzgebenden und der rechtsprechenden Behörden vom Gesetz erfasst werden sollen, sind vielfältig. Zum einen tauschen die Bundesbehörden regelmässig zur Erfüllung ihrer verfassungsmässigen und gesetzlichen Aufgaben Informationen untereinander aus. Es ist

ein Ziel des Bundesrats, vermehrt und verstärkt auf den elektronischen Austausch von Informationen und auf elektronische Dienstleistungen zu setzen (E-Government). Unter diese Informationen fallen auch klassifizierte Informationen oder sonstige Informationen mit erhöhtem Schutzbedarf. Obschon die Klassifizierung bereits heute für die Durchführung von PSP massgebend ist, verwenden jedoch die Bundesbehörden bis anhin kein einheitliches Klassifizierungssystem. Die Sicherheitsmassnahmen der jeweiligen Behörden sind in der Folge sehr unterschiedlich und kaum aufeinander abgestimmt. Alle Bundesbehörden sollen die gleichen Klassifizierungsgrundsätze anwenden und äquivalente Schutzmassnahmen treffen. Nur so kann das beim Umgang mit solchen Informationen erforderliche gegenseitige Vertrauen gewährleistet werden.

Weiter nimmt die Vernetzung der Informatiksysteme der Bundesbehörden untereinander laufend zu. Damit steht fest, dass die Systeme der verschiedenen Bundesbehörden immer mehr gemeinsame Schnittstellen aufweisen werden. Dadurch wird das Risiko erhöht, dass sich Angriffe sowie Bedrohungen gegen eine Behörde auf die Zuständigkeitsbereiche anderer beteiligter Behörden ausbreiten können. Es ist deshalb unentbehrlich, dass die jeweiligen Bundesbehörden gleichwertige Risikobeurteilungskriterien und -methoden anwenden und dass ihre organisatorischen, personellen, technischen und physischen Sicherheitsmassnahmen beim Einsatz von Informatikmitteln aufeinander abgestimmt werden.

Schliesslich haftet der Bund nach Artikel 3 Absatz 1 VG für den Schaden, den das Personal der verpflichteten Behörden und Organisationen in Ausübung seiner amtlichen Tätigkeit Dritten widerrechtlich zufügt. Der Geltungsbereich des ISG stimmt entsprechend mit dem Geltungsbereich des VG überein. Einzig das Parlament und die Armee werden zusätzlich erfasst.

Zusammenarbeit mit den Kantonen

Bund und Kantone sind für ihre jeweilige Aufgabenerfüllung auf eine enge Zusammenarbeit angewiesen. Sie tauschen sehr viele Informationen untereinander aus. Dieser Austausch findet zunehmend elektronisch statt. Die Informatikinfrastrukturen und Systeme des Bundes und der Kantone werden zudem vermehrt untereinander vernetzt. Dadurch wird das Risiko erhöht, dass sich Bedrohungen im Zuständigkeitsbereich einer Behörde auf die Bereiche anderer Beteiligter ausbreiten.

Die Kantone sind für ihre Informationssicherheit selbst zuständig. Der Bundesrat will und kann aus verfassungsrechtlichen Gründen keine allgemeinen Vorschriften für die Kantone festlegen. Allerdings hat der Bund ein direktes Interesse daran, dass die Kantone und ihre untergeordneten Stellen einen gleichwertigen Schutz gewährleisten, wenn sie geschützte Informationen des Bundes bearbeiten oder auf seine Informatikmittel zugreifen. Analog zur Lösung der Datenschutzgesetzgebung (vgl. Art. 37 Abs. 1 DSG) sollen allerdings die Vorschriften des Bundes nur dann zur Anwendung kommen, wenn die Vorschriften und Massnahmen der Kantone den Sicherheitsanforderungen des Bundes nicht genügen (Subsidiarität). Die Kantone sollen zudem verpflichtet werden, die Wirksamkeit der getroffenen Schutzmassnahmen periodisch zu überprüfen und die zuständige Stelle des Bundes über die Ergebnisse zu informieren (vgl. auch. Art. 37 Abs. 2 DSG).

Der Bundesrat will zudem die Kantone bei der Umsetzung eng einbeziehen, um auch mit ihnen ein möglichst einheitliches Sicherheitsniveau zu erreichen. Deshalb sollen zwei Vertreterinnen oder Vertreter der Kantone im behördenübergreifenden Koordinationsorgan Einsitz nehmen. So werden sie den Vollzug des ISG mit den zuständigen Bundesstellen koordinieren und an der Standardisierung mitwirken.

1.2.3 Verhältnis zum Öffentlichkeitsgesetz und zur Datenschutzgesetzgebung

Verhältnis zum Öffentlichkeitsgesetz

Ein Ziel der Vorlage besteht darin, Informationen, die aus gesetzlichen und vertraglichen Gründen vertraulich bleiben müssen, bedarfsgerecht zu schützen. So legt der Entwurf auch die Kriterien fest, nach welchen Informationen zum Eigenschutz der Schweiz und des Bundes klassifiziert werden müssen. Mit dem BGÖ, das jede Person berechtigt, ohne besonderen Interessennachweis amtliche Dokumente einzusehen und von den Verwaltungseinheiten Auskünfte über den Inhalt amtlicher Dokumente zu erhalten, besteht demnach ein Spannungsverhältnis. Das ISG löst dieses, indem es dem BGÖ Vorrang gibt. Damit wird klar festgehalten, dass der Geltungsbereich des Öffentlichkeitsgesetzes durch die Regelung der Informationssicherheit in keiner Art und Weise eingeschränkt wird. Die Klassifizierungsbestimmungen des ISG können entsprechend auch nicht unter den Vorbehalt nach Artikel 4 BGÖ für Spezialbestimmungen, die bestimmte Informationen als geheim bezeichnen, fallen. Für alle Behörden, die dem BGÖ unterstehen, finden die Bestimmungen des BGÖ über den Zugang zu amtlichen Dokumenten auch auf Informationen Anwendung, die nach dem ISG klassifiziert worden sind. Die Beurteilung von Dokumenten im Verfahren nach dem BGÖ erfolgt unabhängig von den Regelungen des ISG. Bei Gesuchen um Zugang zu amtlichen Dokumenten überprüft die zuständige Stelle also unabhängig von einem allfälligen Klassifizierungsvermerk, ob der Zugang zu gewähren, zu beschränken, aufzuschieben oder zu verweigern ist. Die Klassifizierung kann bei der Beurteilung von Dokumenten nach dem BGÖ jedoch als Indiz für die Nichtöffentlichkeit des entsprechenden Dokuments gewertet werden. Der Entscheid zur Klassifizierung setzt nämlich eine Beurteilung des Schutzbedarfs der Information hinsichtlich einer Beeinträchtigung der zu schützenden öffentlichen Interessen nach dem ISG voraus, die materiell einer Beurteilung über die Einschränkung, Aufschiebung oder Verweigerung des Zugangs nach Artikel 7 Absatz 1 BGÖ entsprechen muss.

Die mit dem ISG zu schützenden Interessen stimmen zwar nicht vollständig mit dem Ausnahmekatalog nach Artikel 7 BGÖ überein. Das ISG konzentriert sich nämlich nicht nur auf den Schutz der Vertraulichkeit, sondern schützt auch die Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen. Die Bestimmungen über die Klassifizierung sind jedoch inhaltlich so gestaltet, dass sie dem Ausnahmekatalog inhaltlich nicht widersprechen. Im Übrigen ist darauf hinzuweisen, dass der persönliche Geltungsbereich des ISG weiter als jener des BGÖ gefasst wird, indem er für sämtliche Bundesbehörden anwendbar sein soll.

Verhältnis zur Datenschutzgesetzgebung

Die Datenschutzgesetzgebung regelt für private Personen sowie Bundesorgane den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden (Art. 1 DSG). Sie legt unter anderem fest, dass Personendaten nur rechtmässig, verhältnismässig, zweckmässig und für die betroffenen Personen möglichst transparent bearbeitet werden dürfen (Art. 4 DSG). Es versteht sich, dass Personendaten im Aufgabenbereich der Bundesbehörden weiterhin nach den Regeln der Datenschutzgesetzgebung bearbeitet werden müssen. Diese gilt also im Verhältnis zum ISG als Spezialgesetzgebung. Die Datenschutzgesetzgebung setzt aber auch Anforderungen an den praktischen Schutz der Vertraulichkeit, Verfügbarkeit und Integrität der Daten selbst. So verlangt Artikel 7 DSG, dass Personendaten durch angemessene technische und organisatorische Massnahmen vor unbefugter Bearbeitung geschützt werden. Der Bundesrat hat insbesondere in den Artikeln 8–11 VDSG Anforderungen an den Schutz von Personendaten festgelegt. Diese verlangen unter anderem, dass die technischen und organisatorischen Massnahmen dem gegenwertigen Stand der Technik Rechnung tragen. Es wird jedoch nicht bestimmt, was dieser Stand der Technik ist oder wer dafür zuständig ist, ihn umzuschreiben.

Die Vorschriften des ISG sollen auf die Bearbeitung von Personendaten als ergänzendes Recht angewendet werden. Personendaten gelten nämlich im Sinne des ISG als Informationen, welche die Bundesbehörden hinsichtlich Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit schützen müssen. In der Regel werden Personendaten nicht formell klassifiziert. Diese Klassifizierung ist für eng gefasste öffentliche Interessen des Bundes vorbehalten. Die Ausführungsbestimmungen werden allerdings Informationen und Daten je nach Schutzbedarf ein bestimmtes *Schutzniveau* in Bezug auf die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit zuweisen. Die Standardisierung der Massnahmen nach dem Stand von Wissenschaft und Technik, die mit den jeweiligen Schutzniveaus verknüpft wird, wird auch dazu dienen, die Anforderungen der Datenschutzgesetzgebung an die Datensicherheit zu erfüllen, und somit den Datenschutz beim Bund erhöhen.

1.2.4 Allgemeine Massnahmen

Grundsätze der Informationssicherheit

Informationssicherheit ist Chefsache. Die Verantwortung dafür liegt bei der Behördenleitung. Der Entwurf legt entsprechend bestimmte Pflichten fest, die nur von den jeweiligen Bundesbehörden erfüllt werden dürfen. So werden die obersten Behörden die Informationssicherheit nach dem Stand von Wissenschaft und Technik organisieren, umsetzen und überprüfen müssen. Dazu gehören die Bestimmung des zu erreichenden Sicherheitsniveaus sowie eine Regelung der Kompetenz für den Umgang mit Risiken. Weiter verstärkt der Entwurf die operationelle Rolle des obersten Managements in verschiedenen Bereichen wie der Sicherheit beim Einsatz von Informatikmitteln oder den PSP.

Informationen und Informationssysteme können heute nicht mehr vor allen Gefahren und Bedrohungen gleich geschützt werden. Die Priorität muss auf die wichtigsten, kritischsten Werte gesetzt werden. Diese Ausgangslage erfordert von den Bundes-

behörden, dass sie den Fokus vermehrt auf die systematische Bewertung des Schutzbedarfs von Informationen sowie auf eine laufende Beurteilung der entsprechenden Risiken setzen. Dies wiederum setzt ein wirksames Risikomanagement im Bereich der Informationssicherheit sowie eine regelmässige Überprüfung der Umsetzung, Wirksamkeit und Wirtschaftlichkeit von risikomindernden Massnahmen voraus. Beides fehlt heute weitgehend. Das Auditwesen stellt heute eine der wesentlichsten Schwächen im Bereich der Informationssicherheit des Bundes dar: Es wird nur in Einzelfällen oder erst nach einem Vorfall überprüft. Nur mit angemessenen Audits können Behörden und Organisationen allerdings wissen, in welchem Zustand sich ihre Informationssicherheit befindet, welche Risiken bestehen und welche Korrekturmassnahmen allenfalls erforderlich sind. Da zurzeit fast keine Audits durchgeführt werden, fehlen grösstenteils das entsprechende Knowhow und die personellen Mittel. Es muss deshalb davon ausgegangen werden, dass die verpflichteten Behörden für die Erfüllung dieser Aufgabe nicht darum herumkommen werden, zusätzliche Ressourcen einzusetzen (s. auch Ziff. 1.1.4: Bericht der GPDel über die Informatiksicherheit beim NDB, Empfehlung 9).

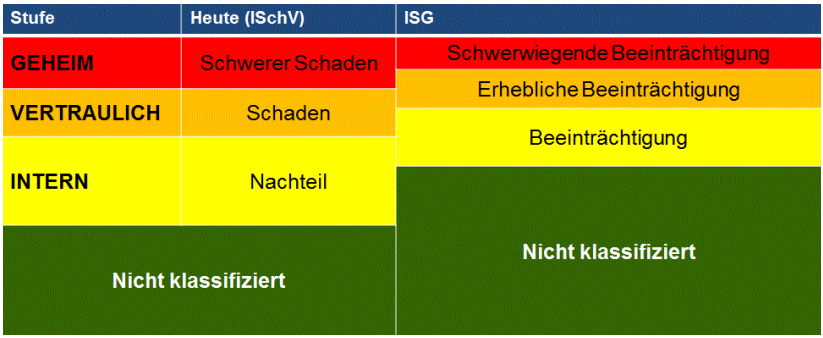
Klassifizierung von Informationen

Die Klassifizierung ist eine seit je angewandte Massnahme zum Schutz von organisationseigenen Informationen, deren unberechtigte Kenntnisnahme die Organisationsziele beeinträchtigen oder der Organisation selbst Schaden zufügen kann. Obschon sie massgebend für die Durchführung von PSP ist, ist heute jede verpflichtete Behörde grundsätzlich frei, ihr eigenes Klassifizierungssystem (wenn überhaupt), ihre eigenen Klassifizierungsgründe sowie ihre eigenen Bearbeitungsvorschriften festzulegen. Einige Vorfälle in den letzten Jahren haben gezeigt, dass diese unterschiedliche Behandlung klassifizierter Informationen zu erhöhtem Misstrauen führen kann. Eines der Regelungsziele ist also ein Klassifizierungssystem, das behördenübergreifend gelten und nach möglichst einheitlichen Grundsätzen umgesetzt werden soll. Das vorgeschlagene dreistufige System erlaubt einen risikogerechten Schutz von Informationen. Damit soll auch im internationalen Verhältnis ein einheitliches Sicherheitsniveau erreicht werden. Mit einem Vorbehalt für das Verfahrensrecht wird sichergestellt, dass die Klassifizierung kein Hindernis für die Bundesversammlung, die Gerichte und die Staatsanwaltschaften darstellt.

Bei der Gestaltung des Klassifizierungssystems wurden die erhöhten Erwartungen der Bürgerinnen und Bürger an die Transparenz des Handelns der Bundesbehörden berücksichtigt. Die Klassifizierung soll deshalb als eine zu begründende Ausnahme zum Grundsatz der Öffentlichkeit konzipiert werden, wobei das BGÖ für die davon betroffenen Behörden und Organisationen weiterhin auch für klassifizierte Informationen uneingeschränkt gelten soll. Zudem sollen gegenüber heute die Schwellenwerte für die Klassifizierung erhöht werden, sodass weniger und zielgerichteter klassifiziert wird (s. Abb. 1).

Abbildung 1

Erhöhung der Schwellenwerte für die Klassifizierung mit dem ISG



Sicherheit beim Einsatz von Informatikmitteln

Aufgrund der zunehmenden Vernetzung der Systeme sowie der zunehmenden Abhängigkeit der Bundesbehörden von diesen Mitteln zur Erfüllung ihrer gesetzlichen Aufgaben hat die Sicherheit der Informatikmittel seit einigen Jahren stark an Bedeutung gewonnen. Zahlreiche Vorfälle weltweit und in der Schweiz belegen die Verwundbarkeit der Informatikmittel und zeigen die potenziellen Konsequenzen solcher Vorfälle. Die Festlegung bestimmter Eckwerte der Informatiksicherheit auf der formell-gesetzlichen Ebene ist heute insbesondere deshalb unerlässlich, weil die behördenübergreifende Vernetzung und der elektronische Informationsaustausch weiterhin zunehmen werden. Deshalb müssen vermehrt behördenübergreifende Lösungen und Prozesse angestrebt werden. Zudem sind die Bestimmungen über die Sicherheitseinstufung der Informatikmittel neu auch massgebend für die Durchführung von PSP und BSV. Die meisten konkreten Massnahmen müssen aber aufgrund der raschen technologischen Entwicklung weiterhin auf Verordnungs- oder Weisungsstufe umschrieben werden.

Die Sicherheit beim Einsatz von Informatikmitteln wird oft als technische Angelegenheit betrachtet. Dies trifft nur am Rande zu: Die überwiegende Mehrheit der Sicherheitsvorkehrungen im Informatikbereich sind organisatorischer Natur. Dafür sind hauptsächlich die Behörden und Organisationen zuständig, die den Einsatz von Informatikmitteln beschliessen (Leistungsbezügerinnen), und nicht die Organisationen, die im Auftrag dieser Behörden und Organisationen die entsprechenden Mittel betreiben (Leistungserbringerinnen). Es ist also der organisatorische Bereich, der den grössten Handlungsbedarf aufweist.

Das ISG basiert auf bestehenden Prozessen und Verfahren, die entsprechend dem erkannten Bedarf angepasst werden. Es verfolgt dabei drei Hauptziele:

– *Ein möglichst einheitliches behördenübergreifendes Sicherheitsniveau erreichen:* Die Vorlage selbst legt fast keine detaillierten Sicherheitsmassnahmen fest, sondern verlangt von den verpflichteten Behörden, dass sie die erforderlichen Prozesse, Zuständigkeiten und Massnahmen festlegen. Obschon

die einzelnen verpflichteten Behörden für den Vollzug zuständig sind, setzt das Gesetz voraus, dass sie diese Prozesse, Zuständigkeiten und Massnahmen gemeinsam und möglichst einheitlich regeln werden.

– *Die Zuständigkeiten und Verantwortlichkeiten zwischen den Leistungsbezügerinnen und den Leistungserbringerinnen klar festlegen:* Die Hauptverantwortung für die Sicherheit beim Einsatz von Informatikmitteln liegt bei den Leistungsbezügerinnen. Sie sind für die Beurteilung des Bedarfs an Informationssicherheit und die Festlegung der erforderlichen Massnahmen zuständig. Die Leistungserbringerinnen sind hingegen dafür zuständig, die Sicherheit der Informatikmittel beim Betrieb zu gewährleisten. Sie müssen die Anforderungen und Massnahmen nach diesem Gesetz sowie die vereinbarten zusätzlichen Anforderungen der Leistungsbezügerinnen berücksichtigen und umsetzen.
– *Den Fokus auf die kritischsten Informatikmittel setzen:* Die Vorlage verlangt eine Sicherheitseinstufung der einzusetzenden Informatikmittel in Bezug auf die Informationen, die damit bearbeitet werden sollen, sowie auf die Aufgabenerfüllung der betroffenen Behörde oder Organisation. Die Sicherheitseinstufung eines Informatikmittels dient einerseits dazu, dass die Behörden die Kritikalität ihrer Informationen und Informatikmittel beurteilen und in der Folge bei der Festlegung der Sicherheitsmassnahmen den Fokus auf ihre kritischsten Werte legen. Andererseits sollen für jede Sicherheitsstufe standardisierte minimale Sicherheitsanforderungen und -massnahmen bestimmt werden, die vor der Inbetriebnahme des Informatikmittels umgesetzt werden sollen.

Personelle und physische Schutzmassnahmen

Die Mitarbeitenden sowie beauftragte Dritte sind für die Einhaltung der Vorschriften beim Umgang mit Informationen und Informatikmitteln verantwortlich. Die Wahrnehmung dieser Verantwortung setzt eine angemessene und stufengerechte Ausbildung voraus. In diesem Bereich ist der Handlungsbedarf besonders gross. Es wurde beispielsweise festgestellt, dass sehr viele Personen, die einer PSP unterzogen wurden, nie in der Handhabung von klassifizierten Informationen geschult wurden. Entscheidend für die Wahrung der Informationssicherheit ist zudem, dass Personen nur über diejenigen Berechtigungen für die Bearbeitung von und den Zugriff auf Informationen sowie für den Zugang zu Räumlichkeiten und Bereichen verfügen, die sie tatsächlich für die Erfüllung ihrer Aufgaben benötigen. Dieser Grundsatz wird zurzeit nicht überall eingesetzt, umgesetzt und überprüft. Das ISG legt deshalb beide Grundsätze als minimale personelle Anforderungen fest. Mit der zunehmenden Digitalisierung der Aufgabenerfüllung sind auch neue Methoden erforderlich, um die Identität von Personen zu verifizieren (Authentisierung), die Zugang zu Informationen oder Informationssystemen des Bundes verlangen. Mit dem ISG dürfen die Behörden biometrische Verifikationsmethoden dafür verwenden.

Eingangskontrollen und sonstige physische Schutzmassnahmen sind wirksame Massahmen der Informationssicherheit. Das ISG legt in diesem Bereich die minimale Anforderung fest, diesen Schutz zu regeln. Es schafft zudem eine Grundlage für die Einrichtung von sogenannten Sicherheitszonen. Dabei handelt es sich um

Räumlichkeiten und Bereiche, die besonders geschützt werden, weil in ihnen häufig klassifizierte Informationen der Stufe «vertraulich» oder «geheim» bearbeitet oder Informatikmittel der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz» betrieben werden. In der Praxis werden solche Sicherheitszonen hauptsächlich für Server-, Führungs- oder Sicherheitsräume errichtet. Solche Sicherheitszonen sind international üblich, beim Bund aber kaum bekannt. Eine formell-gesetzliche Grundlage ist erforderlich, weil Sicherheitszonen mit Massnahmen verbunden werden sind, die einen schweren Eingriff in die Persönlichkeitsrechte darstellen können (z. B. Videoüberwachung, Durchführung von PSP oder BSV).

Identitätsverwaltungs-Systeme

Eine der wirksamsten operativen Massnahmen zur Gewährleistung der Informationssicherheit ist eine wirksame Verwaltung und Kontrolle von Identitäten und Zugriffen. Mit dem stets wachsenden Umfang der Nutzung von Informationen aus unterschiedlichen Quellen und über die Organisationsgrenzen hinweg können die Anforderungen an Schutz und Funktionalität nur noch mit übergreifend koordinierten Systemen effizient gewährleistet werden. Ein solches System wird für die Bundesverwaltung im Rahmen des Programms IAM Bund eingeführt. An sich haben der Bundesrat und die anderen Bundesbehörden ohne Weiteres die Kompetenz, solche Identitätsverwaltungs-Systeme (auch IAM-Systeme genannt) einzuführen. Gewisse Aspekte der Bearbeitung von Personendaten bedürfen aber aus Datenschutzgründen einer formell-gesetzlichen Regelung. Das Gesetz legt den Zweck, die Architektur und die Funktionsweise der Identitätsverwaltungs-Systeme fest, um darauf basierend die Kompetenzen und die Einschränkungen bei der Bearbeitung von Personendaten zu regeln. Die Ausführungsbestimmungen werden unter anderem die Rechte und Pflichten der verschiedenen Beteiligten, die Anforderungen an den Datenschutz und die Datensicherheit, eine detaillierte Aufstellung der zu bearbeitenden Daten sowie die Weitergabe von Daten regeln.

1.2.5 Personensicherheitsprüfungen

Die formell-gesetzlichen Grundlagen für die Durchführung von PSP befinden sich heute in zwei Gesetzen. Für den Bund sind sie im BWIS geregelt. Für das Personal der Betreiberinnen von Kernkraftwerken sieht Artikel 24 KEG Zuverlässigkeitskontrollen vor. Obschon Artikel 113 Absatz 1 Buchstabe d MG ebenfalls eine PSP vorsieht, handelt es sich bei dieser Prüfung nicht um eine PSP im Sinne des BWIS, sondern um eine Beurteilung des Gewaltpotenzials im Hinblick auf die Überlassung der persönlichen Armeewaffe. Mit dem NDG wird das BWIS fast vollständig aufgehoben. Übrig werden nur noch die PSP sowie diejenigen Aufgaben bleiben, für deren Erfüllung das Fedpol zuständig ist. Da die heutige Regelung der PSP im BWIS *fast ausschliesslich* dem Schutz von Informationen dient (s. Art. 19 Abs. 1 BWIS), ist es zweckmässig, diese Regelung in das ISG zu verschieben. Der Bundesrat will diesen Transfer nutzen, um grundlegende Anpassungen am formell-gesetzlichen Rahmen der PSP vorzunehmen. Er will dabei auch präzisieren, welchen Zweck er mit der PSP verfolgt und entsprechend die PSP straffen.

Zweck der PSP

In jüngster Zeit ist die PSP immer wieder in die Kritik geraten. Regelmässig wurde die Überprüfung von Personen veranlasst, die keine besonders sensitiven Aufgaben des Bundes erfüllten (z. B. Reinigungspersonal). In einigen solchen Fällen wurde der Erlass einer Risikoverfügung als unverhältnismässig erklärt (s. Urteil des Bundesverwaltungsgerichts A-6797/2013; s. auch Interpellation 14.3085 vom 12. März 2014 und Postulat 14.4076 vom 4. Dez. 2014: Risikomanagement beim Personal der Bundesverwaltung). Es wurde ferner bemängelt, dass für bestimmte Funktionen, vor allem im Informatikbereich, keine Prüfungen durchgeführt wurden und dass externe und interne Mitarbeitende in ähnlichen Funktionen nicht gleich überprüft wurden (s. Ziff. 1.1.4: Bericht der GPK-S über externe Mitarbeitende der Bundesverwaltung; s. auch Motion 14.3031 vom 4. März 2014: FINMA. Sicherheitsüberprüfung der Führungskräfte vor ihrer Ernennung). Schliesslich werden immer wieder die zum Teil langen Prüffristen kritisiert. Angesichts dieser Lage empfahl die GPDel in ihrem Bericht über die Informatiksicherheit beim NDB dem Bundesrat (s. Ziff. 1.1.4), im Rahmen dieser Botschaft die Rollen, welche die PSP und die Personalführung im Bereich der Informationssicherheit spielen, ausführlich darzulegen und klar voneinander abzugrenzen. Gleichzeitig sollte er erläutern, wie viele personelle Ressourcen er für die PSP einsetzen will und welcher Beitrag an die Informationssicherheit damit geleistet werden soll.

Die PSP stellt eine vorbeugende Massnahme zum Schutz vor «Innentäterinnen» und «Innentätern» dar. Sie hat zum Ziel, das Risiko einer vorsätzlichen oder fahrlässigen Beeinträchtigung wesentlicher öffentlicher Interessen, das mit der Ausübung einer sicherheitsempfindlichen Tätigkeit durch eine bestimmte Person verbunden ist, zu identifizieren. Es liegt anschliessend allein in der Verantwortung der auftraggebenden bzw. anstellenden Behörde oder Organisation, zu entscheiden, ob sie ein allfälliges erhöhtes Risiko tragen will, ob sie es mit bestimmten Auflagen reduzieren will oder ob sie es durch Nichtanstellung oder Kündigung vermeiden will. Die Beurteilung, ob einer Person Vertrauen entgegengebracht werden kann, muss also nach wie vor in erster Linie durch die für die Auswahl verantwortlichen Personen im direkten Gespräch mit der Bewerberin oder dem Bewerber stattfinden, ergänzt durch bestimmte Bewerbungsunterlagen. Für die meisten Stellenbesetzungen, Übertragungen von militärischen Funktionen oder Beschäftigungen bei militärischen Aufträgen reichen die im direkten Auswahlverfahren erhobenen Daten aus; zudem entsteht bei Vertrauensmissbrauch in den meisten Fällen kein erheblicher Schaden für die öffentlichen Interessen nach diesem Gesetz. Muss jedoch mit einem solchen Schaden gerechnet werden, so kann eine PSP Risikofaktoren aufzeigen, die sich aus dem Vorleben oder dem Umfeld der geprüften Person ergeben. Auch eine Beurteilung des Sicherheitsrisikos durch die zuständige Fachstelle (Fachstelle PSP), die zu einer Sicherheitserklärung führt, entbindet die Linienvorgesetzten nicht von ihrer Führungsverantwortung und von ihrer Pflicht, Personalrisiken zu identifizieren und zu bewältigen. Die PSP hat deshalb eine ähnliche Ausprägung wie ein Assessment, das der Arbeitgeber vor der Anstellung einer Führungs- oder Schlüsselperson oft in Auftrag gibt.

Als staatliche Massnahme der Informationssicherheit muss die PSP risikogerecht und wirtschaftlich eingesetzt werden. Da sie zwangsläufig mit einem erheblichen

Eingriff in die Persönlichkeitsrechte der zu prüfenden Person verbunden ist, muss sie zudem hohen Anforderungen an die Verhältnismässigkeit genügen. Bei der Ausarbeitung der ersten Liste von Personen, die nach der per 1. Februar 1999 aufgehobenen Verordnung vom 15. April 1992[18] über die Sicherheitsprüfung in der Bundesverwaltung geprüft werden sollten, hatte sich der Bundesrat aus politischen Erwägungen entschieden, möglichst wenige Funktionen der Prüfung zu unterstellen. Er hatte für die Erstellung der Liste eine Planungsgrösse von 1200 Funktionen festgelegt. Seit dem Inkrafttreten des BWIS im Jahre 1998 ist die Anzahl jährlich geprüfter Personen jedoch stetig angewachsen. So werden seit 2012 jährlich zwischen 70 000 und 80 000 Prüfungen durchgeführt. Über 60 000 solcher PSP werden bei Stellungspflichtigen und Angehörigen der Armee durchgeführt, wobei diese Zahl auch die Beurteilungen des Gewaltpotenzials nach Artikel 113 MG einschliesst. Die Ressourcen der Fachstellen PSP mussten regelmässig erhöht werden. Trotzdem stieg die Anzahl pendenter Fälle stetig.

Der Bundesrat stellt angesichts dieser Entwicklung fest, dass die PSP heute nicht mehr risikogerecht und verhältnismässig eingesetzt wird. Sie darf nicht als Grundschutzmassnahme verstanden werden, die flächendeckend auf alle internen und externen Mitarbeitenden angewendet werden soll. Der mit der PSP verbundene Aufwand und der Eingriff in die Persönlichkeitsrechte lassen sich nämlich nur dann rechtfertigen, wenn die Funktion oder der Auftrag, für deren Ausübung eine PSP vorgesehen ist, tatsächlich die Möglichkeit einschliesst, wesentliche Interessen des Bundes erheblich zu beeinträchtigen. Der Bundesrat will deshalb den Einsatz der PSP auf das Mindestmass reduzieren, das zur Identifizierung und Bewältigung von erheblichen Risiken der Informationssicherheit erforderlich ist. Mit der beantragten Neuregelung soll eine deutliche Reduktion der Anzahl Funktionen, für deren Ausübung eine PSP erforderlich ist, erzielt werden.

Der Gesetzesentwurf sieht mehrere Massnahmen vor, die in ihrer Gesamtheit dazu beitragen werden, die Anzahl zu prüfender Funktionen zu reduzieren, zum Beispiel:

- Die Schwellenwerte für die Klassifizierungen «vertraulich» und «geheim» werden erhöht. Somit soll es auch inskünftig weniger Funktionen geben, für deren Ausübung die Bearbeitung von Informationen dieser Stufe erforderlich ist.
- Die Tätigkeiten, für welche die Prüfung erforderlich ist, werden klarer als im BWIS definiert. Die Prüfgründe werden mit dem Begriff der *sicherheitsempfindlichen Tätigkeit* auf die engen Bedürfnisse der Informationssicherheit reduziert. Bestimmte bisherige Prüfgründe werden ersatzlos gestrichen. Dies betrifft insbesondere den bisherigen Grund des regelmässigen Zugangs zu besonders schützenswerten Personendaten, deren Offenbarung die Persönlichkeitsrechte der Betroffenen schwerwiegend beeinträchtigen könnte (s. Art. 19 Abs. 1 Bst. e BWIS). Es ist in der Praxis kaum möglich, die Informationen zu bestimmen, die unter diesen Begriff fallen.
- Das ISG sorgt für eine mehrstufige Steuerung der PSP. Die Fachstelle des Bundes für Informationssicherheit wird bei der Ausarbeitung sowie bei der

[18] AS **1992** 1022

regelmässigen Überprüfung der Funktionslisten federführend sein. Damit soll sichergestellt werden, dass die Kriterien des Gesetzes restriktiv umgesetzt werden und deren Einhaltung entsprechend überprüft wird. Innerhalb der Bundesbehörden und der Departemente werden die Informationssicherheitsbeauftragten ebenfalls eine Steuerungsrolle wahrnehmen. Des Weiteren werden PSP-Vollzugsprobleme im Rahmen der Konferenz der Informationssicherheitsbeauftragten besprochen und wenn möglich einheitlich gelöst.

– Um die Schaffung eines Sicherheitsvakuums zu vermeiden, sollen schliesslich den Arbeitgebern andere, verhältnismässigere Mittel zur Verfügung gestellt werden, um ihren durchaus legitimen Sicherheitsbedürfnissen zu genügen. Sofern dies für die Wahrung ihrer Interessen erforderlich ist, sollen die Arbeitgeber von Stellenbewerberinnen und Stellenbewerbern sowie den Angestellten verlangen können, dass sie einen Auszug aus dem Strafregister und aus dem Betreibungsregister vorlegen. Es wird eine entsprechende Revision des BPG beantragt.

Behebung rechtlicher Mängel

Im Rahmen der Überarbeitung der Bestimmungen zu den PSP wurden zahlreiche Anpassungen am heutigen System vorgenommen mit dem Ziel, Mängel zu beheben. Die wichtigsten Änderungen werden nachfolgend aufgeführt:

– *erhöhte Regelungsdichte:* Das verfassungsmässige Prinzip der Legalität verlangt für schwere Eingriffe in die Persönlichkeitsrechte eine detaillierte formell-gesetzliche Grundlage. Die vorgeschlagene Regelung ist demnach detaillierter als im heutigen BWIS. Sie erfüllt damit auch die Erwartungen des Parlaments an eine formell-gesetzliche Definition des Sicherheitsrisikos (s. Ziff. 1.1.4).

– *Prüfungen nach der Spezialgesetzgebung:* Obschon die Regelung der PSP im BWIS fast ausschliesslich zum Schutz von Informationen im Bereich der inneren und äusseren Sicherheit dienen soll, wurden in der PSPV die Gründe für die Durchführung einer PSP über die Kriterien des BWIS hinaus erweitert. Nur wenige Amtsdirektorinnen und Amtsdirektoren der Bundesverwaltung erfüllen beispielsweise Aufgaben im Bereich der inneren oder äusseren Sicherheit oder haben einen regelmässigen Zugang zu «geheim» klassifizierten Informationen des Bundes. Sie müssen jedoch vor ihrer Wahl durch den Bundesrat einer erweiterten PSP mit Befragung, also der höchsten Prüfstufe nach der PSPV, unterzogen werden. Eine erweiterte PSP wird bei Personen durchgeführt, die anlässlich eines Auslandeinsatzes die Schweiz hoheitlich vertreten. Dass die Inhaberinnen und Inhabern solcher Funktionen hohe Ansprüche an die Vertrauenswürdigkeit erfüllen müssen, ist weitgehend nachvollziehbar. Es stellt sich jedoch die Frage, inwiefern diese Funktionen tatsächlich einen Zusammenhang mit der Wahrung der inneren Sicherheit im Sinne des BWIS haben.

  Der Bundesrat will Ordnung schaffen. Im ISG sollen nur Tätigkeiten mit klarem Bezug zur Informationssicherheit des Bundes die Durchführung einer PSP rechtfertigen. Entsprechend muss auch der Schaden, dessen Eintrittswahrscheinlichkeit es mit der PSP nach dem ISG zu vermeiden bzw.

reduzieren gilt, als Schaden für die Informationssicherheit verstanden werden. Die erhöhte Wahrscheinlichkeit eines Reputationsverlusts für den Bund wird demnach grundsätzlich kein Sicherheitsrisiko nach dem ISG zu begründen vermögen. Sofern für weitere Tätigkeiten eine Prüfung erforderlich ist, sollen die Prüfgründe in der Spezialgesetzgebung geregelt werden. Um zwischen der PSP nach dem ISG und nach den anderen Erlassen klar unterscheiden zu können, wird für letztere eine andere Terminologie (*Prüfung der Vertrauenswürdigkeit*) verwendet. Entsprechend wird im Anhang eine Änderung je des BPG und des MG vorgeschlagen. So sollen Personen, die regelmässig die Schweiz im Ausland vertreten oder Entscheidungskompetenzen bzw. Aufsichtsaufgaben in wesentlichen Finanzangelegenheiten erfüllen, einer Prüfung der Vertrauenswürdigkeit unterstellt werden können. Der Bundesrat wird die neuen Prüfungen sehr restriktiv anordnen.

– *Streichung des Kriteriums der Regelmässigkeit für die Unterstellung unter die PSP:* Das heutige Kriterium der Regelmässigkeit (s. Art. 19 Abs. 1 BWIS) basiert unter anderem auf einer Beurteilung des NDB, der die Gefährdung im Staatschutz insbesondere dort als hoch einschätzt, wo Mitarbeitende regelmässig und über einen längeren Zeitraum Zugang zu klassifizierten Informationen haben. Personen mit nur punktuellem und befristetem Zugang sind weniger stark gefährdet, weil sie für Stellen, die sich Informationen verschaffen wollen, weniger interessant sind. Mit dem Kriterium der Regelmässigkeit sind jedoch zwei Probleme verbunden. Nachrichtendienstliche Beschaffungsaktivitäten sind vorerst nur eine von vielen Bedrohungen für die Informationssicherheit. Bereits beim einmaligen Zugang zu einer «geheim» klassifizierten Information kann eine Person dem Bund schwerwiegenden Schaden zufügen. Dies kann beispielsweise der Fall sein, wenn diese Person Informationen über die Verhandlungsstrategie der Schweiz in besonders wichtigen Angelegenheiten der Öffentlichkeit preisgibt. Der Schaden selbst ergibt sich also vor allem aus dem Informationsinhalt. Des Weiteren ist der Begriff *regelmässig* selbst nicht eindeutig und hat oft zu uneinheitlichen Auslegungen geführt. Wichtiger für die Unterstellung der Bundesangestellten unter die PSP ist die Frage, ob die Inhaberin oder der Inhaber einer bestimmten Funktion zur Erfüllung ihrer oder seiner Aufgaben klassifizierte Informationen der Stufen «vertraulich» oder «geheim» bearbeiten *muss*, Informatikmittel der Stufe «hoher Schutz» oder «sehr hoher Schutz» verwalten, betreiben, warten oder überprüfen *muss* oder Zugang zu Sicherheitszonen haben *muss*. Wenn eine solche Tätigkeit für die funktionsbedingte Aufgabenerfüllung *erforderlich* ist, dann – und nur dann – muss die Funktion in die Liste der zu prüfenden Funktionen aufgenommen werden. Die verpflichteten Behörden und Organisationen müssen dafür sorgen, dass die Anzahl der Personen, die mit der Ausübung von sicherheitsempfindlichen Tätigkeiten beauftragt werden, auf das notwendige Minimum beschränkt wird.

– *Reduktion von drei auf zwei Prüfstufen:* Das heute geltende Recht (Art. 9–12 PSPV) sieht drei Prüfstufen vor: eine Grundsicherheitsprüfung, eine erweiterte PSP und eine erweiterte PSP mit Befragung. Während die beiden ersten Stufen nach PSPV einen nachvollziehbaren Prüfzweck haben, stellt sich die

Frage, welche Informationen oder Aktivitäten nach Schweizer Recht besser geschützt werden sollten als «geheim» klassifizierte Informationen. Für den Zugang zu letzteren ist bereits eine erweiterte PSP (Art. 11 PSPV) erforderlich. Der Bund kennt aber keine Klassifizierungsstufe «streng geheim», für welche die Prüfung nach Artikel 12 PSPV allenfalls erforderlich sein könnte. Deshalb werden im vorliegenden Gesetz die Prüfstufen von drei auf zwei reduziert. Um die Wirksamkeit der PSP zu erhöhen, wird die Datenerhebung innerhalb der zwei verbleibenden Prüfstufen reorganisiert und wo nötig ergänzt.

Zu Diskussionen Anlass gab auch das heutige System der durch Rechtssatz zu erlassenden Funktionenlisten, welches folgende Nachteile in sich birgt: Die Erstellung der Listen ist mit grossem Aufwand verbunden, sie sind unter den Departementen und mit der BK kaum harmonisiert und müssen zudem aufgrund von Organisationsänderungen und Umbenennungen der Funktionen ständig angepasst werden. Auch aus Sicherheitsgründen sind sie nicht unproblematisch: Sie liefern nämlich den Überblick über alle Funktionen von Behörden, die sicherheitsempfindliche Tätigkeiten beinhalten. Ihre Publikation macht sie weltweit jedermann zugänglich, auch fremden Nachrichtendiensten. Die Listen haben dennoch einen entscheidenden Vorteil gegenüber möglichen Varianten: Sie sorgen für Rechtssicherheit und schränken den zu prüfenden Personenkreis ein, sodass kein Wildwuchs an Prüfungen entstehen sollte. Vor dem Erlass seiner Ausführungsbestimmungen wird der Bundesrat allenfalls prüfen, ob die uneingeschränkte Veröffentlichung der Listen zweckmässig ist.

1.2.6 Betriebssicherheitsverfahren

Das BSV (bis anhin *Geheimschutzverfahren* genannt) befasst sich mit der Wahrung der Informationssicherheit bei der Vergabe von Aufträgen der Bundesbehörden an Dritte (nachfolgend *Betriebe* genannt), die nicht ihrer unmittelbaren Aufsicht unterstehen. Das Verfahren dient einerseits der Prüfung der Vertrauenswürdigkeit der zu beauftragenden Betriebe, andererseits ermöglicht es, die notwendigen Massnahmen zur Gewährleistung der Informationssicherheit während der Ausführung des Auftrags zu kontrollieren und durchzusetzen. Das BSV dient nicht der Produktsicherheit: Dafür ist selbstverständlich einzig die auftraggebende Stelle (Auftraggeberin) zuständig.

Mit dem BSV soll unter anderem verhindert werden, dass sicherheitsempfindliche Informationen oder praktische Angriffsvektoren auf kritische Informatikmittel des Bundes Betrieben zugänglich gemacht werden, die aufgrund ihrer Eigentums- und Rechtsverhältnisse, ihrer Organisationsstrukturen oder ihrer Geschäftsbeziehungen beispielsweise von ausländischen Nachrichtendiensten oder Organisationen mit kriminellem Hintergrund gesteuert oder massgebend beeinflusst werden (*Foreign Ownership, Control or Influence [FOCI]*). Die Prüfung der Vertrauenswürdigkeit von dienstleistenden Betrieben – und insbesondere der potenzielle Ausschluss aus dem Vergabeverfahren von Betrieben, die unter FOCI stehen – hat im Zusammenhang mit den Enthüllungen von Edward Snowden politische an Bedeutung gewon-

nen. Bestimmte Nachrichtendienste können nämlich die Informatikindustrie in ihrem Land gesetzlich oder auf repressivem Weg veranlassen, vertraglich vereinbarte oder gesetzlich vorgeschriebene Geheimhaltungspflichten nicht einzuhalten. Von Nachrichtendiensten verpflichtete Unternehmen solcher Länder können keine glaubhafte Garantie abgeben, dass sie den unter Landesrecht vereinbarten Geheimhaltungsverpflichtungen den Vorrang geben. Der Schaden, der durch so kontrollierte oder beeinflusste Betriebe verursacht werden kann, schränkt sich zudem nicht auf die Vertraulichkeit von Informationen ein. Gefahren bestehen zugleich für die Verfügbarkeit und Integrität von Informatikmitteln. Vor diesem Hintergrund schliessen Staaten mittlerweile vermehrt ausländische Anbieter für kritische staatliche Informatikleistungserbringungen aus. Es ist in diesem Zusammenhang deshalb wichtig zu präzisieren, dass für die Beurteilung des Sicherheitsrisikos immer die Sicherheitsempfindlichkeit des Auftrags sowie die konkreten Verhältnisse des zu prüfenden Betriebs massgebend sind. Das ISG vermag den pauschalen und wettbewerbsverzerrenden Ausschluss *a priori* von ausländischen Anbietern nicht zu begründen.

Das BSV ist zweckmässig und international üblich (s. etwa Art. 11 des Beschlusses des Rates vom 13. September 2013[19] über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (2013/488/EU) resp. Abschnitt VII der Regeln und Vorschriften der Europäischen Weltraumorganisation vom 15. Dezember 2011[20]. Im Verhältnis zum internationalen Beschaffungsrecht stellt das BSV kein Problem dar, weil die Ausnahmebestimmungen zum Übereinkommen vom 15. April 1994[21] über das öffentliche Beschaffungswesen solche beschaffungsrechtlichen Massnahmen zulassen (s. Art. XXIII). Es wird in der Schweiz für Aufträge des Bundes mit militärisch klassifiziertem Inhalt seit Ende der Siebzigerjahre durchgeführt. Aufgrund des begrenzten materiellen Geltungsbereichs der Geheimschutzverordnung werden zurzeit nur militärische klassifizierte Aufträge erfasst. Das Manko eines einheitlichen, d. h. auch für Aufträge aus dem zivilen Bereich durchzuführenden BSV wurde vom Bundesrat bereits vor längerer Zeit erkannt. Es führte einerseits dazu, dass für nicht-militärische klassifizierte Aufträge des Bundes jeweils spezielle Sicherheitsvorkehrungen getroffen werden mussten. Andererseits hinderte es Schweizer Unternehmen mehrfach daran, sich um die Teilnahme an nicht militärisch klassifizierten Projekten des Auslands zu bewerben. Als Beispiele können etwa die Herstellung von Ausweisen oder Zahlungsmitteln für Drittstaaten oder die Mitwirkung in wissenschaftlichen Projekten erwähnt werden. Darunter litt auch die Wettbewerbsfähigkeit der Schweizer Wirtschaft. Der Bundesrat will nun diese Lücke schliessen.

Das BSV läuft in groben Zügen wie folgt ab: Die Auftraggeberin stellt der Fachstelle für Betriebssicherheit (Fachstelle BS) Antrag zur Durchführung des BSV. Nach der Einleitung des Verfahrens legt die Fachstelle BS in Absprache mit der Auftraggeberin zunächst die Sicherheitsanforderungen fest. Hierauf prüft die Fachstelle BS die sicherheitsmässige Eignung der in Frage kommenden Firmen. Es soll insbesondere geprüft werden, ob die betroffenen Firmen von anderen Staaten kontrolliert

19 http://eur-lex.europa.eu/legal-content/de/TXT/PDF/?uri=CELEX:32013D0488
20 Das Reglement kann im Internet unter folgender Adresse abgerufen werden: www.esa.int > About us > Security at ESA > Regeln und Vorschriften der Europäischen Weltraumorganisation.
21 SR **0.632.231.422**

oder beeinflusst werden und gegebenenfalls ob diese Kontrolle oder der Einfluss mit der Informationssicherheit des Bundes vereinbart werden kann. Die Auftraggeberin vergibt anschliessend den Auftrag an eine Firma, die als geeignet beurteilt wurde. Unter der Aufsicht der Fachstelle BS legt der Betrieb alsdann in einem Sicherheitskonzept fest, wie er die Sicherheitsanforderungen umsetzen wird. Nachdem die erforderlichen Sicherheitsmassnahmen umgesetzt wurden, wird dem Betrieb die BSE ausgestellt. Sobald schliesslich nach der Durchführung der PSP auch die erforderlichen Sicherheitserklärungen vorliegen, darf die Auftraggeberin dem Betrieb die für die Erledigung des sicherheitsempfindlichen Auftrags erforderlichen Mittel (Informationen, Daten usw.) zur Verfügung stellen. Die BSE hat besondere Wirkungen sowohl für den Betrieb als auch für die Fachstelle BS. Letztere erhält insbesondere das Recht, den Betrieb unangemeldet zu inspizieren sowie weitere Massnahmen zu treffen.

Die Regelung steht zum Teil mit der PSP in relativ engem Zusammenhang, unterscheidet sich aber von dieser in wesentlichen Punkten. Zwar wird im Grundsatz ebenfalls eine Prüfung der Vertrauenswürdigkeit vorgenommen. Je nach dem Ergebnis wird dann eine BSE ausgestellt, welche die Vertrauenswürdigkeit des Betriebs bescheinigt und es ihm ermöglicht, sicherheitsempfindliche Tätigkeiten des Bundes (oder einer ausländischen Behörde) auszuüben. Anders als die PSP ist das Verfahren mit der Erteilung der BSE nicht abgeschlossen, sondern die Einhaltung der Massnahmen kann jederzeit überprüft werden. Im Gegensatz zur PSP ist beim BSV die Auftraggeberin an die Beurteilung der Fachstelle BS gebunden. Deshalb erlässt die Fachstelle BS auch eine anfechtbare Verfügung. Eine Ausnahme wird für den Fall eingeräumt, dass es für den Auftrag nur Betriebe in Frage kommen, die ein gewisses Risiko mit sich bringen. Dies betrifft vor allem Dienstleistungen im Informatikbereich, denn hier haben einige Firmen eine quasi monopolistische Marktstellung. Muss ein solcher Betrieb wegen mangelnder Alternative beauftragt werden, darf ihm keine schweizerische Sicherheitsbescheinigung ausgestellt werden. Entsprechend wird das BSV eingestellt und die Verantwortung für die Umsetzung und Überprüfung der Sicherheitsmassnahmen der Auftraggeberin übertragen. Diese verfügt von Gesetzes wegen über analoge Durchsetzungsrechte wie die Fachstelle BS.

Der Bundesrat will das BSV gezielt und möglichst unbürokratisch einsetzen. So sieht der Entwurf vor, dass auf die Durchführung eines BSV verzichtet werden kann, wenn das Risiko mit anderen Massnahmen hinreichend reduziert werden kann. Auf Verordnungsstufe wird der Bundesrat diesen Richtsatz konkretisieren.

1.2.7 Kritische Infrastrukturen

Der Bundesrat hat in der NCS am Grundsatz der dezentralen Regulierung der KI festgehalten (s. Ziff. 1.1.2). Soweit sektorspezifisch formell-gesetzlicher Handlungsbedarf besteht, muss die entsprechende Fachgesetzgebung angepasst werden. Die Prüfung des Regelungsbedarfs obliegt demnach grundsätzlich denjenigen Departementen, die im Rahmen ihrer Aufgabenerfüllung gegenüber KI-Betreiberinnen über Regulationsbefugnisse verfügen (z. B. dem UVEK für den Sektor der Energie-

versorgung). Es gibt demgegenüber auch bestimmte Aufgaben, die sektorübergreifend angegangen werden müssen und aus Effizienz- und Kostengründen nicht durch die dezentralen Regulatoren wahrgenommen werden können. Primär betroffen ist die Unterstützung der KI-Betreiberinnen durch den gegenseitigen Austausch von Informationen über Bedrohungen im Bereich der die, welche insbesondere der Früherkennung von Risiken und der Abwehr von Gefahren dient. In diesem Bereich hat sich in der Praxis gezeigt, dass von den KI-Betreiberinnen die Verbindung zu einer einheitlichen Ansprechstelle auf der Seite des Bundes ausdrücklich erwünscht ist. Diese Rolle einer zentralen Ansprechstelle wird heute von MELANI wahrgenommen.

MELANI wird nach den Beschlüssen des Bundesrates vom 29. Oktober 2003 und 24. Januar 2007 vom ISB und dem NDB, basierend auf ihren jeweiligen gesetzlichen Grundlagen, gemeinschaftlich betrieben. Die strategische Führung von MELANI und das technische Kompetenzzentrum sind im ISB angesiedelt; die Informationsdrehscheibe in Form des *Operation and Information Center* wird vom NDB betrieben. Es hat sich erwiesen, dass die im Rahmen von MELANI aufgebaute öffentlich-private Partnerschaft auch dank ihrem Zugang zu Informationen aus dem NDB sehr wirksam ist. Geschätzt wird neben den bereitgestellten Informationen insbesondere der Verbleib der Informationsherrschaft (an wen die Information weitergegeben werden darf) beim Informationslieferanten bezüglich ausgetauschten Informationen über Vorfälle. Positiv bewerten die KI-Betreiberinnen auch die Freiwilligkeit der Zusammenarbeit sowie den Ansatz, durch Informationen und gegebenenfalls Empfehlungen den Informationssicherungs- und Risikomanagementprozess zu unterstützen, statt Massnahmen vorzuschreiben.

Zur Erfüllung ihrer Aufgaben bearbeitet MELANI Adressierungselemente im Fernmeldebereich nach Artikel 3 Buchstabe f FMG (insb. Domainnamen, IP- und E-Mail-Adressen), die in Verbindung mit konkreten Gefährdungen oder Bedrohungen stehen, und tauscht diese mit den KI-Betreiberinnen aus. Infrastrukturen, die als kriminelle Tatmittel verwendet werden, bestehen nämlich häufig aus mit Schadsoftware infizierten Computern nichtsahnender Eigentümerinnen und Eigentümer, unter falschem Namen registrierten Domainnamen, unbefugt veränderten – eigentlich legitimen – Webseiten und Servern, die unter Verwendung einer fremden Identität gemietet werden. Mit den Informationen von MELANI können die KI-Betreiberinnen ihre Systeme schützen, indem sie beispielsweise Kommunikationsanfragen aus infizierten Computern blockieren. Weil sich Adressierungselemente auf bestimmte oder bestimmbare Personen beziehen (oder auf Geräte oder Fernmeldeanschlüsse, die wiederum einer bestimmten oder bestimmbaren Person zugeordnet werden können), können sie als Personendaten gelten. Sobald eine Strafanzeige erfolgt oder wenn Informationen im Rahmen von polizeilichen Ermittlungen anfallen, stehen diese Adressierungselemente im Zusammenhang mit strafrechtlichen Verfolgungen und können in der Folge als besonders schützenswerte Personendaten nach Artikel 3 Buchstabe c Ziffer 4 DSG gelten. Da jedoch mit einer Strafanzeige allein die Gefahr zumindest kurzfristig nicht gebannt wird, ist die Information der KI bezüglich dieser Angriffsvektoren essenziell, damit diese ihre Systeme schützen und allenfalls bereits erfolgte Angriffe erkennen können. Zur Bearbeitung solcher Informationen und Daten sowie zu deren Austausch mit den KI-Betreiberinnen benötigt MELANI

allerdings eine formell-gesetzliche Grundlage (s. Art. 17 Abs. 2 DSG), die heute fehlt.

Mit Beschluss vom 30. November 2011 hat der Bundesrat das VBS beauftragt, die für die Datenbearbeitung im Rahmen der Unterstützung der KI-Betreiberinnen durch den Bund nötige Grundlage in dieses Gesetz zu integrieren. Das ISG regelt die zentralen Aufgaben von MELANI zur Unterstützung der KI-Betreiberinnen. Es schafft weiter die erforderlichen formell-gesetzlichen Grundlagen für die Bearbeitung und den Austausch von Personendaten, soweit dies für die Gewährleistung der technischen Informationssicherheit von KI erforderlich ist. Dieser Informationsaustausch muss zwangsläufig auch mit den ausländischen und internationalen Partnern der Schweiz sichergestellt werden. Deshalb legt das ISG die Grundsätze und die nötigen Schranken für die internationale Zusammenarbeit fest. Diese Regelung ermöglicht beispielsweise den Austausch von Adressierungselementen mit dem deutschen *Bundesamt für Sicherheit in der Informationstechnik*, der französischen *Agence nationale de la sécurité des systèmes d'information* oder den *National Cyber Security Centers* in Holland und Finnland. Die Organisationseinheiten, die für den Schutz von kritischen (Informations-)Infrastrukturen zuständig sind, sind je nach Land verschieden aufgestellt: Sie sind typischerweise entweder eigenständig oder der Polizei, einem Nachrichtendienst, dem Militär oder dem Telekommunikationsregulator angegliedert.

Die Zusammenarbeit mit jeglichen Partnern im In- und Ausland basiert auf Freiwilligkeit und Transparenz. Die zuständigen Stellen können keine Zwangsmassnahmen anwenden und müssen sich bei jeder Anfrage um Informationen und Daten korrekt identifizieren sowie der potenziellen Datenlieferantin bekanntgeben, wofür die Daten benötigt und verwendet werden. Gleichwohl werden Daten unaufgefordert an Partnerorganisationen bekannt gegeben, wenn diese Daten geeignet sind, Vorfälle in ihrem Zuständigkeitsbereich zu erkennen oder zu beheben.

Auch wenn der NDB vom Bundesrat als für Aufgaben nach diesem Gesetz (mit-) zuständige Stelle bezeichnet wird, räumt das ISG dem NDB für seine anderen Aufgaben keine weitergehenden Datenbearbeitungsrechte ein, als ihm das NDG gewährt. Das ISG hat einen stark fokussierten Anwendungsbereich auf die technische Informationssicherheit und damit das bestimmungsgemässe Funktionieren von Informationsinfrastrukturen – mithin des Internets und daran angeschlossener Systeme. Diese Aufgaben sollen zukünftig von den zuständigen Stellen unabhängig von ihrer administrativen Zuordnung und allfälligen Rechtsgrundlagen ihrer Mutterorganisationen wahrgenommen werden können. Die Nutzung von Kenntnissen und Fähigkeiten im ISB und im NDB haben entscheidend zum bisherigen Erfolg von MELANI beigetragen, weshalb diese Kooperation weitergeführt werden soll. Im Rahmen der Ausführungserlasse wird der Austausch von Daten zwischen den verschiedenen Akteuren im Bereich der Informationssicherheit in transparenter Weise geregelt. Der Bundesrat sorgt zudem für eine periodische Kontrolle der Datenbearbeitung durch eine externe Stelle. Er kann die Datenbearbeitung im Anwendungsbereich des ISG, soweit sie im NDB vorgenommen wird, neben dessen Aufsichts- und Kontrollorganen also auch noch durch eine weitere Stelle überprüfen lassen.

1.2.8 Vollzug

Die Regelung des Vollzugs steht vor der Herausforderung, dass die Anwendung des Gesetzes nach möglichst einheitlichen Kriterien erfolgen soll. Kann ein einheitlicher Vollzug nicht erreicht werden, sind im behördenübergreifenden Informationsaustausch zwangsläufig Lücken bei der Informationssicherheit die Folge. Die Organisations- und Vollzugsautonomie der betroffenen Behörden muss aber gewahrt bleiben. Die verfassungsmässige Zuständigkeit der verschiedenen Behörden darf durch partielle behördenübergreifende Vollzugsvorgaben einer einzelnen Behörde (etwa des Bundesrats) nicht in Frage gestellt werden. Das ISG berücksichtigt diese an sich widersprüchlichen Anforderungen mit drei Mechanismen:

- *Eine «Opting-out»-Regelung:* Jede Behörde vollzieht in ihrem Bereich den Erlass selbständig und erlässt entsprechendes Ausführungsrecht. Das Vollzugsrecht des Bundesrats gilt jedoch für die übrigen Bundesbehörden sinngemäss, solange sie keine eigenen Regelungen erlassen.
- *Standards:* Der Bundesrat wird ermächtigt, standardisierte Anforderungen und Massnahmen nach dem Stand von Wissenschaft und Technik festzulegen, die für die anderen Bundesbehörden als Empfehlungen gelten. Dabei handelt es sich nicht um grundsätzliche Organisationsfragen, sondern um untergeordnete Prozesse, Mittel und Dienstleistungen (Erhebung des Schutzbedarfs von Informationen, Methoden für die Risikobeurteilung, Verschlüsselung usw.). Damit soll ein einheitliches Sicherheitsniveau erreicht werden, es sollen aber auch die Projekt- und Umsetzungskosten reduziert werden. Der Bundesrat soll die Möglichkeit haben, die Festlegung an kompetente Fachorgane zu delegieren.
- *Schaffung eines Koordinationsorgans:* Die Schaffung einer Konferenz der Informationssicherheitsbeauftragten, in welcher alle Bundesbehörden, die Kantone sowie der EDÖB vertreten werden, stellt eine zentrale Massnahme dar. Die für die fachliche Steuerung der Umsetzung des ISG zuständigen Informationssicherheitsbeauftragten werden umfassende Kenntnisse der Probleme der Informationssicherheit in ihrem Zuständigkeitsbereich, insbesondere bei der Umsetzbarkeit, Wirksamkeit und Wirtschaftlichkeit der Vorschriften sowie der beschlossenen Massnahmen erhalten. Die Konferenz wird dem einheitlichen, behördenübergreifenden und risikobasierten Vollzug sowie der Koordination mit den Kantonen und dem EDÖB dienen. Sie soll hierzu auch bei der Standardisierung von Anforderungen und Massnahmen massgebend mitwirken.

Mit der vorgeschlagenen Lösung wird die Unabhängigkeit der Bundesbehörden beim Vollzug bewahrt. Dieser erfolgt dezentral. Das angestrebte einheitliche Sicherheitsniveau wird durch einheitliche Doktrin, durch die Erarbeitung von Standards sowie durch die professionelle Unterstützung von Fachorganen erreicht.

Der Entwurf regelt hauptsächlich den behördenübergreifenden Rahmen. Für den Vollzug in der Bundesverwaltung ist der Bundesrat allein zuständig. Seine Vollzugsautonomie ist kaum eingeschränkt. Das Gesetz lässt ihm in Bezug auf die Organisation viel Spielraum. In diesem Zusammenhang wird er beschliessen, ob er am heutigen, grösstenteils dezentralisierten Vollzug festhalten oder ob er bestimmte

Kompetenzen und Zuständigkeiten zentralisieren will. Der Vollzug durch die dem Gesetz unterstellten Einheiten der dezentralen Bundesverwaltung und Organisationen des öffentlichen oder privaten Rechts, die Verwaltungsaufgaben erfüllen, wird sich aus dem Umfang ihrer Unterstellung und Autonomie ableiten lassen.

1.2.9 Organisation

Bei der Erarbeitung des Entwurfs wurde geprüft, ob und inwieweit die Zuständigkeiten und Verantwortlichkeiten im Bereich der Informationssicherheit den heutigen Anforderungen genügen. Dieser Prüfauftrag betrifft grundsätzlich nur die Bundesverwaltung. Seine Ergebnisse liefern aber wichtige Erkenntnisse, die für die Organisation der behördenübergreifenden Informationssicherheit ebenfalls gelten.

Heutige Organisation der Informationssicherheit in der Bundesverwaltung

In der Bundesverwaltung werden die Zuständigkeiten und Verantwortlichkeiten für den Schutz von Informationen je nach Art der Information (z. B. klassifizierte Informationen oder Personendaten) oder der Bearbeitung und Schutzmassnahmen (elektronisch oder physisch) durch verschiedene rechtliche Erlasse und Vorgabestellen geregelt. Der Bund betreibt in der Folge auch mehrere parallele Organisationen, die sich mit Haupt- oder Teilaufgaben der Informationssicherheit befassen (Informationsschutz, Datenschutz, Informatiksicherheit usw.).

Organisation des Informationsschutzes

Der Informationsschutz ist zur Hauptsache in der ISchV geregelt. Ergänzende Regelungen finden sich in den sogenannten Informationsschutzabkommen. Die ISchV gilt nur für die Bundesverwaltung und die Armee. Die Umsetzung des Informationsschutzes erfolgt dezentral und wird zentral durch Organe ohne Weisungsbefugnisse koordiniert. Für die detaillierten Vorgaben (Klassifizierungskatalog und Bearbeitungsvorschriften) ist die Generalsekretärenkonferenz zuständig. Die Bearbeitungsvorschriften enthalten auch Verhaltensvorschriften für den elektronischen Umgang mit klassifizierten Informationen sowie Anforderungen an die Sicherheit von Informatikmitteln. Die Departemente und die BK müssen je eine Informationsschutzbeauftragte oder einen Informationsschutzbeauftragten bezeichnen. Obschon die ISchV es nicht verlangt, haben alle Departemente auf Stufe Verwaltungseinheit weitere Informationsschutzberaterinnen und -berater bezeichnet. Ein Koordinationsausschuss sorgt für einen einheitlichen Vollzug beim Bund und erarbeitet die Vorlagen zuhanden der GSK. Er wird durch eine Koordinationsstelle unterstützt.

Organisation des Datenschutzes

Die Rechtsgrundlagen für die Bearbeitung von Personendaten finden sich in den jeweiligen Spezialgesetzen. Die Organisation des Datenschutzes beim Bund ist dagegen grundsätzlich im DSG und in der VDSG geregelt. Im Gegensatz zur ISchV gelten diese Erlasse auch für Private. Der Vollzug des Datenschutzes erfolgt dezentral. Er wird aber zentral durch den EDÖB überwacht und durch die Gruppe Datenschutz, ein informelles Organ ohne Weisungsbefugnisse, koordiniert. Die Departemente und die BK müssen je eine Datenschutzberaterin oder einen Datenschutz-

berater bezeichnen. Obschon dazu nicht verpflichtet, haben alle Departemente auf Stufe Verwaltungseinheit weitere Datenschutzberaterinnen und -berater bezeichnet.

Organisation der Informatiksicherheit

Die Organisation der Informatiksicherheit ist hauptsächlich in der BinfV geregelt, wobei zahlreiche andere Erlasse Einfluss auf die entsprechenden Zuständigkeiten und Verantwortlichkeiten haben (ISchV, ISA, VDSG, GEVER-Verordnung usw.). Der Bundesrat erlässt Weisungen über die Informatiksicherheit. Der Vollzug der Informatiksicherheit erfolgt dezentral. Die Departemente und die BK sind für die Umsetzung in ihrem Bereich selbst verantwortlich. Der Vollzug wird aber zentral durch ein Organ mit Weisungsbefugnissen (ISB) gesteuert. Das ISB entscheidet über Sonderregelungen bezüglich der Vergabe von sicherheitsrelevanten Rechten und Mandaten, insbesondere im Zusammenhang mit Firewalls, Zugriffsrechten und Privilegien. Bei Gefährdungen der Bundesverwaltung entscheidet es über spezifische Sicherheitsmassnahmen. Es klärt als Sachverständigenorgan im Auftrag eines Departements oder der BK vermutete oder erfolgte Sicherheitsvorfälle ab. Es stellt die Informatiksicherheitsbeauftragte oder den Informatiksicherheitsbeauftragten des Bundes.

Das ISB wird von zwei Konsultativorganen begleitet. Der Ausschuss Informatiksicherheit unterstützt das ISB als Konsultativorgan bei allen Informatiksicherheitsfragen und dient der überdepartementalen Koordination. Der Informatikrat des Bundes ist das Konsultativorgan des ISB zu Informatikgeschäften (inkl. Geschäfte mit Bezug zur Sicherheit), die der Absprache mit den Departementen und der BK bedürfen, insbesondere für den Erlass von Vorgaben und für die Genehmigung von Ausnahmen. Für den Vollzug müssen die Departemente, die BK und alle Verwaltungseinheiten je eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten bezeichnen, die oder der Koordinationsaufgaben erfüllt.

Neben dieser Grundorganisation gibt es viele Stellen, die sich ebenfalls mit Informatiksicherheit beim Bund befassen, namentlich die IOS beim Armeestab, das militärische CERT und der Bereich Informationssicherheit und Kryptologie bei der FUB, Wissenschaft und Technologie bei der Armasuisse (die Armasuisse ist die Beschaffungsstelle des Bundes für kryptologische Güter und Dienstleistungen), MELANI, der Sonderstab Informationssicherung sowie das CSIRT *(Computer Security Incident Response Team)* beim BIT. Die EFK nimmt die Informatikrevision in der Bundesverwaltung wahr.

Lücken und Schwachstellen im organisatorischen Bereich

Die heutige Organisation weist viele Lücken und Schwachstellen auf, zum Beispiel:

– Der Bund betreibt heute sowohl rechtlich als auch organisatorisch parallele Strukturen für Teilbereiche der Informationssicherheit. Die Abgrenzung der Zuständigkeiten ist dabei oft unklar. Die Schnittstellen werden ungenügend gepflegt. Dadurch leidet nicht nur die effektive Informationssicherheit: Auch die Koordination von politischen Geschäften mit Bezügen zur Informationssicherheit sowie die Zusammenarbeit mit den Kantonen und den internationalen Partnern werden erheblich erschwert.

- Es gibt zu viele Akteure, die nicht über genügend Fachwissen verfügen, weil sie die Informationssicherheit nur als Nebenaufgabe wahrnehmen können.
- Die heutigen Beauftragten verfügen zur Aufgabenerfüllung häufig über zu wenig Ressourcen. Die kritische Masse wird nirgends erreicht. In manchen Organisationen wären zwar insgesamt genügende Ressourcen vorhanden, diese werden aber schlecht genutzt, weil sie auf zahlreiche Personen verteilt sind.
- Die Sicherheitskosten werden mehrheitlich nicht transparent dargelegt, was eine Beurteilung der Wirtschaftlichkeit der Massnahmen verunmöglicht.
- Die Befugnisse der Spezialistinnen und Spezialisten sind ungenügend: Meistens nehmen sie nur Koordinationsaufgaben wahr und können deshalb weder Audits durchführen noch bei festgestellten Mängeln intervenieren. Die Fachkräfte, insbesondere im Informatikbereich, sind zudem oft einem Fachbereich unterstellt, dessen Risiken sie unabhängig beurteilen müssten, was zu Interessenkonflikten führt.
- Das Sicherheitsmanagement ist mangelhaft. Informationssicherheit wird als rein technische Angelegenheit betrachtet. Demzufolge finden die geschäftsüblichen Führungstätigkeiten (z. B. Zielsetzung, Umsetzungskontrolle oder Wirksamkeitsprüfung) im Sicherheitsbereich nur selten Anwendung. Die Linie muss auf allen Ebenen kompetenter beraten, unterstützt und ausgebildet werden.
- Das Sicherheitsbewusstsein ist ungenügend. Die Ausbildungsmassnahmen erreichen die Personen, die sicherheitsempfindliche Aufgaben erfüllen, häufig nicht. Sehr viele Personen werden zwar einer PSP unterzogen, aber in den Belangen der Informationssicherheit nicht entsprechend ausgebildet.

Die heutige Organisation wuchs aus sektoriellen gesetzlichen und materiellen Bedürfnissen. Sie lieferte lange Zeit genügend Resultate. Mit der Entwicklung zu einer Informationsgesellschaft wurden aber die Bedrohungen für Informationen und Informatikmittel komplexer und dynamischer. Ihnen muss integral und professionell begegnet werden, was entsprechende rechtliche und organisatorische Vorkehren sowie erhöhtes Fachwissen und -kompetenz voraussetzt. Es ist offensichtlich, dass die Organisation des Bundes diesen Anforderungen nicht genügt.

Die verschiedenen Fachorgane müssen soweit möglich zusammengeführt werden, um Synergien zu nutzen und Skaleneffekte zu erzielen. Mit der Zusammenführung können auch die Zuständigkeitsprobleme gelöst und das interdisziplinäre Fachwissen erhöht werden. Bei den verschiedenen Beauftragten kann durch zunehmende Professionalisierung eine Erhöhung der Kompetenzen erreicht werden. Die Professionalisierung würde verbessert, wenn die Managementaufgaben der Informationssicherheit auf möglichst wenige Funktionsinhaberinnen und -inhaber konzentriert würden.

Neuregelung der Organisation auf Stufe Bund

Der Entwurf liefert die Grundlage für eine Klärung und Vereinfachung der Zuständigkeiten und Verantwortlichkeiten. Er legt ein Schwergewicht auf die Kompetenzbildung der Stellen, die für den Vollzug zuständig sind, wobei die Kompetenzbil-

dung insbesondere durch die Unterstützung durch Sachverständige und einen verstärkten Informationsaustausch erfolgt. Der Entwurf sieht in der Folge eine einzige Beauftragtenrolle, ein einziges Koordinationsorgan sowie eine Fachstelle des Bundes vor, die alle Querschnittaufgaben der Informationssicherheit erfüllen sollen. Mit der Neuregelung sollen die Vollzugsstrukturen der bisherigen Bereiche des Informationsschutzes und der Informatiksicherheit zusammengelegt werden.

Informationssicherheitsbeauftragte

Die neue Rolle der beziehungsweise des Informationssicherheitsbeauftragten ist für den Vollzug zentral. Diese neue Funktion ist vor allem eine Managementfunktion. Die Informationssicherheitsbeauftragten werden sich nicht primär mit hochtechnischen Informationssicherheitsfragen befassen, sondern im Auftrag ihrer Behörde (oder der Departemente und der BK) die Informationssicherheit steuern sowie die Umsetzung der beschlossenen Massnahmen überprüfen. Schwergewichte werden sie auch auf das Risikomanagement sowie auf die Koordination mit anderen Bereichen legen müssen. Eine wirksame Aufgabenerfüllung durch die Informationssicherheitsbeauftragten setzt – neben einer klaren Unterstützung durch die Geschäftsleitung – eine enge Zusammenarbeit mit den Stellen voraus, die für das allgemeine Risikomanagement, den Datenschutz und die Sicherheit zuständig sind. Die Informationssicherheitsbeauftragten werden also als Drehscheibe zwischen der Geschäftsleitung und den Stellen, die für die Umsetzung der Massnahmen zuständig sind, agieren.

Bei den Departementen und der BK wird diese neue Funktion die bisher getrennten Rollen der Informationsschutzbeauftragten und der Informatiksicherheitsbeauftragten ersetzen. Der Bundesrat soll auf Verordnungsebene beschliessen, ob eine entsprechende Zusammenlegung der Funktionen auch auf Stufe der unterstellten Verwaltungseinheiten zweckmässig und erforderlich ist.

Konferenz der Informationssicherheitsbeauftragten

Aufgrund der verfassungsmässigen Unabhängigkeit der Behörden kann ein einheitliches Sicherheitsniveau nur erreicht werden, wenn in Bezug auf die Informationssicherheit trotz teilweise unterschiedlicher Bedürfnisse eine möglichst einheitliche Fachdoktrin herrscht. Aufgrund ihrer Stellung haben die Informationssicherheitsbeauftragten umfassende Kenntnisse der Situation und der Probleme der Informationssicherheit in ihrem Zuständigkeitsbereich, insbesondere in Bezug auf die Umsetzbarkeit und Wirksamkeit der Vorschriften und Massnahmen. Es bietet sich daher an, eine Konferenz dieser Beauftragten als Koordinationsorgan zu institutionalisieren.

Die Konferenz wird sich hauptsächlich mit der behördenübergreifenden Koordination des Vollzugs und mit der Beurteilung der vorgeschlagenen Standards beschäftigen. Sie wird dabei eine wichtige Rolle für die Bildung einer einheitlichen Doktrin spielen. In der Konferenz sind auch die Kantone und die oder der EDÖB vertreten. Für strategische Fragen soll die Konferenz Fachleute aus der Wissenschaft und der Wirtschaft beiziehen können. Sie wird für die Bundesverwaltung den heutigen Koordinationsausschuss für den Informationsschutz im Bund (ISchV) sowie den Ausschuss Informatiksicherheit (BinfV) ersetzen, wobei die technischen Angelegenheiten weiterhin in unterstellten Fachorganen behandelt werden sollen.

Fachstelle des Bundes für Informationssicherheit

Die Informationssicherheit muss nach einem integralen Ansatz organisiert, gesteuert und überprüft werden. Diverse Aufgaben nach diesem Gesetz, die bereits heute bestehen, werden von verschiedenen Fachorganen wahrgenommen. In der Folge werden sie nach einer sektoriellen Betrachtungsweise konzipiert und angegangen sowie kaum aufeinander abgestimmt. Eine verbesserte Koordination allein genügt nicht, um den integralen Ansatz zu verwirklichen. Deshalb soll eine zentrale Fachstelle als Kompetenzzentrum für die behördenübergreifenden Aufgaben geschaffen werden. Es kommen ihr keine Weisungsbefugnisse zu: Sie handelt grundsätzlich immer auf Antrag oder im Auftrag einer verpflichteten Behörde. Ihr Auftrag ist unterstützend und beratend zu verstehen.

Die konkreten behördenübergreifenden Aufgaben der Fachstelle werden abschliessend im Gesetz festgehalten. Nebst Beratung und Unterstützung kann die Fachstelle auf Antrag die Risiken beim Einsatz neuartiger Technologien beurteilen oder im Rahmen wichtiger behördenübergreifender Projekte die Belange der Informationssicherheit steuern und koordinieren. Eine weitere Kernaufgabe der Fachstelle soll (auf Antrag der verpflichteten Behörden) die Prüfung sicherheitsrelevanter Aspekte bestimmter Prozesse, Mittel und Dienstleistungen darstellen. Wird bestätigt, dass diese die Anforderungen des Bundes erfüllen, können sie standardisiert werden und somit auch von anderen Behörden oder Organisationen des Bundes eingesetzt werden (Aufwandreduktion). Die Fachstelle darf ferner auf Antrag Sicherheitskontrollen und -audits durchführen. Schliesslich soll sie als Ansprechstelle für Fachkontakte mit ausländischen und internationalen Stellen im Bereich der Informationssicherheit gelten. Diese Rolle ist für die Umsetzung völkerrechtlicher Verträge erforderlich (s. Ziff. 5.2).

Der Bundesrat soll auf Verordnungsebene die Organisation der Fachstelle regeln. Er soll festlegen, welche Aufgaben die Fachstelle selbst und welche sie in Zusammenarbeit mit anderen Bundesstellen erfüllen soll. Aktuell nehmen in der Bundesverwaltung viele Stellen Querschnittsaufgaben im Bereich der Informationssicherheit wahr, die zum Pflichtenheft der künftigen Fachstelle des Bundes gehören. Die Fachstelle soll beispielweise für die Bundesverwaltung bestimmte Aufgaben übernehmen, die heute durch den Bereich Sicherheit des ISB und die IOS wahrgenommen werden. Die Aufgaben bestehender Verwaltungseinheiten werden demzufolge auf Verordnungsebene neu definiert und bestimmte Schnittstellen überprüft werden müssen.

Neuregelung für die Bundesverwaltung

Nach dem oben Ausgeführten verfügt die Fachstelle des Bundes für Informationssicherheit im behördenübergreifenden Rahmen über keine rechtliche Durchsetzungskraft. Für die Bundesverwaltung kann der Bundesrat der Fachstelle hingegen weitere Kompetenzen erteilen sowie ihr Verhältnis zu den Linienvorgesetzten und zu den Informationssicherheitsbeauftragten differenziert gestalten. Obschon die Verantwortung für den Beschluss und die Umsetzung der Vorgaben bei der Führungsebene bleiben muss, hat sich im Rahmen der Gesetzgebungsarbeiten eine klare Mehrheit der Beteiligten für eine verstärkte Durchsetzungskompetenz der Fachstelle, insbesondere im Bereich der Audits, ausgesprochen. Die Organisation der Informationssicherheit bei den unterstellten Einheiten der dezentralen Bundesverwaltung sowie

bei den Organisationen nach Artikel 2 Absatz 4 RVOG wird der Bundesrat im Rahmen des Erlasses des Ausführungsrechts prüfen. Das ISG sieht allerdings vor, dass der Bundesrat diesen Organisationen genügend Autonomie gewährt.

1.3 Begründung und Bewertung der vorgeschlagenen Lösung

Die Gründe für die vorgeschlagene Regelung wurden ausführlich unter Ziffer 1.2 erläutert. Nachfolgend wird das Schwergewicht auf die jeweils geprüften Alternativen sowie auf die Vor- und Nachteile der gewählten Lösung gelegt.

1.3.1 Geprüfte Alternativen

Einheitserlass

Die Rechtsgrundlagen des Bundes für den Schutz von Informationen sind sehr sektoriell ausgeprägt, kaum aufeinander abgestimmt und oft lückenhaft. Sie sind zudem nicht auf die Bedürfnisse der Informationsgesellschaft ausgerichtet. Die sektorielle Ausprägung erschwert die Steuerung von politischen und operativen Geschäften, die einen Bezug zum Schutz von Informationen haben. Da die Zuständigkeiten je nach Fachgebiet geteilt sind, hat der erforderliche Koordinationsaufwand stark zugenommen. Deshalb sollen alle Massnahmen, die der Bund zum Schutz von Informationen treffen muss, in einem einzigen Erlass zusammengeführt werden. Dieser integrale Ansatz entspricht den internationalen Standards.

Geprüft wurde die Schaffung eines eigenständigen Gesetzes für die PSP und das BSV. Eine solche Lösung hätte den Vorteil, dass die allgemeinen Massnahmen der Informationssicherheit (zweites Kapitel) von der Anzahl Bestimmungen her mehr Gewicht erhalten würden. Sie wurde aber verworfen, weil sowohl die PSP als auch das BSV bereits heute Massnahmen der Informationssicherheit sind und die Durchführung von PSP und BSV von den Regelungen betreffend Klassifizierung, Einstufung von Informatikmitteln und Sicherheitszonen abhängt. Zudem müssten neue Zuständigkeiten und Verantwortlichkeiten definiert werden, was den Koordinationsaufwand sowohl rechtlich also auch organisatorisch erhöhen würde.

Geprüft wurde auch die Ergänzung bzw. Änderung bestehender Gesetze (RVOG, ParlG, MG, BPG usw.). Diese Lösung hätte den Vorteil, dass auf die Schaffung eines neuen Gesetzes verzichtet werden könnte. Sie hätte aber auch entscheidende Nachteile. Alle anzupassenden Gesetze verfügen über einen engen sektoriellen Geltungsbereich, was einen nach einem integralen Ansatz gesteuerten Vollzug praktisch verhindern würde. Die erkannten Lücken könnten somit – wenn überhaupt – nur mit einem unverhältnismässig grossen Koordinationsaufwand geschlossen werden. Eine solche Lösung würde faktisch auch die erforderliche behördenübergreifende Anwendung einheitlicher Kriterien und Massnahmen verhindern. Deshalb hat der Bundesrat diese Alternative bereits früh verworfen.

Die Informationssicherheit (einschliesslich der PSP und des BSV) hat einen sehr engen Zusammenhang mit dem Objektschutz. Diese Materie wird derzeit durch verschiedene gesetzliche Bestimmungen mit relativ unterschiedlicher Ausgestaltung und in unterschiedlicher Weise erfasst. Die Prüfung hat ergeben, dass eine gewisse Harmonisierung dieser Bestimmungen bzw. die Schaffung einer einheitlichen gesetzlichen Grundlage zwar wünschbar wäre, von der materiellen und organisatorischen Tragweite her aber den Rahmen des ISG sprengen würde. Die Vorlage enthält jedoch zwei Bestimmungen über physische Schutzmassnahmen.

Auf materiell-strafrechtliche Tatbestände wurde ebenfalls verzichtet. Die Bestimmungen im StGB und im MStG, die sich mit dem Schutz des Amtsgeheimnisses und dem Schutz klassifizierter oder schutzwürdiger Informationen des Bundes befassen, sollten nicht annexweise im Rahmen eines besonderen Organisationserlasses, sondern durch ein selbstständiges Gesetzgebungsprojekt revidiert werden.

Geltungsbereich

Materieller Geltungsbereich

Der Entwurf erfasst sämtliche Informationen und Daten und bezweckt, sie im Hinblick auf ihren Bedarf an Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit zu schützen. Der umfassende materielle Geltungsbereich entspricht dem Stand von Wissenschaft und Praxis. Eine Einschränkung auf sensitive Informationen wäre nicht sinnvoll. Die Beurteilung, ob eine Information sensitiv ist, setzt Beurteilungskriterien und -mechanismen voraus, die zwangsläufig auf alle Informationen anzuwenden sind. Zudem könnten die durch die beabsichtigte Standardisierung angestrebte Effizienzsteigerung und die erwünschten Synergien nicht erreicht werden.

Institutioneller Geltungsbereich

Die Gründe, weshalb alle Bundesbehörden vom Gesetz erfasst werden sollen, werden unter Ziffer 1.2.2 ausführlich erläutert. Eine Einschränkung auf die Bundesverwaltung und die Armee würde zwar eine wesentliche Kürzung des ISG bewirken, weil der Bundesrat alsdann allein für den Vollzug zuständig wäre. Sie würde aber die Lücken im behördenübergreifenden Rahmen bestehen lassen. Zudem könnten die anderen Bundesbehörden wichtige Fachressourcen der Bundesverwaltung (z. B. PSP oder BSV) nicht in Anspruch nehmen. Das Ziel, ein einheitliches Sicherheitsniveau zu gewährleisten, wäre nur mit einem erheblichen Verwaltungsaufwand zu erreichen. Aus diesen Gründen bewertet der Bundesrat den breiteren Geltungsbereich mit dezentralem Vollzug als die effizientere und wirtschaftlichere Lösung.

Klassifizierung

Der Bundesrat hat ein alternatives, zweistufiges Klassifizierungsmodell verworfen, weil das dreistufige Modell einerseits die Zusammenarbeit mit ausländischen und internationalen Partnern, die mehrheitlich ein vierstufiges System kennen, erleichtert, andererseits aber auch, weil es einen risikogerechteren Schutz der eigenen Informationen ermöglicht. Verworfen wurde ebenfalls die Klassifizierung von Personendaten sowie von Geschäfts- und Fabrikationsgeheimnissen, weil die Einstufungskriterien entweder durch die sektorielle Gesetzgebung (DSG) festgelegt wer-

den oder sie mit den Eigentümerinnen und Eigentümern der Informationen vereinbart werden müssen.

Geprüft wurde zudem, ob die Bearbeitung von «geheim» klassifizierten Informationen des Bundes grundsätzlich Schweizer Bürgerinnen und Bürgern vorbehalten sein sollte. Solche Einschränkungen sind im internationalen Verhältnis üblich. Weil die Bundesbehörden auch im Sicherheitsbereich auf ausländische Fachkräfte angewiesen sind, hat der Bundesrat darauf verzichtet.

Identitätsverwaltungs-Systeme

Geprüft wurde ein Verzicht auf die Verwendung der AHV-Versichertennummer. Der Bundesrat ist aber überzeugt, dass die vorgeschlagene Lösung wirtschaftlicher und einfacher ist und einen mindestens gleichwertigen Datenschutz gewährleistet.

PSP

Der Bundesrat ist der Auffassung, dass die vorgeschlagene Regelung die heutigen Bedürfnisse der Informationssicherheit besser abdeckt und gleichzeitig geeignet ist, die Durchführung von PSP deutlich zu reduzieren. Dadurch soll auch der entsprechende finanzielle und personelle Aufwand reduziert werden. Geprüft wurde auch, ob die Durchführung von PSP in der Schweiz nur noch für die Bearbeitung von «geheim» klassifizierten Informationen, für die Verwaltung und den Betrieb von Informatikmitteln mit sehr hohem Schutz und für den Zugang zu entsprechenden Sicherheitszonen zulässig sein sollte, wobei die Durchführung von PSP für den Zugang zu «vertraulich» klassifizierten Informationen des Auslands vorbehalten bleiben würde. Ein ähnlicher Ansatz würde auch für die Prüfungen der Vertrauenswürdigkeit nach BPG und MG gelten. Diese Lösung würde den Aufwand noch weiter reduzieren. Sie wurde aber verworfen, weil sie im internationalen Verhältnis eine Ausnahme darstellen und der beabsichtigten Harmonisierung im Bereich der internationalen Zusammenarbeit zuwiderlaufen würde.

BSV

Der Bundesrat ist der Ansicht, dass die neue Regelung es ermöglichen wird, das BSV gezielt und möglichst unbürokratisch einzusetzen. Der damit verbundene Aufwand soll auf ein Minimum beschränkt werden. Analog zur Regelung der PSP wurde geprüft, ob das BSV nur für die Bearbeitung von «geheim» klassifizierten Informationen, für die Verwaltung und den Betrieb von Informatikmitteln mit sehr hohem Schutz und für den Zugang zu entsprechenden Sicherheitszonen durchgeführt werden sollte, wobei es im internationalen Verhältnis breitere Anwendung finden würde. Diese Variante wurde aus den gleichen Gründen wie bei den PSP verworfen.

Ebenfalls geprüft wurde eine Regelung, wonach die Beurteilung der Fachstelle BS für die Auftraggeberin nicht verbindlich wäre. Dieses System entspräche der Regelung der PSP. Es hätte den Vorteil, die vollständige Verantwortung für die Auftragserteilung bei der Auftraggeberin zu belassen, die auch erhöhte Risiken in Kauf nehmen könnte. Diese Alternative wurde jedoch aus mehreren Gründen nicht berücksichtigt. Erstens gilt die BSE als staatliches «Sicherheitssiegel», das durch die nationale Sicherheitsbehörde erteilt werden muss. Die Wahrung der Integrität dieses Siegels kann nur dann sichergestellt werden, wenn der Entscheid über die Eignung

von Fachleuten getroffen wird. Zweitens hört das BSV im Gegensatz zur PSP nicht nach der Prüfung des Betriebs auf, sondern erstreckt sich auch auf die Kontrolle der Umsetzung der Massnahmen. Wäre die Auftraggeberin nicht an die Beurteilung gebunden, wären diese Kontrollbefugnisse sinnlos. Drittens kommt es in der Praxis nur selten vor, dass ein Betrieb als sicherheitsmässig problematisch beurteilt wird. Liegt ein solcher Ausnahmefall aber vor, muss sichergestellt werden, dass der Betrieb keinen heiklen Auftrag für den Bund ausübt.

Kritische Infrastrukturen

Die Gründe für den Verzicht auf zentrale Vorgaben und Meldepflichten für die KI im Bereich der Informationssicherheit werden in der NCS erläutert.

Vollzug

Der institutionelle Geltungsbereich darf die verfassungsmässige Unabhängigkeit der betroffenen Behörden nicht einschränken. Deshalb sollen die Bundesbehörden das Gesetz eigenständig vollziehen, wobei der Entwurf diverse Instrumente zur Sicherstellung einheitlicher Vorschriften und Massnahmen festlegt. Der eigenständige Vollzug hat einen Nachteil: Die minimalen organisatorischen Anforderungen, die von allen Bundesbehörden erfüllt werden sollen, müssen zwingend auf Gesetzesebene verankert werden. Demzufolge enthält die Vorlage auch diverse Bestimmungen, die von der Normenhierarchie her eher dem Verordnungsrecht entsprechen.

Geprüft wurde auch eine Delegation von behördenübergreifenden Rechtsetzungsbefugnissen an die Bundesversammlung (Parlamentsverordnung) oder an den Bundesrat. Mit einer solchen Delegation könnten zahlreiche Bestimmungen auf Verordnungsebene verankert werden. Der Entwurf wäre entsprechend schlanker. Im Rahmen der verschiedenen Konsultationen haben sich die betroffenen Bundesbehörden jedoch gegen jegliche Unterstellung unter das Vollzugsrecht einer anderen Behörde ausgesprochen. Aus demselben Grund wurde auf ein behördenübergreifendes Steuerungsorgan mit Weisungsbefugnissen verzichtet. Die dezentrale Vollzugslösung wahrt die verfassungsmässige Unabhängigkeit der verschiedenen Bundesbehörden. Sie erlaubt einen flexiblen, risikogerechten Vollzug nach den tatsächlichen Sicherheitsbedürfnissen der jeweiligen Behörden. Aus Sicht des Bundesrats überwiegen die Vorteile der vorgeschlagenen Lösung ihre Nachteile deutlich.

Organisation

Die vorgeschlagene Organisation erhöht die Professionalität im Bereich der Informationssicherheit, legt klare Zuständigkeiten fest und trägt dem dezentralen Vollzug Rechnung. Sie beruht im Allgemeinen auf bestehenden Strukturen und Organen, die teilweise zusammengeführt werden und Aufgaben erhalten, die an die Anforderungen einer Informationsgesellschaft angepasst werden. Ein Verzicht auf diese Organe, insbesondere auf die Fachstelle des Bundes für Informationssicherheit, würde den wirksamen einheitlichen Vollzug wesentlich erschweren. Die Behörden und Organisationen müssten zudem selber Fähigkeiten aufbauen (z. B. Kryptologie, technische Audits), die aus wirtschaftlichen Gründen eher zentral zur Verfügung stehen sollten.

1.3.2 Vernehmlassungsverfahren

Stellungnahmen im Vernehmlassungsverfahren

Am 26. März 2014 verabschiedete der Bundesrat den Vorentwurf zum Informationssicherheitsgesetz und eröffnete das Vernehmlassungsverfahren, welches bis zum 4. Juli 2014 dauerte. Zur Vernehmlassung eingeladen wurden 62 Adressaten. Insgesamt gingen beim VBS in der Folge 55 Antworten ein (Kantone: 26, Parteien: 4, Organisationen und weitere interessierte Kreise: 24).

Die überwiegende Mehrheit der Vernehmlassungsteilnehmer begrüsste grundsätzlich die Schaffung eines Informationssicherheitsgesetzes. Teilweise bestanden gewisse Vorbehalte gegenüber einzelnen Punkten des Entwurfs. Lediglich eine Partei (SVP) lehnte den Gesetzentwurf vollumfänglich ab. Ein Kanton und ein gesamtschweizerischer Dachverband der Wirtschaft könnten der Vorlage allenfalls nach einer substanziellen Überarbeitung bestimmter Regelungsaspekte beziehungsweise der begleitenden Unterlagen zustimmen.

Verbesserungsbedarf wurde insbesondere festgestellt bei:

- der Zusammenarbeit zwischen Bund und Kantonen;
- der Regelung bezüglich kritischer Infrastrukturen;
- den finanziellen Auswirkungen für Bund und Kantone.

Anpassung des Vernehmlassungsentwurfs

Am 5. November 2014 nahm der Bundesrat vom Ergebnisbericht[22] zum Vernehmlassungsverfahren Kenntnis und beauftragte das VBS mit der Ausarbeitung einer Botschaft.

Die wichtigsten Änderungen der Vernehmlassungsvorlage sind folgende:

- Die Regelung der Zusammenarbeit zwischen Bund und Kantonen wurde neu nach dem Modell der Datenschutzgesetzgebung konzipiert. Zudem sollen die Kantone bei der Ausarbeitung des Vollzugsrechts und der Standards eng mitwirken. Ferner sollen sie in der Konferenz der Informationssicherheitsbeauftragten vertreten sein und die Beratung und Unterstützung der Fachstelle des Bundes für Informationssicherheit in Anspruch nehmen können. Der Bundesrat soll schliesslich die Kantone ermächtigen können, die Leistungen der vom Entwurf vorgesehenen Fachstellen für ihre eigenen Bedürfnisse in Anspruch zu nehmen.
- Die Bestimmungen über die kritischen Infrastrukturen wurden überarbeitet. Dies betrifft insbesondere die Regelung über die Datenbearbeitung.
- Das ISG wurde mit einem Abschnitt über den Einsatz von Informationssystemen zur zentralen Verwaltung von Identitäten (IAM Bund) ergänzt.
- Der strafrechtliche Schutz vor Amtsgeheimnisverletzungen nach Artikel 320 StGB und vor Dienstgeheimnisverletzungen nach Artikel 77 MStG wurde

22 www.admin.ch > Bundesrecht > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2014 > VBS > Bundesgesetz über die Informationssicherheit

auf externe Hilfspersonen erweitert. Der Bundesrat ist aufgrund des heute unentbehrlichen Bezugs von externen Informatikdienstleistungen durch Bund und Kantone der Ansicht, dass diese Erweiterung rasch erfolgen soll.

– Einige Bestimmungen wurden so angepasst, dass die Handlungsfreiheit der verpflichteten Behörden und insbesondere des Bundesrats hinsichtlich Umsetzungskosten und Organisation bewahrt wird.

Zudem wurden zahlreiche Vereinfachungen vorgenommen. Viele Bemerkungen wurden über Ergänzungen oder Präzisierungen der Erläuterungen abgefangen.

1.3.3 Gesamthafte Beurteilung

Die Informationssicherheit hat in jüngster Zeit eindeutig stark an Bedeutung, auch aus politischer Sicht, gewonnen. Zahlreiche Vorfälle und internationale Entwicklungen haben gezeigt, wie verletzlich unsere Gesellschaft aufgrund der zunehmenden Abhängigkeit von der Informatik geworden ist. Dass der Bund sich vor den neuen Bedrohungen besser schützen muss, ist politisch unumstritten. Letztlich geht es dabei um die Sicherstellung grundlegender Aufgaben wie der Wahrung der inneren und äusseren Sicherheit, der wirtschafts-, finanz- und währungspolitischen Interessen der Schweiz sowie sie Sicherstellung der Entscheidungs- und Handlungsfähigkeit der Bundesbehörden. Der Bundesrat ist der Auffassung, dass er mit dieser Vorlage einen ausgewogenen und gleichzeitig zielgerichteten formell-gesetzlichen Rahmen für eine zeitgemässe Informationssicherheit beim Bund vorschlägt. Das haben die Ergebnisse der Vernehmlassung überwiegend bestätigt. Die wichtigsten Anliegen der Beteiligten, insbesondere jene der Kantone, wurden berücksichtigt.

1.4 Rechtsvergleich

Allgemeine Bemerkungen

Die meisten Nachbarstaaten der Schweiz sowie die internationalen Organisationen, mit welchen die Schweiz enge Beziehungen pflegt, überprüfen infolge der Entwicklungen in der Informatik ihre Sicherheitsvorschriften. Es ist nicht möglich, eine Übersicht über diese laufenden Arbeiten anzubieten. Zudem sind Regelungen im Sicherheitsbereich häufig nur schwer zugänglich. In einer thematischen Zusammenstellung werden die Regelwerke und Vorschriften einiger Länder aus dem europäischen Umfeld der Schweiz in ausgewählten Punkten der Informationssicherheit miteinander verglichen. Für den Rechtsvergleich wurden folgende Länder gewählt: Deutschland, Frankreich, Italien und Österreich, als direkte Nachbarn der Schweiz, sowie Grossbritannien, die Niederlanden und Schweden. Dabei wurden insbesondere folgende Punkte untersucht: Die Art der Regelung der Informationssicherheit und deren institutioneller Geltungsbereich, das Klassifizierungssystem, die PSP, das BSV und die behördliche Organisation.

Art der Regelung der Informationssicherheit

Deutschland regelt die Grundsätze der Informationssicherheit auf Gesetzesstufe mit ausführenden Verwaltungsvorschriften und Richtlinien. In Frankreich regeln verschiedene Erlasse auf Verfassungs-, Gesetzes- und Verordnungsstufe die Informationssicherheit. In Italien wird der Bereich Informationssicherheit in einem Gesetz, zwei Beschlüssen des Ministerpräsidenten und Weisungen der nationalen Sicherheitsbehörde geregelt. In den Niederlanden wird der Bereich Informationssicherheit in verschiedenen Erlassen unterschiedlichster Stufe geregelt. In Schweden sind Regeln für den Bereich Informationssicherheit in mehreren Gesetzen enthalten. Für den Bereich Industriesicherheit gibt es keine speziellen Erlasse. In Österreich existiert kein einheitliches Regelwerk, das die Informationssicherheit gesamthaft abdeckt. Das österreichische Informationssicherheitsgesetz regelt jedoch die Klassifizierung sowie die Durchführung von PSP. Auf Stufe Bundesland gelten lediglich Bestimmungen aus dem Beamtendienstrecht, beispielsweise die Amtsverschwiegenheit. In Grossbritannien existieren ebenfalls keine speziellen Gesetze betreffend Informationssicherheit. Verschiedene Erlasse bilden aber eine Basis. Die Leitlinien für die nationale Sicherheitspolitik werden im sogenannten *Security Policy Framework* statuiert, das die zwingenden Voraussetzungen festgelegt, welche die Verwaltung, die Regierung, die Behörden und die Auftraggeberinnen einzuhalten haben.

Die EU regelt den Schutz ihrer klassifizierten Informationen beinahe umfassend. Sowohl der Beschluss des Rates vom 13. September 2013[23] über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (2013/488/EU) als auch der Beschluss der Kommission vom 13. März 2015[24] über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (2015/444/EU, Euratom) regeln die Klassifizierungen, den personellen – einschliesslich PSP – und den materiellen Geheimschutz, die Informatiksicherheit und den Geheimschutz in der Industrie. Nennenswert für die technische Informationssicherheit ist auch die EU-Verordnung 526/2013 vom 21. Mai 2013[25] über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004.

Institutioneller Geltungsbereich

In Deutschland werden die Bundesbehörden und die bundesunmittelbaren Einrichtungen erfasst. Daneben gibt es Richtlinien für Firmen, die Verschlusssachen (VS) bearbeiten. In Frankreich gilt für alle Ministerien eine Regelung zum Informationsschutz, die aber von den einzelnen Ministerinnen und Ministern präzisiert werden kann. In Italien gelten die Vorgaben für die gesamte öffentlichen Hand, die Industrie und Einzelpersonen, die klassifizierte Informationen bearbeiten. Parlamentarierinnen und Parlamentarier, Ministerinnen und Minister sowie Richterinnen und Richter, die kraft ihres Amtes Zugang zu klassifizierten Informationen benötigen, werden nicht geprüft. In Österreich gelten die Regelungen ausschliesslich für die Dienststellen des Bundes. Die Industrie wird mit privatrechtlichen Vereinbarungen dazu verpflichtet, die Bestimmungen des Bundes anzuwenden. In Grossbritannien ist das Security Policy Framework auf alle Behördenstellen, Agenturen und Auftraggeber anwend-

23 http://eur-lex.europa.eu/legal-content/de/TXT/PDF/?uri=CELEX:32013D0488
24 http://eur-lex.europa.eu/legal-content/de/TXT/PDF/?uri=OJ:JOL_2015_072_R_0011
25 http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32013R0526

bar, die klassifizierte Aufträge bearbeiten. Gewisse Teile gelten auch für die Polizei. In den Niederlanden gilt der *Security Investigation Act* für alle Verwaltungseinheiten sowie die Industrie. Die Vorschriften zur Behandlung von klassifizierten Informationen und zur Informationssicherheit gelten nur für die Verwaltung. Die Regeln für die Industriesicherheit im Verteidigungsbereich gelten für die entsprechenden Firmen. In Schweden sind gewisse Erlasse auf alle Behörden anwendbar, andere für die Regierung, das Parlament aber nicht.

In der EU sind die Vorschriften zwar weitgehend harmonisiert, jedes unabhängige Organ erlässt seine Vorschriften aber selbst (Parlament, Rat und Kommission).

Klassifizierungssystem

Ein dreistufiges Klassifizierungssystem kennen Frankreich und Grossbritannien. Vier Stufen haben Deutschland, Italien, Österreich und die Niederlanden. Schweden hat im militärischen Bereich vier Stufen, bei den anderen Behörden nur zwei.

Für die EU gelten die vier nachfolgenden Klassifizierungsstufen:

- *TRÈS SECRET UE / EU TOP SECRET:* Die unbefugte Weitergabe könnte den wesentlichen Interessen der EU oder eines oder mehrerer Mitgliedstaaten äusserst schweren Schaden zufügen.
- *SECRET UE / EU SECRET:* Die unbefugte Weitergabe könnte den wesentlichen Interessen der EU oder eines oder mehrerer Mitgliedstaaten schweren Schaden zufügen.
- *CONFIDENTIEL UE / EU CONFIDENTIAL:* Die unbefugte Weitergabe könnte den wesentlichen Interessen der EU oder eines oder mehrerer Mitgliedstaaten Schaden zufügen.
- *RESTREINT UE / EU RESTRICTED:* Die unbefugte Weitergabe könnte für die Interessen der EU oder eines oder mehrerer Mitgliedstaaten nachteilig sein.

PSP

In Deutschland sind für eine PSP der zeitnahe und tatsächliche Zugang zu Verschlusssachen oder die Möglichkeit der Kenntnisnahme von klassifizierten Informationen erforderlich. Die Prüfung erfolgt durch das Bundesamt für Verfassungsschutz, dessen Beurteilung bindend ist. In Frankreich muss für eine PSP die Funktion der betroffenen Person in der Verwaltung oder in der Privatwirtschaft auf einer Funktionsliste aufgeführt sein. Die Sicherheitsermächtigung wird je nach Klassifizierungsstufe von einer bestimmten Behörde erteilt. Die Risikobeurteilung ist nicht bindend. In Italien müssen im Antrag zur PSP die Gründe, weshalb die Person Zugang zu klassifizierten Informationen benötigt sowie die Klassifizierungsstufe ausgewiesen werden. Die zu prüfende Person muss bestätigen, dass sie über Notwendigkeit der PSP informiert und damit einverstanden ist. Das Verfahren wird durch die zuständige Behörde in Zusammenarbeit mit der Polizei, der Finanzpolizei, den Streitkräften und der Verwaltung durchgeführt. Die Beurteilung ist bindend.

In Österreich können Personen auf Antrag von Unternehmen überprüft werden, wenn diese in sensiblen Funktionen oder in sicherheitskritischen Bereichen verwen-

det werden und der PSP zustimmen. Im militärischen Bereich ist der beabsichtigte Zugang zu klassifizierter Information massgebend. Für die Prüfungen im zivilen bzw. militärischen Bereich ist je eine andere Behörde zuständig. In Grossbritannien wird eine PSP durchgeführt, um die Identität einer Person zu bestätigen und ihre Vertrauenswürdigkeit zu prüfen, bevor ihr Zugang zu klassifizierten Informationen und Material oder nationaler kritischer Infrastruktur gegeben wird. In Schweden ist auch der Zugang zu klassifizierten Informationen massgebend. In den Niederlanden werden die PSP-relevanten Funktionen in eine Funktionsliste eingetragen. Diese Funktionen werden durch jedes Ministerium festgelegt. Kriterium dafür ist der Schaden, der in dieser Stelle verursacht werden kann. Die PSP werden durch den allgemeinen Nachrichtendienst und den militärischen Nachrichtendienst durchgeführt, deren Risikobeurteilungen bindend sind.

In der EU wird eine PSP für den Zugang zu CONFIDENTIEL UE/EU CONFIDENTIAL oder höher eingestuften Verschlusssachen verlangt. Die Prüfung wird durch die nationale Sicherheitsbehörde des Mitgliedstaats nach Massgabe der innerstaatlichen Rechtsvorschriften durchgeführt. Der Entscheid der nationalen Sicherheitsbehörde ist für die EU-Behörde bindend.

BSV

In Deutschland ist für ein BSV die konkrete Vergabe eines Verschlusssachenauftrags VS-VERTRAULICH oder höher oder die Teilnahme an einer entsprechend Ausschreibung erforderlich. Das Bundesministerium für Wirtschaft und Energie führt die für die Auftraggeberin bindende Risikobeurteilung durch. In Frankreich wird für die Durchführung eines BSV das Vorliegen eines Vertrags verlangt, zu dessen Erfüllung klassifizierte Informationen oder klassifiziertes Material erstellt oder Zugang dazu erforderlich ist. Die Risikobeurteilung ist nicht bindend. In Italien muss die Auftraggeberin nach der Vergabe eines «geheim» eingestuften klassifizierten Auftrags für die Einleitung des BSV betreffend das entsprechende Unternehmen sorgen. Die Risikobeurteilung ist bindend. In Österreich ist der beabsichtigte Zugang zu klassifizierten Informationen entscheidend. Die Risikobeurteilung ist nicht bindend. In Grossbritannien ist Voraussetzung für das BSV, dass eine Firma im Zusammenhang mit einem Regierungsauftrag klassifizierte Informationen der Stufe «geheim» oder höher oder entsprechendes Material bearbeitet.

In den Niederlanden ist Voraussetzung für ein BSV, dass das Unternehmen als möglicher Auftragnehmer für einen klassifizierten Auftrag im Verteidigungsbereich vorgesehen ist. Das Verfahren wird durch je eine Stelle des Verteidigungsministeriums durchgeführt. Ist das Unternehmen als möglicher Auftragnehmer für einen internationalen klassifizierten Auftrag vorgesehen, wird das Verfahren durch das Ministerium für Inneres und Überseegebiete durchgeführt, dessen Beurteilung bindend ist. In Schweden verlangt die *Protective Security Act,* dass Behörden, die eine Beschaffung mit Bezug zur nationalen Sicherheit durchführen, eine Sicherheitsvereinbarung mit der zu beauftragenden Firma abschliessen. Das Unternehmen hat sich vorgängig einem Audit gemäss den im *Industrial Security Manual* vorgegebenen Kriterien zu unterziehen. Sobald das Resultat vorliegt, führt die Rüstungsbeschaffungsagentur beim Unternehmen Kontrollen durch.

In der EU wird das BSV bei öffentlichen Aufträgen mit Zugang zu Verschlusssachen ab EU CONFIDENTIAL verlangt. Das Verfahren richtet sich nach den innerstaatlichen Rechtsvorschriften des Mitgliedstaats. Der Entscheid der nationalen Sicherheitsbehörde ist für die EU-Behörde bindend.

Behördliche Organisation

In Deutschland ist das Bundesministerium des Innern die nationale Sicherheitsbehörde. Das Bundesministerium für Wirtschaft und Energie ist einzig für den Geheimschutz in der Wirtschaft zuständig. In Frankreich ist der Generalsekretär der Verteidigung und nationalen Sicherheit die einzige nationale Sicherheitsbehörde. Die *Agence nationale de la sécurité des systèmes d'information* ist für die IT-Sicherheit zuständig. In Italien repräsentiert die Ministerpräsidentin oder der Ministerpräsident die nationale Sicherheitsbehörde. Sie oder er kann die entsprechenden Kompetenzen teilweise an die Staatssekretärin oder den Staatssekretär delegieren und wird durch ein nationales Sicherheitsgremium, geleitet durch die Generaldirektorin oder den Generaldirektor des *Dipartimento Informaziono per la Sicurezza,* unterstützt. In Österreich existiert eine Informationssicherheitskommission für den zivilen Bereich und das Abwehramt für den militärischen Bereich. Obwohl in Grossbritannien das *Cabinet Office* als nationale Sicherheitsbehörde figuriert, sind die einzelnen Verwaltungseinheiten und Agenturen weiterhin für die Sicherheit ihrer Informationen sowie die Sicherheit der Informationen ihrer Auftragnehmer verantwortlich.

In den Niederlanden existieren zwei nationale Sicherheitsbehörden: die zivile nationale Sicherheitsbehörde beim allgemeinen Nachrichten- und Sicherheitsdienst im Ministerium für Inneres und Überseeangelegenheiten und die militärische nationale Sicherheitsbehörde als Teil des niederländischen Verteidigungsministeriums. In Schweden gibt es ebenfalls keine umfassende Sicherheitsbehörde. Die Aufgabe ist zwischen den Streitkräften und dem Aussenministerium (für Informationen der ESA, EU und NATO) aufgeteilt. Das Aussenministerium koordiniert die verschiedenen Kompetenzen, um alle Aufgaben einer nationalen Sicherheitsbehörde ausüben zu können.

Auch in der EU sind mehrere Sicherheitsbehörden vorhanden. So ist beim Rat das Sicherheitsbüro des Generalsekretariats für die technischen Regelungen zum Schutz von Verschlusssachen zuständig. Bei der europäischen Kommission erfüllt die Direktion Sicherheit diese Rolle. Im Bereich der Netz- und Informationssicherheit ist die ENISA zuständig.

Kritische Infrastrukturen

Die Informationssicherheit bei kritischen Infrastrukturen wurde in der NCS ausführlich verglichen, weshalb vorliegend nicht mehr im Detail darauf eingegangen wird. Seit der Verabschiedung der NCS haben aber die EU und Deutschland Neuregelungen entworfen, die nachfolgend summarisch erläutert werden.

Europäische Union

Am 8. August 2016 ist die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016[26] über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU in Kraft getreten. Die EU betrachtet eine sichere Informatikinfrastruktur als unerlässlich für das zuverlässige Funktionieren des Binnenmarktes. Dieses Ziel soll erreicht werden, indem die Mitgliedstaaten verpflichtet werden, ihre Abwehrbereitschaft zu erhöhen und ihre Zusammenarbeit zu verbessern. Überdies werden die KI-Betreiberinnen und gewisse Anbieterinnen von digitalen Diensten (Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste) verpflichtet, Mindestmassnahmen zur Beherrschung von Sicherheitsrisiken zu treffen und den zuständigen nationalen Behörden gravierende Sicherheitsvorfälle zu melden. Die Sicherheitsanforderungen für die Anbieterinnen von digitalen Diensten sind jedoch weniger streng als diejenigen für KI-Betreiberinnen. Kleine und mittlere Unternehmen sowie öffentliche Verwaltungen sind von diesen Pflichten grundsätzlich befreit.

Für die Behörden legt die Richtlinie eine Serie von organisatorischen Massnahmen fest. So muss jeder Mitgliedstaat beispielsweise:

- eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festlegen;
- eine oder mehrere nationale Behörden einrichten, die für die Überwachung der Umsetzung der Richtlinie bei den KI-Betreiberinnen und den Anbieterinnen von digitalen Diensten zuständig sind;
- eine Anlaufstelle benennen, die als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit der Mitgliedstaaten dient;
- ein oder mehrere Computer-Notfallteams benennen, die zuhanden der KI-Betreiberinnen und der verpflichteten Anbieterinnen von digitalen Diensten einen nationalen Frühwarndienst und eine Anlaufstelle im Bereich der technischen Informationssicherheit betreiben (vgl. auch Art. 75 ISG).

Die Richtlinie legt zudem Anforderungen an die nationale und internationale Zusammenarbeit sowie an die Ressourcen der zuständigen Fachbehörden fest.

Die Mitgliedstaaten müssen die Richtlinie bis Mai 2018 in ihrem nationalen Recht umsetzen. Folglich werden in den kommenden Jahren zahlreiche Mitgliedstaaten der EU ihre nationale Gesetzgebung bezüglich Informationssicherheit anpassen.

Deutschland

Das deutsche Gesetz vom 17. Juli 2015 zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) verfolgt ähnliche Ziele wie die oben genannte Richtlinie der EU. Es ist aber früher in Kraft getreten. Im Zentrum der Regelung stehen die KI. Deren Betreiberinnen müssen ein Mindestniveau an Informationssicherheit einhalten und dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) Sicherheitsvorfälle melden. Die beim BSI zusammenlaufenden Informationen werden ausgewertet und den Betreiberinnen zur Verbesserung

26 Abl. L 194 vom 19.7.2016. S. 1.

des Schutzes ihrer Infrastrukturen zur Verfügung gestellt. Gleichzeitig ist die Beratungsfunktion des BSI in diesem Bereich gestärkt worden. Die Telekommunikationsanbieterinnen sind verpflichtet, Sicherheit *nach dem Stand der Technik* zu gewährleisten. Zudem müssen sie bestimmte Sicherheitsvorfälle unverzüglich melden und betroffene Nutzer über bekannte Störungen informieren.

Im Gegensatz zur Richtlinie der EU, die öffentliche Behörden von ihrem Geltungsbereich ausnimmt, erfasst der Geltungsbereich des IT-Sicherheitsgesetzes auch die deutschen Bundesbehörden, mit Ausnahme des Bundestags.

Ergebnisse des Rechtsvergleichs

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

Im Bereich der kritischen Infrastrukturen geht der Bundesrat hingegen mit der NCS und dem ISG in eine andere, den KI-Betreiberinnen gegenüber wesentlich weniger verpflichtende Richtung als die EU oder Deutschland. Der Bundesrat setzt auf die Eigenverantwortung der KI sowie auf eine gezielte, bedarfsgerechte Unterstützung durch den Bund. Demzufolge will er weder Mindeststandards für die KI festlegen noch diese dazu verpflichten, bei schwerwiegenden Vorfällen Meldung zu erstatten.

1.5 Umsetzung

Zur Vollzugsregelung durch die verpflichteten Behörden siehe Ziffer 1.2.9. Die verpflichteten Behörden sind eigenständig für den Vollzug des Gesetzes zuständig. Sie werden die erforderlichen Ausführungsbestimmungen erlassen, wobei die Ausführungsbestimmungen des Bundesrats für die anderen Bundesbehörden gelten, sofern diese keine eigenen Vollzugsbestimmungen erlassen (Subsidiarität). Dieser Vollzugsgrundsatz wurde mit den betroffenen Behörden vereinbart.

Im Rahmen der Vernehmlassung wurde die Vollzugstauglichkeit des Vorentwurfs in Bezug auf die Kantone in Frage gestellt. Es wurde unter anderem bemängelt, dass die Kriterien für die Anwendung der Vorlage auf die Kantone unklar und daher auch die Auswirkungen für die Kantone kaum abschätzbar seinen. Im Rahmen der Bewertung der Vernehmlassungsergebnisse wurde deshalb beschlossen, neu die Zusammenarbeit mit den Kantonen nach dem bewährten Modell der Datenschutzgesetzgebung (vgl. Art. 37 DSG) zu konzipieren. Die anderen Anliegen der Kantone (Mitwirkung an der Ausarbeitung der Vollzugsbestimmungen, Zugriff auf die Ressourcen des Bundes für die Durchführung von PSP, Beratung durch die Fachstelle

des Bundes für Informationssicherheit usw.) wurden ebenfalls grösstenteils berücksichtigt (siehe Ziff. 1.2.2).

In der Praxis wird die Fachstelle des Bundes für Informationssicherheit die Entwürfe zu den Ausführungsbestimmungen und Standards vorbereiten und sie der Konferenz der Informationssicherheitsbeauftragten zur Beurteilung der Wirksamkeit, Wirtschaftlichkeit und Vollzugstauglichkeit unterbreiten. Die konsolidierten Vorgaben werden anschliessend vom Bundesrat verabschiedet. Die Bundesbehörden und die Kantone sollen für alle wichtigen und kostenverursachenden Regelungen zur Stellungnahme eingeladen werden. So wird einerseits ein möglichst einheitliches Sicherheitsniveau erreicht und andererseits den Bedürfnissen aller Bundesbehörden sowie der Kantone gebührend Rechnung getragen.

Für gewisse Regelungsgegenstände kann das Ausführungsrecht rasch und unkompliziert erlassen werden. Dies betrifft vor allem die PSP (3. Kap.), das BSV (4. Kap.) und die Informationssicherheit bei KI (5. Kap.), aber auch die Informationssysteme zur zentralen Kontrolle von Identitäten (2. Kap. 6. Abschn.). Hingegen sind für den Vollzug der allgemeinen Massnahmen der Informationssicherheit (2. Kap.) weitere Abklärungen erforderlich. Es geht hier um Kernprozesse und Anforderungen, die an den Stand von Wissenschaft und Technik angepasst und behördenübergreifend harmonisiert werden müssen.

Das ISG sieht genügend Zeit für eine vernünftige Umsetzung vor. Der Bundesrat wird es erst in Kraft setzen, wenn die erforderlichen Ausführungsbestimmungen und Grundlagen bereit sind. Allenfalls ist eine gestaffelte Inkraftsetzung möglich. Der Bundesrat wird die Wirksamkeit des Entwurfs periodisch prüfen lassen und der zuständigen Aufsichtskommission Bericht erstatten. Die Kantone sind für entsprechende Prüfungen selber verantwortlich.

2 Erläuterungen zu einzelnen Artikeln

2.1 Informationssicherheitsgesetz

Titel

Der Erlass stellt kein allgemeines Informationssicherheitsgesetz dar. Er richtet sich primär an die Bundesbehörden sowie an zu bestimmende Organisationen des öffentlichen und privaten Rechts, die Aufgaben des Bundes erfüllen. Dritte können zwar vom Gesetz erfasst werden, wenn sie mit Informationen oder mit Informatikmitteln des Bundes umgehen. Dies geschieht jedoch nur durch die Anwendung der relevanten Bestimmungen durch eine Behörde oder eine Organisation des Bundes.

Beim Begriff *Informationssicherheit* wird grundsätzlich auf die derzeit gängigen Normenwerke abgestellt. Die Informationssicherheit umfasst demnach die Gesamtheit aller Anforderungen und Massnahmen, mit denen die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Nachvollziehbarkeit von Informationen sowie die Verfügbarkeit und die Integrität von Informatikmitteln geschützt wird (vgl. Art. 6). Sie darf nicht auf die Informatiksicherheit reduziert werden. Sie umfasst nämlich alle Bearbeitungsvorgänge, also auch Papierdokumente und mündliche Äusserun-

gen, und nicht nur die elektronische Bearbeitung. Vom Begriff wird auch die Datensicherheit nach Artikel 7 DSG oder die Umsetzung anderer Gesetze, die Anforderungen an den Schutz von Informationen festlegen, erfasst.

Die Integration der Regelung der PSP und des BSV in die Vorlage bedeutet, dass beide Instrumente als *besondere* Massnahmen der Informationssicherheit zu verstehen sind. Die Gründe zur Durchführung solcher Prüfungen werden von den allgemeinen Massnahmen der Informationssicherheit abgeleitet.

Ingress

Siehe Ziffer 5.1.

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Zweck

Absatz 1 weist darauf hin, dass sowohl die Informationen als solche als auch die Informatikmittel vom Gesetz erfasst werden. Der Begriff *Information* wird im ISG nicht definiert, da sich der Begriff im ISG mit dem umgangssprachlichen Gebrauch deckt. Das Gesetz macht grundsätzlich auch keinen Unterschied zwischen *Informationen* und *Daten*: Beide Begriffe werden unter dem Begriff *Informationen* subsumiert. Der Begriff *Daten* wird nur dann verwendet, wenn Personendaten nach dem DSG betroffen sind. Der Begriff *Informatikmittel* wird in Artikel 5 definiert.

Absatz 2: Sicherheit ist kein Selbstzweck. Der Schutz der Informationen dient bestimmten öffentlichen Interessen bzw. Eigeninteressen des Bundes als Institution. Geschützt werden hier also primär die Interessen des Bundes bzw. der Schweiz und nicht diejenigen Dritter. Diese Interessen werden abschliessend aufgelistet (Bst. a–e). Die Liste orientiert sich im Wesentlichen an der bereits bestehenden Liste von Artikel 7 Absatz 1 BGÖ. Diese nennt die Bereiche, in denen der Zugang zu amtlichen Dokumenten eingeschränkt, aufgeschoben oder verweigert werden kann. Die Liste von Artikel 1 Absatz 2 ISG ist allerdings mit derjenigen des BGÖ nicht völlig identisch, da die Ziele und der Geltungsbereich des BGÖ und des ISG nicht übereinstimmen (s. auch Ziff. 1.2.3).

Das vorliegende Gesetz schützt folgende Interessen:

- Der Schutz der Entscheidungs- und Handlungsfähigkeit der Bundesbehörden (Bst. a) durch Massnahmen der Informationssicherheit ist ein Kerninteresse dieses Gesetzes. Die Bundesbehörden sind für die Erfüllung ihrer verfassungsmässigen und gesetzlichen Aufgaben immer mehr von der Verfügbarkeit, der Integrität sowie, in bestimmten Fällen, der Vertraulichkeit ihrer Informationen sowie vom zuverlässigen Funktionieren der Informatikinfrastruktur abhängig (s. Art. 7 Abs. 1 Bst. a und b BGÖ sowie Ziff. 2.2.2.1.1 und 2.2.2.1.2 BGÖ-Botschaft).
- Mit dem Interesse nach Buchstabe b werden in erster Linie Informationen aus dem Bereich des Polizei-, Zoll-, Nachrichtendienst- und Militärwesens und der Landesversorgung sowie die Mittel, welche die Bundesbehörden zur

Sicherstellung der inneren und äusseren Sicherheit einsetzen, geschützt. Derartige Informationen weisen oft einen erhöhten Bedarf an Vertraulichkeit auf, da ihr Missbrauch existenzgefährdende Folgen für den Staat, die Bevölkerung oder bestimmte Personen oder Personengruppen haben kann. Aus demselben Grund müssen die Informatikmittel der Behörden, welche zur Unterstützung von kritischen Sicherheitsaufgaben eingesetzt werden, auch in Krisenzeiten stets verfügbar und funktionstüchtig bleiben (s. Art. 7 Abs. 1 Bst. c BGÖ sowie Ziff. 2.2.2.1.3 BGÖ-Botschaft).

– Die Aussenbeziehungen (Bst. c) zählen gemeinsam mit den Sicherheitsfragen zu den sensitiven Bereichen staatlicher Tätigkeit. Im Vordergrund steht hier die Wahrung der Vertraulichkeit von Informationen. Insbesondere die Informationsbeschaffung über Situationen und Vorgänge im Ausland sowie die Absichten ausländischer und internationaler Behörden sind für die Führung der Aussenpolitik und die Pflege der Aussenbeziehungen von grosser Bedeutung. Für die erfolgreiche Verhandlungsführung ist es entscheidend, dass die entsprechenden Strategien und Absichten nicht an die Gegenpartei oder die Öffentlichkeit gelangen. Ähnliches gilt für diplomatische Schritte im zwischenstaatlichen Verkehr. Zu erwähnen ist schliesslich, dass die Schweiz aufgrund internationaler vertraglicher Verpflichtungen oder anerkannter Staatenpraxis gehalten sein kann, gewisse ausländische Dokumente nicht öffentlich zugänglich zu machen (s. Art. 7 Abs. 1 Bst. d BGÖ sowie Ziff. 2.2.2.1.4 BGÖ-Botschaft).

– Buchstabe d: Die unberechtigte Bekanntgabe oder die Verfälschung bestimmter Informationen sowie die Störung von Informationssystemen der Bundesbehörden können zu erheblichem Schaden für die wirtschafts-, finanz- oder währungspolitischen Interessen der Schweiz führen. Beim heutigen unerbittlichen internationalen Wettbewerb gewinnen diese wirtschaftlichen Interessen zusätzlich an Bedeutung (s. Art. 7 Abs. 1 Bst. f BGÖ sowie Ziff. 2.2.2.1.6 BGÖ-Botschaft).

– Mit Buchstabe e wird der Bereich *Compliance*, d. h. die Einhaltung der gesetzlichen und vertraglichen Verpflichtungen der Bundesbehörden zum Schutz von Informationen erfasst, die nicht unter die Buchstaben a–d fallen. Die Bundesbehörden bearbeiten zur Erfüllung ihrer gesetzlichen Aufgaben sehr viele Informationen, die sie aufgrund verschiedenster gesetzlicher Bestimmungen schützen müssen (DSG, RVOG, ParlG, NBG, BÖB, FHG usw.) oder die sie von Dritten nur unter der Bedingung der Gewährleistung eines angemessenen Schutzes erhalten. Berufs-, Geschäfts- und Fabrikationsgeheimnisse oder die Wahrung der Vertraulichkeit und Integrität von Personendaten stellen zwar keine unmittelbaren Eigeninteressen des Bundes dar. Der Bund ist aber entweder gesetzlich oder durch Vereinbarung verpflichtet, diese Informationen zu schützen. Wenn bekannt wird, dass die Bundesbehörden ihre Verpflichtungen zum Schutz dieser Informationen nicht einhalten, kann ihre Vertrauenswürdigkeit erheblich darunter leiden und der Bund zur Verantwortung gezogen werden. Buchstabe e stellt somit ein Auffangbecken für alle Informationen dar, welche die Bundesbehörden bearbeiten und schützen, aber nicht unbedingt klassifizieren müssen. Er schützt überdies das

Interesse der Bundesbehörden an der Aufrechterhaltung ihrer hohen Vertrauenswürdigkeit. (s. Art. 7 Abs. 1 Bst. e, g und h BGÖ sowie Ziff. 2.2.2.1.5, 2.2.2.1.7 und 2.2.2.1.8 BGÖ-Botschaft).

Art. 2 Verpflichtete Behörden und Organisationen

Als verpflichtete Behörden nach Absatz 1 werden die Bundesversammlung bzw. die eidgenössischen Räte, der Bundesrat, die eidgenössischen Gerichte (Bundesgericht, Bundesstrafgericht, Bundesverwaltungsgericht, Bundespatentgericht sowie die Militärgerichte, die Militärappellationsgerichte und das Militärkassationsgericht), die Schweizerische Bundesanwaltschaft und ihre Aufsichtsbehörde sowie – im Interesse der Währungs- und Wirtschaftspolitik des Bundes – die Schweizerische Nationalbank genannt. Alle diese Institutionen unterstehen in ihrer Tätigkeit als Behörden keiner unmittelbaren Weisungsbefugnis einer anderen Behörde. Sie sollen aber infolge des behördenübergreifenden Informationsflusses für ihren eigenen organisatorischen Zuständigkeitsbereich zur Anwendung dieses Erlasses verpflichtet werden. Sofern das Gesetz Rechtsetzungsdelegationen enthält, spricht es diese Behörden stets als *die verpflichteten Behörden* an. Zu den Gründen, weshalb alle Bundesbehörden vom Gesetz erfasst werden sollen, siehe Ziffer 1.2.2.

Es versteht sich, dass das ISG bei einzelnen Regelungen der verfassungsmässigen Stellung und den Besonderheiten der verschiedenen Behörden bzw. Institutionen Rechnung zu tragen hat. Es enthält daher beispielsweise Ausnahmen von der Pflicht zur PSP bei den vom Volk gewählten Personen sowie Ausnahmen bei bestimmten Vollzugszuständigkeiten, insbesondere im Bereich der eidgenössischen Gerichte. In denjenigen Bestimmungen des Erlasses, die nur Pflichten für bestimmte Behörden oder Organisationen enthalten, werden diese entsprechend spezifiziert (z. B. Art. 7 oder 10 Abs. 2). Auf der Ebene des Gesetzes sollen auch nicht die gesamte Vollzugsorganisation der verschiedenen Behörden und die Kompetenzen ihrer Organe bzw. Stellen festgelegt werden. Dies hat durch die entsprechende Vollzugsrechtsetzung der einzelnen Behörden zu erfolgen.

Absatz 2 berücksichtigt, dass die in Absatz 1 erwähnten Behörden sich nur beschränkt mit eigentlichen Vollzugsaufgaben zu befassen haben und dass die ihnen unterstellten Organisationen im Bereich ihrer gesetzlichen Aufgaben von den neuen Regelungen im Rahmen ihrer Zuständigkeiten unmittelbar verpflichtet sein sollen. Die Aufteilung zwischen Behörden und unterstellten Organisationen soll insbesondere sicherstellen, dass das unterschiedliche Organisationsrecht der erfassten Behörden von der neuen Regelung nicht angetastet wird. Einerseits sollen die verpflichteten Behörden selbst keine untergeordneten Vollzugsaufgaben übernehmen müssen, andererseits sollen aber die erfassten Organisationen keine vom Organisationsrecht abweichenden Rechtsetzungs- oder Entscheidbefugnisse erhalten. Der Begriff *verpflichtete Organisationen* wird im Interesse der gesetzestechnischen Vereinfachung der nachfolgenden Artikel als Kurzbezeichnung eingeführt. Es handelt sich insbesondere um die Parlamentsdienste, die Verwaltungen der einzelnen eidgenössischen Gerichte, die Departemente, die BK, die Armee sowie die Bundesverwaltung einschliesslich der dezentralen Verwaltungseinheiten nach Artikel 2 Absatz 3 RVOG.

Ebenso grundsätzlich dem Gesetz unterstellt sind Organisationen des öffentlichen und privaten Rechts, die Verwaltungsaufgaben des Bundes im Sinne von Artikel 2 Absatz 4 RVOG erfüllen (s. dazu Art. 8 Abs. 4 und 5 RVOG). Es handelt sich insbesondere um Organisationen, die durch Gesetz gegenüber Privaten verfügungsbefugt sind. Für solche Organisationen haftet der Bund nämlich subsidiär (s. Art. 19 VG). Die Unterstellung der dezentralen Verwaltungseinheiten und der mit Verwaltungsaufgaben betrauten Organisationen ausserhalb der Bundesverwaltung ist nicht absolut. Da aufgrund ihrer respektiven Organisationserlasse die Verhältnisse dieser Organisationen zum Bund teilweise sehr unterschiedlich sind, rechtfertigt sich eine effektive Unterstellung nur dann, wenn diese Organisationen für den Bund sicherheitsmässig relevant sind. Dies ist nach Absatz 3 der Fall, wenn sie sicherheitsempfindliche Aufgaben ausüben, wenn sie Informatikmittel des Bundes benutzen oder wenn ihre Informatikmittel eng mit den Informatikmitteln des Bundes vernetzt sind. Der Bundesrat wird die Sicherheitsrelevanz der jeweiligen Organisationen im Rahmen des Ausführungsrechts prüfen und auf Verordnungsebene festlegen, welche von ihnen das ISG ganz oder nur teilweise anwenden müssen. Dies kann entweder in den Ausführungserlassen zum ISG oder in den Ausführungsbestimmungen zur Spezialgesetzgebung erfolgen. Der Bundesrat kann bei Bedarf nur Teile des Gesetzes von diesen Organisationen anwenden lassen (z. B. Bestimmungen über die Klassifizierung, über den Einsatz von Informatikmitteln oder über die PSP). In diesem Zusammenhang wird er im Sinne von Absatz 4 auch bestimmen, ob und inwiefern diese Organisationen das Gesetz autonom vollziehen sollen. Wird eine Organisation vom Geltungsbereich des ISG ausgenommen, dann gilt sie als Dritte.

Absatz 5 hält vorab im Allgemeinen fest, dass sich die Unterstützung der KI-Betreiberinnen nach den Bestimmungen des 5. Kapitels richtet. Ausserhalb des Bundes stehende KI-Betreiberinnen können freiwillig eine Partnerschaft mit dem Bund eingehen und in diesem Rahmen seine Unterstützung in Anspruch nehmen, weshalb die entsprechenden Artikel grundsätzlich für KI-Betreiberinnen gültig erklärt werden – jedoch ohne dass dadurch eine Verpflichtung entsteht. Es versteht sich, dass KI, die der Bund selber betreibt, das ISG uneingeschränkt anwenden müssen. Mit dem ISG verfügt der Bund über besondere Instrumente im Bereich der Informationssicherheit, auf die gewisse Regulatoren und KI-Betreiberinnen zugreifen möchten. Auf Interesse stossen insbesondere die PSP, zum Teil aber auch die Bestimmungen über die Klassifizierung oder über die Sicherheit beim Einsatz von Informatikmitteln. Bestimmte KI-Betreiberinnen greifen bereits heute auf diese Instrumente des Bundes zu. Dies ist beispielsweise der Fall im Bereich der Kernkraftwerke, in welchem der Bund bestimmte Massnahmen der Informationssicherheit vorschreibt (s. Art. 5 und 24 KEG). Es wird deshalb festgehalten, dass die Spezialgesetzgebung bei Bedarf eine Unterstellung bestimmter KI-Betreiberinnen unter das ISG (oder Teile davon) vorsehen kann.

Art. 3 Geltung für die Kantone

Zur Zusammenarbeit mit den Kantonen, siehe Ziffer 1.2.2; zu den PSP für kantonale Angestellte, siehe die Artikel 30 und 32; zum kantonalen Vollzug, siehe Artikel 87.

Art. 4 Verhältnis zu anderen Erlassen des Bundes

Zum Verhältnis zum BGÖ und zur Datenschutzgesetzgebung siehe Ziffer 1.2.3. Absatz 1 hält fest, dass das BGÖ gegenüber den Bestimmungen des ISG Vorrang hat und somit in keiner Art und Weise durch das ISG eingeschränkt wird. Absatz 2 regelt das Verhältnis des neuen Erlasses zu den zahlreichen Bundesgesetzen, die Anforderungen an den Schutz der Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit von Informationen oder an die Verfügbarkeit und Integrität von Informatikmitteln festlegen. Die ergänzende Anwendung des ISG bedeutet, dass seine Bestimmungen einen einheitlichen Rahmen zur Beurteilung des Schutzbedarfs dieser Informationen und zur Umsetzung der spezialgesetzlichen Sicherheitsanforderungen an diese Informationen schaffen.

Art. 5 Begriffe

Einige Begriffe oder Ausdrücke, die für die Vorlage wesentlich sind, können auf Gesetzesstufe nicht näher definiert werden, weil sie ansonsten den erforderlichen Handlungsspielraum der Behörden, Organisationen und Stellen zu sehr einschränken würden. Dies ist insbesondere der Fall für Ausdrücke wie *Beeinträchtigung*, *erhebliche Beeinträchtigung* und *schwerwiegende Beeinträchtigung* der Interessen nach Artikel 1 Absatz 2.

Buchstabe a: Der Begriff *Informatikmittel* wird als Oberbegriff für alle Mittel der Informations- und Kommunikationstechnik verwendet. Auf Verordnungs- und Weisungsstufe werden wo nötig detailliertere Begriffe (Informationssystem, Netzwerk, Anwendung, Sprachübermittlung, Telefonie usw.) verwendet und definiert. Ein Informatikmittel kann auch aus mehreren Systemen oder Mitteln bestehen, die eine funktionale Einheit bilden.

Buchstabe b: Die *sicherheitsempfindliche Tätigkeit* stellt einen zentralen Begriff dar. Die Ausübung einer solchen Tätigkeit ist nämlich nicht nur für die Anwendung des ISG auf Organisationen nach Artikel 2 Absätze 3 und 4 RVOG wichtig, sondern auch Voraussetzung für die Durchführung von PSP und BSV. Sie wird im engen Kontext der Informationssicherheit nach diesem Gesetz definiert.

– Mit der Erwähnung der Klassifizierungsstufe «vertraulich» als Ausgangspunkt für die Definition der sicherheitsempfindlichen Tätigkeit legt Ziffer 1 implizit fest, dass die Sicherheitsempfindlichkeit einer Tätigkeit erst dann angenommen wird, wenn die Interessen nach Artikel 1 Absatz 2 mindestens *erheblich* beeinträchtigt werden können. Sicherheitsempfindlich ist zudem nicht der blosse *Zugang* zu diesen Informationen, sondern deren tatsächliche und berechtigte *Bearbeitung*. Mit anderen Worten übt beispielsweise das Reinigungspersonal in der Regel keine sicherheitsempfindliche Tätigkeit nach diesem Gesetz aus, obwohl die Wahrscheinlichkeit gross ist, dass es während seiner Tätigkeit hin und wieder faktisch Zugang zu klassifizierten Informationen erhalten wird, weil die Mitarbeitenden die Sicherheitsvorschriften nicht immer einhalten. Nicht ausdrücklich erwähnt, aber auch darunter zu subsumieren ist die Benutzung von *klassifiziertem Material* ab der Stufe «vertraulich». Das Material ist nicht mit dem *Informationsträger* zu verwechseln, der dazu dient, für verschiedenste Zwecke die immaterielle

Information materiell zu tragen. Bei klassifiziertem Material handelt sich hingegen um Geräte und Gegenstände, deren Eigenschaften klassifizierte Informationen vermitteln können: Das Material *ist* bzw. enthält *in untrennbarer Weise* die zu schützende (immaterielle) Information. Betroffen sind hauptsächlich Rüstungsgegenstände oder integrierte Kommunikationssysteme im militärischen Bereich. Häufig schreibt ein Drittstaat, der die Lieferung an die Schweiz bewilligt hat, die Klassifizierung vor.

– In Ziffer 2 werden Tätigkeiten erfasst, die mit besonderen Zugriffsrechten auf Informatikmittel der beiden höheren Sicherheitsstufen verbunden sind oder bei deren Ausübung Personen in der Lage sind, beispielsweise durch Datendiebstahl oder Sabotage die Interessen nach Artikel 1 Absatz 2 erheblich zu beeinträchtigen. Die blosse Benützung dieser Informatikmittel wird also nicht als sicherheitsempfindlich betrachtet (ob die Anwender eine sicherheitsempfindliche Tätigkeit ausüben, entscheidet sich aufgrund der Inhalte der bearbeiteten Informationen). Erfasst werden vor allem Administratoren und Anwendungsverantwortliche der Systeme mit hohem oder sehr hohem Schutzbedarf. Der Begriff *Betrieb* nach dieser Ziffer bezieht sich auf die Aktivität der Leistungserbringerinnen im Sinne von Artikel 19 ISG. Er ist klar vom Ausdruck *ein Informationssystem betreiben* abzugrenzen, der in der Datenschutzgesetzgebung verwendet wird, um eigentlich den *Einsatz* eines Informationssystems durch die Leistungsbezügerin regeln (vgl. z. B. Art. 24 Abs. 1 ISG).
– Als sicherheitsempfindlich bezeichnet schliesslich Ziffer 3 den Zugang zu Sicherheitszonen (Art. 23), weil das Schadenspotenzial bei Spionage oder bei Sabotage in diesen Zonen aufgrund der darin befindlichen Informationen und Informatikmittel sehr hoch ist. Erfasst wird auch der Zugang zu den Schutzzonen 2 und 3 nach der Gesetzgebung über den Schutz militärischer Anlagen, die als Sicherheitszonen gelten (vgl. Art. 19 Abs. 1 Bst. c BWIS).

Im Vergleich zur heutigen Regelung bezüglich Voraussetzung für die Durchführung von PSP (s. Art. 19 Abs. 1 BWIS) ist der Begriff der *sicherheitsempfindlichen Tätigkeit* einerseits breiter gefasst, weil er die erhöhten Sicherheitsbedürfnisse im Bereich der Informatik berücksichtigt. Er ist andererseits aber auch enger konzipiert, weil er den regelmässigen Zugang zu besonders schützenswerten Personendaten, deren Offenbarung die Persönlichkeitsrechte der Betroffenen schwerwiegend beeinträchtigen könnte, nicht mehr umfasst (s. Ziff. 1.2.5).

Buchstabe c: Diese Begriffsdefinition ist identisch mit der Definition von Artikel 6 Absatz 1 Buchstabe a Ziffer 4 NDG. Beide Definitionen orientieren sich an der Terminologie des Bevölkerungsschutzes.

2. Kapitel: Allgemeine Massnahmen

1. Abschnitt: Grundsätze

Art. 6 Informationssicherheit

Artikel 6 erfasst den materiellen Inhalt der Informationssicherheit sowie die wichtigsten Grundsätze, nach welchen sie umgesetzt werden muss. Er ergänzt somit den Zweckartikel (Art. 1), indem er die detaillierten Schutzziele darlegt.

Der Schutzbedarf der Informationen nach Absatz 1 wird hinsichtlich der potenziellen Beeinträchtigung der Interessen nach Artikel 1 Absatz 2 erhoben und in Bezug auf die detaillierten Kriterien von Absatz 2 definiert. Der spezifische, sachbedingte Schutzbedarf wird implizit sehr häufig von anderen Gesetzen vorgegeben (s. auch Art. 1 Abs. 2 Bst. e sowie Art. 4 Abs. 2).

In sachlicher Hinsicht nennen Lehre und Praxis meistens vier jeweils nach den Umständen zu gewichtende Schutzkriterien der Informationssicherheit, nämlich die Wahrung der Vertraulichkeit, der Integrität, der Verfügbarkeit und der Nachvollziehbarkeit der Informationen. Oft werden noch weitere Schutzkriterien erwähnt, die aber grundsätzlich durch die in Absatz 2 aufgeführten Kriterien oder allenfalls durch eine Kombination derselben abgedeckt werden, beispielsweise die Authentizität (unter Integrität erfasst), die Zurechenbarkeit oder die Nichtabstreitbarkeit (von den Kriterien der Integrität und der Nachvollziehbarkeit abgeleitet).

- *Vertraulichkeit:* Dieser Grundsatz wird dahingehend konkretisiert, dass Informationen nur Berechtigten zugänglich sein sollen. Der Kreis der Berechtigten ergibt sich aus dem Kontext der jeweiligen gesetzlichen Aufgabenerfüllung sowie dem Inhalt und der Bedeutung der Information. Entsprechend kann der Kreis der Berechtigten auf wenige Personen beschränkt oder gross sein.
- *Verfügbarkeit:* Für die Entscheidungs- und Handlungsfähigkeit der Behörden und Organisationen ist erforderlich, dass sie im Rahmen der gesetzlichen Aufgabenerfüllung die notwendigen Informationen rechtzeitig abrufen können. Die Anforderungen an die Verfügbarkeit von Informationen sind höher, wenn diese für die Erfüllung von wesentlichen Aufgaben unterbruchlos verfügbar sein müssen.
- *Integrität:* Die Wahrung der Unversehrtheit und Richtigkeit der Informationen ist unter anderem für Informationen von Bedeutung, die zur Veröffentlichung oder Wiederverwendung (s. Ziff. 1.1.1, OGD) bestimmt sind. Auch Personendaten (Art. 5 DSG) oder Informationen in der Buchführung (Art. 38 FHG) müssen richtig sein. Die Wahrung der Integrität ist zudem für das korrekte Funktionieren bestimmter Informatikmittel entscheidend.
- *Nachvollziehbarkeit:* Die nachvollziehbare Bearbeitung der Informationen ist insbesondere für alle öffentlichen Verfahren (Strafverfahren, Beschwerdeverfahren usw.) von grosser Bedeutung, aber auch für die Erfüllung von Kontroll- und Aufsichtsaufgaben und das Vorgehen bei Missbräuchen.

Die verpflichteten Behörden und Organisationen müssen somit nach den Absätzen 1 und 2 eine Beurteilung des Schutzbedarfs von Informationen vornehmen und bestimmen, in welcher Hinsicht und wie stark die Informationen geschützt werden müssen. Der Schutz der Vertraulichkeit ist beispielsweise nur erforderlich, wenn sie aus einem rechtlichen Grund gewährleistet werden muss. Bestimmte Informationen können höhere Anforderungen an den Schutz ihrer Integrität oder Verfügbarkeit haben, ohne dass diese besonderen Anforderungen gesetzlich festgelegt sind, etwa dann, wenn die entsprechenden Informationen für die Aufgabenerfüllung einer Behörde unbedingt richtig oder verfügbar sein müssen. Dies trifft insbesondere für Informationen und Informatikmittel zu, die geschäftskritische Prozesse unterstützen.

Obwohl sich die Anforderung nach einem angemessenen Schutz der Informatikmittel vor Missbrauch und Störung grundsätzlich bereits aus Absatz 2 Buchstaben b und c ergibt, wird sie noch ausdrücklich erwähnt, weil die Unterstützung der Geschäftsprozesse durch die Technik immer mehr an Bedeutung gewonnen hat. Ihr gutes Funktionieren stellt heute eine unentbehrliche Voraussetzung für die effiziente Aufgabenerfüllung der Bundesbehörden dar.

Es versteht sich, dass eine absolute Sicherheit ein unerreichbares Ideal darstellt, und dass der Aufwand für die Behebung verbleibender kleinerer Sicherheitslücken unverhältnismässig hoch werden kann. Die zuständigen Behörden und Organisationen müssen daher darauf achten, dass ihre Massnahmen zweckmässig und wirtschaftlich sind. Entsprechend ist bei der Verfolgung der Schutzmassnahmen von den übergeordneten Stellen eine Güterabwägung zwischen Sicherheitskosten und -nutzen vorzunehmen. Erschweren Sicherheitsmassnahmen die Aufgabenerfüllung der Mitarbeitenden zu sehr, ist die Wahrscheinlichkeit gross, dass sie entweder nicht eingehalten oder gar absichtlich umgegangen werden.

Art. 7 Oberste Führungsverantwortung

Sicherheit ist Chefsache. Die verpflichteten Behörden werden deshalb vorab aufgefordert, die Informationssicherheit in ihrem Bereich nach dem Stand von Wissenschaft und Technik zu organisieren, umzusetzen und zu überprüfen. Mehrere Fachnormen formulieren entsprechende *Best Practices* und legen Anforderungen für die Umsetzung von Sicherheitsmassnahmen fest, die auf die Bedürfnisse der jeweiligen Behörden, Organisation oder von Teilen derselben zugeschnitten werden können. Das Gesetz verlangt nicht, dass die Behörden beispielsweise ein ISMS nach DIN ISO/IEC Norm 27 001 umsetzen. Ihre Organisation sollte sich aber zumindest darauf ausrichten. Personalmässig kleinere Behörden werden selbstverständlich keine eigene derartige Organisation aufbauen können. Das Gesetz lässt es deshalb zu, dass beispielsweise die eidgenössischen Gerichte den Aufbau einer einzigen gemeinsamen Organisation beschliessen, die gleichzeitig die Unabhängigkeit der verschiedenen Gerichte wahrt. Für die einheitliche behördenübergreifende Umsetzung ist es notwendig, dass die Behörden sich für ein gemeinsames Organisationsmodell entscheiden. Da die Verwirklichung von Informationssicherheit viele Fachbereiche (Finanzen, Personaldienste, Recht, Informatik, Risikomanagement usw.) betrifft, müssen die betroffenen Fachbereiche, die Anliegen der Informationssicherheit mittragen, an der entsprechenden Beschlussfassung beteiligt werden.

Von den Behörden wird auch verlangt, dass sie die Überprüfung der Informationssicherheit regeln. Grundsätzlich obliegt diese Kontrolle den Linienvorgesetzten. Die Informationssicherheitsbeauftragten werden ebenfalls Überprüfungen im Auftrag ihrer Behörde durchführen (s. Art. 82 Abs. 2 Bst. c). Dies kann zum Beispiel durch den jährlichen Vorschlag eines Auditplans erfolgen, der die Auditprioritäten begründet sowie die dafür erforderlichen Ressourcen umschreibt. Die Standards verlangen überdies, dass die Wirksamkeit der Organisation und der Massnahmen periodisch durch eine externe (unabhängige) Stelle überprüft wird. Der Entscheid sowohl über die Periodizität als auch über die Stelle, welche die Prüfung durchführen soll, obliegt der betroffenen Behörde. In der Bundesverwaltung können solche Audits entweder durch die internen Aufsichtsstrukturen der Departemente, durch die EFK, die bereits heute die Revision im Informatikbereich wahrnimmt, oder durch eine externe Firma durchgeführt werden.

In Absatz 2 werden die Behörden aufgefordert, bestimmte Grundsätze festzulegen:

- Die Ziele der verpflichteten Behörde geben das Sicherheitsniveau vor, das erreicht werden soll (Soll-Zustand der Informationssicherheit). Sie setzen eine Kosten-Nutzen-Analyse voraus (wie viel Sicherheit will die Behörde haben und wie viel darf sie kosten) und sind für die Erteilung der erforderlichen Ressourcen massgebend. Die Wirksamkeit der Massnahmen zur Gewährleistung der Informationssicherheit muss am zu erreichenden Sicherheitsniveau gemessen werden.
- Die Behörden müssen auch bestimmen, wie ihre unterstellten Organisationen mit Risiken umgehen sollen, welche Risiken sie ohne Weiteres tragen dürfen und welche Risiken der Behörde rapportiert werden müssen (Risikoakzeptanz). Auch wenn die meisten Risiken der Informationssicherheit auf der operativen Ebene (Departement, Amt oder sogar unterstellte Einheit) behandelt und getragen werden können, können bestimmte Risiken eine strategische Ausprägung haben. Solche Risiken sollen zumindest der betroffenen Behörde kommuniziert werden. Dies ist insbesondere der Fall bei Risiken in Zusammenhang mit Informatikmitteln der Sicherheitsstufe «sehr hoher Schutz» (Art. 17 Abs. 3).
- In jeder Organisation gibt es immer wieder Personen, welche die Informationssicherheit nicht ernst nehmen und vorschriftswidrig oder unsorgfältig mit Informationen oder Informatikmitteln umgehen. Sehr oft werden solche Verstösse *a priori* entschuldigt und entsprechend nicht untersucht. Diese Verstösse können jedoch erhebliche Auswirkungen zur Folge haben. Die verpflichteten Behörden müssen deshalb die Vorschriften konsequent durchsetzen und die Folgen bei Missachtungen festlegen und erläutern.

Art. 8 Risikomanagement

Ein wirksames Risikomanagement ist eine unabdingbare Voraussetzung für eine zweckmässige und wirtschaftliche Informationssicherheit. Das Schwergewicht muss nämlich dort gelegt werden, wo die grössten Risiken stehen, und zwar mit den effizientesten Massnahmen. Deshalb werden die Behörden und Organisationen des Bundes aufgefordert, sowohl in ihrem eigenen Zuständigkeitsbereich als auch im

Rahmen der Zusammenarbeit mit Dritten die Risiken unter Kontrolle zu haben. Die Beurteilung der Risiken setzt profunde Kenntnisse der gesetzlichen Aufgaben und der entsprechenden Geschäftsprozesse, die regelmässige Beurteilung der Bedrohungen, die Analyse der Schwachstellen sowie die Einschätzung der Eintrittswahrscheinlichkeit und des potenziellen Schadensausmasses bestimmter Gefahren voraus. Auch wenn das vorliegend geforderte Risikomanagement fachspezifisch ist und deshalb von Fachspezialisten gesteuert und laufend betrieben werden muss, bleibt Informationssicherheit ein Anliegen, das die Bewirtschaftung von üblichen Geschäftsrisiken betrifft. Deshalb muss es in das übergeordnete Risikomanagement der betroffene Behörde oder Organisation integriert werden.

Ein wichtiges Ziel des Risikomanagements besteht darin, die geeignetsten Massnahmen zur Risikovermeidung oder -reduktion treffen zu können. Risiken können vermieden werden, indem auf eine bestimmte, zu riskante Tätigkeit ganz verzichtet wird (z. B. wird auf ein Informatikvorhaben verzichtet, für welches die Umsetzung von risikogerechten Massnahmen wirtschaftlich nicht vertretbar ist). Selbstverständlich können Risiken auch in Kauf genommen oder getragen werden. Sie sollten aber nicht ignoriert werden. Risiken, die nach der Umsetzung der vorgesehenen Sicherheitsmassnahmen bestehen bleiben (sogenannte Restrisiken), oder Risiken, die nicht vermindert werden sollen, sind klar auszuweisen. Die Entscheidungsträger sind für ihre diesbezügliche Güterabwägung in dokumentierter Form auf diese Risiken und die potenziellen Auswirkungen hinzuweisen. Die verbleibenden Risiken müssen nachweisbar akzeptiert und entsprechend getragen werden.

Im Bereich der Informationssicherheit werden regelmässig organisatorische Massnahmen entwickelt, die wirksamer oder wirtschaftlicher sind. Neue technische Entwicklungen erfolgen noch rascher, insbesondere bei den Informatikmitteln, aber auch bei der Sensorik (z. B. Feuer-, Hitze- oder Bewegungsdetektoren) oder bei der Schliesstechnik (z. B. Schliesssysteme für Türen). Es ist sehr wichtig, dass Sicherheitsmassnahmen nicht auf veralteten Technologien basieren, sondern gegen aktuelle Bedrohungen wirken. Die verpflichteten Behörden und Organisationen sollen möglichst einheitliche Methoden verwenden. Hierzu sollen Standardanforderungen nach dem Stand von Wissenschaft und Technik festgelegt werden (s. Art. 86). Dies im Wissen darum, dass die Kriterien für die Risikoakzeptanz, die für die Bewertung der Risiken massgebend sind, von den jeweiligen verpflichteten Behörden gestützt auf ihre eigenen Informationssicherheit-Bedürfnisse festgelegt werden.

Art. 9 Zusammenarbeit mit Dritten

Als Dritte gelten nach diesem Gesetz alle Behörden, Organisationen und Personen des öffentlichen oder privaten Rechts, die keine verpflichteten Behörden und Organisation (einschliesslich der Kantone) sind und deshalb grundsätzlich unabhängig von diesen Behörden und Organisationen handeln. Die Bundesbehörden sind für ihre Aufgabenerfüllung häufig auf eine Mitwirkung der Privatwirtschaft oder anderer Stellen angewiesen. Die auftragserteilenden Behörden und Organisationen haben in diesem Fall dafür zu sorgen, dass bei der Auftragserteilung und -ausführung die gesetzlich vorgesehenen Massnahmen eingehalten werden. Die einzuhaltenden Sicherheitsmassnahmen werden in der Regel vertraglich geregelt. Grundsätzlich sollten Dritte erst dann Zugang zu Informationen oder zu Informatikmitteln des

Bundes erhalten, wenn sie die erforderlichen Massnahmen umgesetzt haben. Das ISG verlangt von den verpflichteten Behörden und Organisationen auch, dass sie die Umsetzung der Massnahmen angemessen (d. h. risikogerecht) überprüfen. Dies kann zum Beispiel im Rahmen eines Besuchs vor Ort oder mittels schriftlicher Bestätigung durch die Drittpartei erfolgen. Schliesst der Auftrag die Ausübung einer sicherheitsempfindlichen Tätigkeit ein, so müssen die verpflichteten Behörden und Organisationen die erforderlichen PSP (s. Art. 28 ff.) einleiten oder die Durchführung eines BSV (s. Art. 50 ff.) beantragen.

Art. 10 Vorgehen bei Verletzungen der Informationssicherheit

Zu Vorfällen im Bereich der Informationssicherheit wird es auch in Zukunft kommen. Es ist deshalb nötig, einen einheitlichen und effektiven Ansatz für den Umgang mit solchen Vorfällen anzuwenden. Die verpflichteten Behörden und Organisationen müssen die erforderlichen Massnahmen treffen, um Informationssicherheitsvorfälle überhaupt frühzeitig identifizieren zu können (z. B. regelmässige Kontrollen, Sensoren, Alarmanlagen, Netzwerküberwachung, regelmässige Auswertung von Log-Files). Sie müssen ein Verfahren festlegen, nach welchem vorgegangen werden soll, wenn Vorfälle oder Schwachstellen identifiziert werden, und klare Zuständigkeiten für die Behandlung der Vorfälle zuweisen. Interne und externe Mitarbeitende müssen zudem wissen, wie sie beim Eintreten eines Ereignisses zu reagieren haben, damit dessen Auswirkungen minimiert werden können. Damit aus Vorfällen gelernt wird, müssen die verpflichteten Behörden und Organisationen dafür sorgen, dass die Ursachen eines Vorfalls abgeklärt und ausgewertet werden.

Die Bundesbehörden und insbesondere der Bundesrat müssen darüber hinaus alle notwendigen Vorkehrungen treffen, damit sie ihre Kernaufgaben selbst in ausserordentlichen Situationen termingerecht erfüllen können (*Business Continuity Management*, vgl. Art. 6 Abs. 3 RVOG). Es ist heute davon auszugehen, dass die Erfüllung aller kritischsten Aufgaben des Bundes vom zuverlässigen Einsatz von Informatikmitteln abhängt. Das ISG verlangt deshalb, dass die verpflichteten Behörden die aus ihrer strategischen Sicht unverzichtbaren Aufgaben identifizieren und für den Fall einer schwerwiegenden Verletzung der Informationssicherheit (z. B. dauernder Ausfall eines Systems) Vorsorgeplanungen erstellen und entsprechende Übungen durchführen lassen. Für Informatikmittel, die zur Erfüllung solcher unverzichtbarer Aufgaben eingesetzt werden, gilt die Sicherheitsstufe «sehr hoher Schutz» (Art. 17 Abs. 3).

2. Abschnitt: Klassifizierung von Informationen

Art. 11 Grundsätze der Klassifizierung

Die Klassifizierung ist zwingend, sofern die entsprechenden Kriterien erfüllt sind. Sie muss angesichts des Öffentlichkeitsprinzips und des mit der Klassifizierung verbundenen Aufwands jedoch die Ausnahme darstellen. Der Schutzbedarf von Informationen nimmt mit der Zeit oftmals ab oder erübrigt sich nach einem bestimmten Ereignis (z. B. Veröffentlichung eines Berichts oder Abschluss einer

bestimmten Massnahme). Die Klassifizierung derartiger (beispielsweise nicht mehr aktueller) Informationen rechtfertigt sich dann nicht mehr. Sie würde bloss unnötigen Aufwand verursachen. Informationen, die für längere Zeit klassifiziert bleiben müssen, erfordern zudem zunehmend andere technische Schutzvorkehrungen als jene, die nur eine befristete Schutzwürdigkeit haben. Soweit eine Klassifizierung auf Zeit im Voraus nicht möglich ist, muss sichergestellt werden, dass Informationen nicht unnötig klassifiziert bleiben. Eine Überprüfung des Schutzbedarfs soll mindestens im Rahmen der Anbietepflicht an das Bundesarchiv erfolgen.

Der Schutz von klassifizierten Informationen muss während der ganzen Dauer des Schutzbedarfs der betreffenden Informationen gewährleistet werden. Die entsprechenden Massnahmen werden auf Verordnungsebene festgelegt. Sofern die Schweiz mit einem bestimmten Land oder einer bestimmten internationalen Organisation einen völkerrechtlichen Vertrag zum Austausch von klassifizierten Informationen abgeschlossen hat (s. Art. 88 Bst. b), wird die Bearbeitung der Informationen, die unter den Geltungsbereich des Vertrags fallen, nach dessen besonderen Vorschriften geregelt. Liegt kein solcher Vertrag vor, richtet sich die Bearbeitung klassifizierter Informationen nach den Vorschriften des ISG und seiner Ausführungserlasse.

Es kommt auch vor, dass *Material* klassifiziert wird (s. Erläuterungen zu Art. 5 Bst. b Ziff. 1). Das Klassifizieren von Material ist ein Anwendungsfall der Klassifizierung von Informationen, für welchen grundsätzlich dieselben Beurteilungsmethoden und Schutzvorkehrungen gelten (inkl. PSP und BSV).

Art. 12 Zuständigkeiten

In der Bundesverwaltung wird die Zuständigkeit zur Klassifizierung heute der Verfasserin oder dem Verfasser eines Dokuments zugewiesen, weil sie oder er am Besten den Schutzbedarf der Informationen sowie allfällige Risiken einschätzen kann. Die verpflichteten Behörden können aber auch beschliessen, dass die Klassifizierung beispielsweise durch die Behördenleitung, durch eine zentrale zuständige Stelle oder ausschliesslich durch die Linie erfolgen muss. Die Klassifizierung ist grundsätzlich verbindlich. Ist eine Information klassifiziert, wird sie auf ihrem weiteren Weg sozusagen von dieser Klassifizierung begleitet. Wer Zugang zu einer solchen Information erhält, muss die Vorgaben einhalten, die mit der Klassifizierung verbunden sind. Eine Änderung oder Aufhebung der Klassifizierung darf im Grundsatz nur von der Stelle vorgenommen werden, welche die Klassifizierung festgelegt hat. Es versteht sich, dass auch hier der Dienstweg, die Dienstaufsicht und die entsprechenden Weisungsbefugnisse der vorgesetzten Stellen bzw. Aufsichtsbehörden zum Tragen kommen. Letztere können Entscheide der klassifizierenden Stelle gegebenenfalls korrigieren. Die Zuständigkeitsregelung von Artikel 12 schliesst nicht aus, dass die Umsetzung der Klassifizierungs- und Entklassifizierungsvorschriften in Informationssystemen (z. B. GEVER) automatisiert erfolgt.

Absatz 3 ermächtigt dem Bundesrat, die Entklassifizierung von Unterlagen im Hinblick auf oder während deren Archivierung zu regeln. Es handelt sich nicht um eine allgemeine Zuständigkeit zur Regelung der Entklassifizierung von Informationen, denn für ihren eigenen Bereich sind die anderen Bundesbehörden nämlich gemäss Artikel 85 Absatz 1 allein zuständig.

Mit dieser Bestimmung soll einerseits sichergestellt werden, dass nur Informationen, die langfristig einen erhöhten Schutz benötigen, klassifiziert archiviert werden (klassifiziertes Archivgut). Klassifizierte Informationen sollten wenn möglich vor deren Ablieferung ans Bundesarchiv entklassifiziert werden (vgl. Erläuterungen zu Art. 11 Abs. 3). So soll ihr Schutzbedarf spätestens bei der Anbietepflicht an das BAR überprüft werden. Andererseits geht es auch darum, dass klassifiziertes Archivgut nicht ewig klassifiziert bleibt. Deshalb sollen entsprechende Informationen in der Regel nach Ablauf der Schutzfrist automatisch entklassifiziert werden. Der Bundesrat wird in seinem Ausführungsrecht dafür sorgen, dass die Enklassifizierungsmechanismen für das Bundesarchiv und die abliefernden Stellen keinen unnötigen Aufwand verursachen.

Diese Bestimmung zeigt auch implizit auf, dass zwischen ISG und dem Archivierungsgesetz Schnittstellen vorhanden sind. Sowohl das ISG als auch das BGA sind nämlich auf alle Informationen anwendbar, für welche die Bundesbehörden zuständig sind. Es muss deshalb sichergestellt werden, dass keine Ziel- und Zuständigkeitskonflikte zwischen beiden Rechtssystemen entstehen. Im Grundsatz ist das Verhältnis beider Gesetze zueinander jedoch einfach: Das BGA regelt die Archivierung von Unterlagen des Bundes und den Zugang zu diesen Informationen einheitlich; für die üblichen – nicht archivierungstechnischen – Massnahmen zum Schutz von Informationen (und Informatikmitteln) gelten die Vorschriften des ISG. Sofern im Bereich der Informationssicherheit Sonderregelungen für Archivgut nötig sind, werden diese Normen im ISG festgehalten (s. Art. 14 Abs. 2 ISG). Der rechtliche Vollzug dieser Regelung ist unproblematisch, weil der Bundesrat sowohl für den Vollzug des BGA als auch – soweit die Bundesverwaltung betroffen ist – für das Ausführungsrecht zum ISG zuständig ist.

In der Praxis ist der Schutz von Papierdokumenten mit erhöhtem Schutzbedarf unproblematisch. Mit der zunehmenden elektronischen Archivierung von Unterlagen sind jedoch sowohl für die abliefernden Stellen als auch für das Bundesarchiv neue Herausforderungen entstanden. Die für die Planung des Vollzugs zuständigen Stellen werden zusammen mit dem Bundesarchiv überprüfen, ob der heutige organisatorische und technische Schutz gemäss der Archivierungsgestzgebung ausreichend ist oder wie dieser angepasst werden muss, um den Ansprüchen gemäss ISG zu genügen. Für die dafür benötigten personellen und finanziellen Ressourcen wird, so bald abschätzbar, der Bundesrat die entsprechenden Ressourcen für das BAR plafonderhöhend beantragen.

Art. 13 Klassifizierungsstufen

Artikel 13 regelt die materiellen Voraussetzungen für die Klassifizierung von Informationen für alle verpflichteten Behörden und Organisationen und legt die Klassifizierungsstufen fest. Der vorgeschlagene Text beschränkt sich auf eher allgemeine Kriterien und nimmt direkten Bezug auf die in Artikel 1 Absatz 2 Buchstaben a–d umschriebenen und zu schützenden öffentlichen Interessen. Der Verweis auf diese Interessen ist jedoch eingeschränkt: Der Schutz der öffentlichen Interessen nach Buchstabe e stellt keinen eigenen Grund zur Klassifizierung dar. Mit dem Schutz dieses Interesses soll nämlich die rechtmässige Bearbeitung von Informationen sichergestellt werden, deren Schutz in anderen Gesetzen vorgesehen oder mit Dritten

durch Vertrag vereinbart wird. Personendaten nach dem DSG oder Geschäfts-, Fabrikations- oder Berufsgeheimnisse werden demnach grundsätzlich nicht klassifiziert, es sei denn, dass einzelne Informationen zum Schutz eines Interesses nach Artikel 1 Absatz 2 Buchstaben a–d klassifiziert werden müssen. Dasselbe gilt für Informationen, die bei den Gerichten oder Staatsanwaltschaften im Rahmen ihrer ordentlichen Verfahren bearbeitet werden. Die Mehrheit dieser Informationen sind Personendaten, die zwar schützenswert sind, die aber aufgrund des vorliegenden Gesetzes nicht klassifiziert werden müssen. Hingegen können die besonderen Massnahmen, die zum Schutz solcher Informationen getroffen werden, klassifiziert werden (zum Beispiel ein Informationssicherheitskonzept).

Für die Klassifizierungsstufe selbst ist der *Grad der Beeinträchtigung* massgebend, den eine Kenntnisnahme durch Unberechtigte den Interessen nach Artikel 1 Absatz 2 Buchstaben a–d zufügen kann. Für die Zuweisung zu einer Klassifizierungsstufe ist massgebend, ob die Kenntnisnahme durch Unberechtigte diese Interessen:

- *beeinträchtigen kann:* Klassifizierungsstufe «intern»;
- *erheblich beeinträchtigen kann:* Klassifizierungsstufe «vertraulich»;
- *schwerwiegend beeinträchtigen kann:* Klassifizierungsstufe «geheim».

Diese Qualifizierungen stellen unbestimmte Rechtsbegriffe dar, die unter Berücksichtigung der Risikopolitik noch zu konkretisieren sind.

Obschon das Kriterium der Schwere der potenziellen Beeinträchtigung der Interessen nach Artikel 1 Absatz 2 Buchstaben a–d für die Klassifizierung massgebend ist, genügt es alleine nicht. Es muss auch eine vernünftige kausale Verbindung zwischen der unberechtigten Kenntnisnahme der Information und der potenziellen Beeinträchtigung der geschützten Interessen geben. Erforderlich ist somit, dass auch die Eintrittswahrscheinlichkeit des Schadens berücksichtigt wird. Die Klassifizierung einer Information entspricht also dem Ergebnis einer Risikobeurteilung und soll somit den tatsächlichen *Schutzbedarf* dieser Information wiedergeben.

Bei der Beurteilung des Schutzbedarfs von Informationen *politischer Natur* ist besondere Zurückhaltung erforderlich. Zwar wird der Schutz der freien Meinungs- und Willensbildung der verpflichteten Behörden und Organisationen von Artikel 1 Absatz 2 Buchstabe a (Entscheidungsfähigkeit) erfasst. In einer modernen Demokratie gehört es aber zur normalen Regierungstätigkeit, dass politische Ideen, Vorschläge, Konzepte und Entscheide in der Öffentlichkeit besprochen und gegebenenfalls (auch heftig) kritisiert werden. Die Klassifizierung darf also nicht dazu dienen, bestimmte Sachverhalte der öffentlichen Debatte zu entziehen, wenn kein überwiegendes öffentliches Interesse dafür besteht.

Absatz 1: Als Grenzkriterium zwischen «nicht klassifiziert» und «klassifiziert» gilt auch für eine gesetzlich nicht weiter qualifizierte «Beeinträchtigung» der betreffenden Interessen, dass qualifizierte Anhaltspunkte vorliegen müssen, welche die Klassifizierung «intern» zu begründen vermögen. So darf der potenzielle Schaden nicht einfach vernachlässigbar sein: Die Beeinträchtigung der Interessen nach Artikel 1 Absatz 2 Buchstaben a–d muss vielmehr *spürbar* sein. Im Vergleich zum heutigen Artikel 7 ISchV, wonach bloss ein «Nachteil» verlangt wird, stellt die Neuregelung also eine wesentliche Erhöhung der Klassifizierung dar. Wenn es um *sicherheits-*

relevante Informationen im Sinne von Artikel 1 Absatz 2 Buchstabe b geht, kann der Schwellenwert für die Klassifizierung «intern» relativ rasch erreicht werden. Die Klassifizierung «intern» wird für derartige Fälle am häufigsten verwendet. So werden einzelne Sicherheitsunterlagen zu Informatikmitteln oder einfache Einsatzpläne von Sicherheitskräften in der Regel als «intern» klassifiziert.

Absatz 2: Im Vergleich zur heutigen Regelung, wonach bloss ein unqualifizierter *Schaden* verlangt wird (Art. 6 ISchV), stellt die vorgeschlagene Neuregelung eine Erhöhung der Anforderungen zur Klassifizierung dar. Mit dem gewählten Ausdruck wird ein deutlicher und gewichtiger Schaden verlangt, beispielsweise:

- Die freie Meinungs- und Willensbildung der verpflichteten Behörden wird vorübergehend unrechtmässig erschwert.
- Eine verpflichtete Organisation wird vorübergehend handlungsunfähig.
- Die Erfüllung bestimmter Aufgaben einer Behörde oder Organisation wird über längere Zeit erheblich erschwert.
- Bestimmte Ressourcen der Armee oder der Sicherheitsorgane des Bundes sind vorübergehend einsatzunfähig.
- Die Position der Schweiz in Rahmen von internationalen Verhandlungen wird erheblich erschwert.
- Die Sicherheit von Personen oder Gruppen von Personen wird gefährdet.
- Dem Bund entsteht ein erheblicher finanzieller Schaden.

Absatz 3: Mit der gewählten Formulierung wird ein besonders grosser, katastrophaler Schaden für den Bund verlangt, beispielsweise:

- Eine verpflichtete Behörde ist vorübergehend entscheidungs- oder handlungsunfähig oder ihre Entscheidungs- oder Handlungsfähigkeit ist über längere Zeit besonders ernsthaft erschwert.
- Die Erfüllung unverzichtbarer Aufgaben einer verpflichteten Organisation wird vorübergehend verhindert oder über längere Zeit ernstlich erschwert.
- Wesentliche Ressourcen der Armee oder der Sicherheitsorgane des Bundes sind einsatzunfähig.
- Leib und Leben von Bevölkerungsgruppen werden gefährdet.
- Das Erbringen unverzichtbarer Dienstleistungen durch kritische Infrastrukturen wird unterbrochen.
- Besonders sicherheitsempfindliche Funktionen eines Kernkraftwerks werden sabotiert.
- Der Bund erleidet einen schwerwiegenden finanziellen Schaden.

Die Klassifizierung muss sofort ersichtlich und darf nicht mit anderen Vermerken verwechselbar sein. Im internationalen Rahmen hat sich die Regel durchgesetzt, dass die Klassifizierung immer in Grossbuchstaben und in fetter Schrift vermerkt wird. Absatz 4 ist nötig, damit diese Regel für alle Behörden des Bundes gilt.

Art. 14 Zugang zu klassifizierten Informationen

Absatz 1 umschreibt die Voraussetzungen für den Zugang zu klassifizierten Informationen, der wiederum Voraussetzung für das Bearbeiten der entsprechenden Informationen ist. Der Grundsatz «Kenntnis nur wenn nötig» gilt für jede einzelne klassifizierte Information. Es besteht also kein allgemeines Recht, Zugang zu allen klassifizierten Informationen zu haben. Dies trifft auch für Prüf-, Kontroll- oder Aufsichtsorgane zu, die gegebenenfalls zwar ein allgemeines Informationsrecht haben, die aber für jede einzelne klassifizierte Information den Nachweis dafür erbringen müssen, dass sie zur Erfüllung ihres Auftrags tatsächlich von den betreffenden Informationen Kenntnis haben müssen. Bei einem vertraglich vereinbarten Zugangsrecht müssen die entsprechenden Verträge den Zugang zu klassifizierten Informationen vorsehen und deren Bearbeitung regeln. «Gewähr bieten» für einen sachgerechten Umgang setzt voraus, dass die Personen, die klassifizierte Informationen bearbeiten sollen, entsprechend ausgebildet wurden. Ferner müssen sie gegebenenfalls den Nachweis für die Fähigkeit erbringen, die erforderlichen technischen und physischen Sicherheitsmassnahmen einhalten zu können. Für «vertraulich» oder «geheim» klassifizierte Informationen kann zudem die Durchführung einer PSP eine weitere Bearbeitungsvoraussetzung darstellen.

Absatz 2: Die Regelung des Zugangs zu Archivgut (Art. 9–16 BGA) hat sich auch in Bezug auf klassifiziertes Archivgut bewährt und soll weiterhin gelten (s. auch Erläuterungen zu Art. 12 ISG).

Absatz 3: Die Mehrheit der Länder und internationalen Organisationen, mit welchen die Schweiz einen völkerrechtlichen Vertrag zum Austausch klassifizierter Informationen abgeschlossen hat, verlangt, dass ihre klassifizierten Informationen ausschliesslich von Personen mit ihrem Bürgerrecht oder mit Schweizer Bürgerrecht bearbeitet werden (sogenannte *Drittstaatenausschluss-Klausel*). Derartige Informationen sind also Personen anderer Nationalität grundsätzlich nicht zugänglich. Vorbehalten bleibt eine vorgängige Bewilligung der Verfasserin der Informationen.

Art. 15 Zugang zu klassifizierten Informationen in besonderen Verfahren

Das Verfahrensrecht der Bundesversammlung sowie dasjenige der Gerichte und der Staatsanwaltschaften bleiben vorbehalten. Für den Zugang zu klassifizierten Informationen (z. B. im Rahmen der Verwendung derselben als Entscheidgrundlage oder als Beweismittel) soll das jeweilige Verfahrensrecht zur Anwendung kommen. Die Verfahrensgesetze des Bundes enthalten selbst Regelungen darüber, wie weit solche Informationen den Verfahrensbeteiligten zur Einsicht freigegeben werden bzw. wie weit sie im Rahmen öffentlicher Verfahren bekannt werden dürfen oder wie weit Zeugen die Aussage unter Hinweis auf gesetzliche Geheimhaltungspflichten verweigern können (s. etwa Art. 47, 150, 153 und 154 ParlG, Art. 56 Abs. 2 und 59 Abs. 2 BGG, Art. 16 Abs. 2, 18 Abs. 2, 27 und 28 VwVG, Art. 40 Abs. 3 VGG oder Art. 70, 170, 173 Abs. 2 und 194 Abs. 2 StPO sowie Art. 45, 48 Abs. 2 und 77 MStP; s. auch Art. 58 der Verordnung vom 24. Oktober 1979[27] über die Militärstrafrechtspflege). Vor dem Entscheid über eine Bekanntgabe klassifizierter Informatio-

27 SR **322.2**

nen kann allerdings der klassifizierenden Stelle Gelegenheit gegeben werden, sich zu den Klassifizierungsgründen zu äussern und zu den allfälligen Auswirkungen einer Bekanntgabe angehört zu werden. Das zuständige Organ bzw. Gericht entscheidet dann unter Würdigung der Umstände über das weitere Vorgehen.

3. Abschnitt: Sicherheit beim Einsatz von Informatikmitteln

Art. 16 Sicherheitsverfahren

Die Zeiten sind längst vorbei, als beispielsweise die Bundesämter oder die Gerichte ihre eigenen Informatikmittel im eigenen Haus betrieben. Heute beziehen die Behörden und Organisationen des Bundes in der Regel ihre Informatikleistungen bei hochspezialisierten externen Leistungserbringerinnen. Dadurch ist eine organisatorische Trennung zwischen Einsatz und Betrieb von Informatikmitteln entstanden, die auch wesentliche Auswirkungen auf die Sicherheit hat. Dies ist insbesondere der Fall, weil die Informationssicherheit meistens als reine technische Angelegenheit betrachtet wird, für welche die Leistungserbringerinnen verantwortlich sind. Das Gesetz legt im Grundsatz fest, welche Aufgaben die leistungsbeziehenden Behörden und Organisationen erfüllen müssen, um ihre Verantwortung in Bezug auf die Sicherheit wahrzunehmen. Die verpflichteten Behörden (und nicht die Organisationen) müssen diese Aufgaben in ein sogenanntes Sicherheitsverfahren näher umschreiben. Alle Bundesbehörden verwenden bereits heute ein solches Verfahren. Die vorhandenen Verfahren müssen aber systematisiert und wo nötig ergänzt werden. Die wichtigsten Verfahrensetappen müssen auf Verordnungsebene behördenübergreifend vereinheitlicht werden. Das Sicherheitsverfahren muss insbesondere die sicherheitsmässigen Aufgaben, Kompetenzen und Verantwortungen derjenigen Stellen festlegen, die den Einsatz von Informatikmitteln planen und beschliessen. Absatz 2 führt einige Eckpunkte des Verfahrens auf:

– Buchstabe a: Informatikmittel werden für bestimmte Zwecke und für eine geplante Lebensdauer eingesetzt. Der erste Schritt in Bezug auf die Umsetzung der Informationssicherheit besteht darin, bei der Bestimmung des Einsatzzwecks des Informatikmittels die Geschäftsprozesse zu bestimmen, die mit dem einzusetzenden Informatikmittel unterstützt werden sollen, sowie die Informationen zu identifizieren, die damit bearbeitet werden sollen. Zu diesem Zeitpunkt – also in der Planungsphase – muss die Leistungsbezügerin den Schutzbedarf der Informationen nach Artikel 6 Absatz 1 erheben sowie die potenziellen Auswirkungen einer Störung oder eines Missbrauchs des einzusetzenden Informatikmittels auf die Interessen nach Artikel 1 Absatz 2 beurteilen. Es handelt sich dabei grundsätzlich um eine sogenannte *Business Impact Analyse*, die zwingend von der für den Geschäftsprozess verantwortlichen Stelle durchgeführt werden muss. Bei der Beurteilung des Schutzbedarfs muss auch berücksichtigt werden, dass Informatikmittel in der Regel in einer bestimmten technischen und logischen Umgebung (sog. Architektur) vernetzt und betrieben werden. Die frühzeitige Identifizierung von Vernetzungen und Abhängigkeiten hilft auch, die Massnahmen dort umzusetzen, wo sie am wirksamsten sind. Aus der Schutzbedarfsanalyse

ergeben sich die Anforderungen an den Schutz der Informationen sowie die Sicherheitseinstufung des Informatikmittels nach Artikel 17.

- Buchstabe b: Die verpflichteten Behörden haben festzulegen, welche Massnahmen umgesetzt werden müssen (s. auch Art. 18) und wie die Umsetzung dieser Massnahmen zu prüfen ist. Grundsätzlich sollen standardisierte Massnahmen zur Anwendung kommen (s. Art. 86). Die Überprüfung der Umsetzung der Massnahmen ist in diesem Zusammenhang besonders wichtig. So sollte die zuständige Behörde oder Organisation vor dem Einsatz eines Informatikmittels einen Beleg dafür haben, dass das Sicherheitsverfahren rechtmässig stattgefunden hat und die erforderlichen Massnahmen tatsächlich umgesetzt wurden (Konformität).
- Buchstabe c: Informatikmittel werden regelmässig in Betrieb genommen, ohne dass der Bedarf an Informationssicherheit abgedeckt wird. Mit der Sicherheitsfreigabe soll sichergestellt werden, dass die zuständige Behörde oder Organisation vor dem Einsatz eines Informatikmittels die identifizierten Restrisiken kennt und auch bereit ist, diese zu tragen. Ist sie der Meinung, die Restrisiken seien noch zu hoch, kann sie die Freigabe verweigern und die Umsetzung ergänzender risikomindernder Massnahmen verlangen.
- Buchstabe d: Informationssicherheit verändert sich kontinuierlich. Die Behörden müssen deshalb ein Vorgehen festlegen, um eine Veränderung der Risiken bei bereits eingesetzten Informatikmitteln zu berücksichtigen.

Nach Absatz 3 obliegt die Zuständigkeit für die Durchführung des Sicherheitsverfahrens derjenigen Behörde oder Organisation, die den Einsatz von Informatikmitteln beschliesst (Leistungsbezügerin). Die Leistungsbezügerin ist nämlich für die Geschäftsprozesse sowie für die Umsetzung der Sicherheitsanforderungen verantwortlich. Sie muss deshalb ihre Geschäfts- und Sicherheitsanforderungen ihrer Leistungserbringerin, welche die Informatikmittel betreibt, klar kommunizieren.

Art. 17 Sicherheitsstufen

Die Sicherheitseinstufung dient zur Identifizierung der Kritikalität eines bestimmten Informatikmittels in Bezug auf die öffentlichen Interessen nach Artikel 1 Absatz 2. Diese Kritikalität wird von der Schwere des Schadens abgeleitet, der verursacht werden kann, wenn die Informationen, die mit dem betroffenen Informatikmittel bearbeitet werden, oder das Informatikmittel selber missbraucht oder gestört werden. Massgebend für die Einstufung sind entsprechend sowohl der Schutzbedarf von Informationen in Bezug auf die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit als auch die Kritikalität einer zeitnahen und sachgemässen Erfüllung der Geschäftsprozesse, die mit dem Informatikmittel unterstützt werden. Für die Beurteilung der Schwere des Schadens kann *mutatis mutandis* auf die Erläuterungen zu Artikel 13 verwiesen werden.

Die geltenden Vorschriften der Bundesverwaltung sehen nur zwei Stufen vor: einen generellen Schutzbedarf und einen erhöhten Schutzbedarf. Das neue Einstufungsmodell mit drei Stufen orientiert sich am Standard des Deutschen Bundesamts für Sicherheit in der Informationstechnik:

- Die Sicherheitsstufe «Grundschutz» gilt für alle Informatikmittel, die keine besonderen Schutzanforderungen aufweisen. Die grosse Mehrheit der Systeme des Bundes soll dieser Sicherheitsstufe zugeordnet werden. Personendaten, «intern» klassifizierte Informationen sowie weitere Informationen, die zwar in Bezug auf ihre Vertraulichkeit geschützt werden müssen, aber nicht einen hohen Schutz benötigen, können mit so eingestuften Mitteln bearbeitet werden.
- In die Sicherheitsstufe «hoher Schutz» gehören Informatikmittel, wenn ein Missbrauch der Informationen, die damit bearbeitet werden, oder des Informatikmittels selbst einen erheblichen Schaden zufügen kann. Informatikmittel, mit welchen «vertraulich» klassifizierte Informationen bearbeitet werden sollen, gehören in diese Stufe. Dies trifft auch für Informatikmittel zu, die für die Bearbeitung von besonders schützenswerten Personendaten oder von Geschäfts- oder Fabrikationsgeheimnissen benützt werden, sofern der potenzielle Schaden bei einem Missbrauch dieser Daten erheblich ist. Werden mit einem Informatikmittel Geschäftsprozesse unterstützt, deren Ausfall oder Störung zu einer erheblichen Beeinträchtigung der Handlungsfähigkeit einer Behörde führen kann, so ist das Informatikmittel ebenfalls dieser Sicherheitsstufe zuzuweisen.
- In die Sicherheitsstufe «sehr hoher Schutz» gehören Informatikmittel, wenn ein Missbrauch der Informationen, die damit bearbeitet werden, oder des Informatikmittels selbst einen *schwerwiegenden* Schaden zufügen kann. Es geht hier um Informatikmittel, deren Ausfall oder Störung den Interessen nach Artikel 1 Absatz 2 schwerwiegend beeinträchtigen kann (s. auch Art. 10 Abs. 2), oder solche, mit welchen «geheime» Informationen bearbeitet werden.

Die Zuweisung zu einer Sicherheitsstufe gibt auch vor, welche Sicherheitsanforderungen gelten und wie die Schutzmassnahmen definiert werden müssen. Für jede Sicherheitsstufe sollen in Bezug auf den Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit standardisierte Sicherheitsanforderungen und -massnahmen gelten (Art. 86). Die Standardisierung ist für einen effizienten und sicheren behördenübergreifenden Informationsaustausch zwingend notwendig. Sie hat wichtige Vorteile: Vorab werden den Entwicklungs- und Beschaffungsstellen klar zu erfüllende Sicherheitsanforderungen vorgelegt, die sie bei der Implementierung der Sicherheit in die Informatikmittel unterstützen. Sodann werden die Sicherheitskosten in Projekten transparenter und einfacher berechen- und planbar.

Eine Konkordanztabelle (Mapping), die beschreibt, welche Informationen und Geschäftsprozesse zu welcher Sicherheitsstufe gehören, kann zurzeit noch nicht erstellt werden. Die Einstufungskriterien von Artikel 17 sind neu und deshalb in der Praxis noch nicht umgesetzt. Zudem bearbeiten nicht alle Behörden und Organisationen dieselben Informationen, was es verunmöglicht, den tatsächlichen Schutzbedarf der jeweiligen Information *in abstracto* zu beurteilen. Im Rahmen des Vollzugs werden allerdings Informationen und Daten je nach Schutzbedarf ein bestimmtes *Schutzniveau* in Bezug auf die Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit zugewiesen werden. Die Schutzniveaus werden mittels Konkordanztabellen zur nötigen Standardisierung der Massnahmen dienen.

Art. 18 Sicherheitsmassnahmen

Die verpflichteten Behörden müssen für jede Sicherheitsstufe festlegen, welche Sicherheitsanforderungen ihre Informatikmittel erfüllen müssen. Die Praxis hat gezeigt, dass mit einer Anzahl bestimmter und vordefinierter Anforderungen und Massnahmen die Risiken für eine Mehrheit der Informatikmittel auf ein tragbares Mass reduziert werden können. Die Gesamtheit aller solchen Anforderungen und Massnahmen bildet den *Grundschutz*. Der Vorteil eines definierten und standardisierten Grundschutzes besteht darin, dass die Behörden und Organisationen für Informatikmittel dieser Stufe keine detaillierten und aufwendigen Risikobeurteilungen durchführen müssen. Der Grundschutz wird somit auch als Fundament definiert, auf welches Informatikmittel der Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz» aufbauen müssen. Die Massnahmen des Grundschutzes müssen relativ flexibel und modular ausgestaltet werden. Sind bestimmte Massnahmen bei einem besonderen Informatikmittel nicht umsetzbar, so müssen andere Massnahmen zur Anwendung kommen, die einen gleichwertigen Schutz ermöglichen.

Für die Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz» genügen die Anforderungen und Massnahmen des Grundschutzes oft nicht. Heute wird deshalb für solche Mittel zuerst eine objektbezogene Risikoanalyse durchgeführt. Das Schwergewicht liegt dabei auf dem Schutz derjenigen Kriterien, welche erhöhte Schutzanforderungen haben. Wenn einem Informatikmittel aufgrund erhöhter Anforderungen an die Verfügbarkeit die Stufe «hoher Schutz» zugeordnet wird, es aber gleichzeitig keine erhöhten Anforderungen an den Schutz der Vertraulichkeit aufweist, dann müssen in erster Linie die Risiken für die Verfügbarkeit beurteilt werden. Gestützt auf diese Risikoanalyse wird heute ein Informationssicherheits- und Datenschutzkonzept erstellt, das die Umsetzung der Grundschutzmassnahmen attestiert und die zusätzlichen Sicherheitsmassnahmen beschreibt.

Am heutigen System (Risikoanalyse und Sicherheitskonzept) soll für Informatikmittel der beiden höheren Sicherheitsstufen festgehalten werden. Das Gesetz schreibt dies dennoch nicht vor und lässt somit die Tür offen für eine andere Lösung.

Die Wirksamkeitsprüfung nach Absatz 3 ist die einzige Massnahme, mit welcher die tatsächlich gewährleistete Informationssicherheit gemessen werden kann. Das Informatikmittel wird detailliert auditiert. Es können zudem echte Angriffe ausgeführt werden, um allfällige Sicherheitslücken und ausnutzbare Schwachstellen zu identifizieren (z. B. mittels Penetrationstests). Die Wirksamkeitsprüfung wird nur für die kritischsten Informatikmittel verlangt, weil sie mit einem nicht unerheblichen finanziellen Aufwand verbunden ist (0,5 bis 2 % der gesamten Investitionskosten).

Art. 19 Sicherheit beim Betrieb

Die Hauptverantwortung für die Sicherheit beim Einsatz von Informatikmitteln liegt nach den Artikeln 16–18 bei den Leistungsbezügerinnen. Die Leistungserbringerinnen sind ihrerseits dafür zuständig, beim Betrieb dieser Informatikmittel die Sicherheit nach dem Stand der Wissenschaft und Technik zu gewährleisten. Sie müssen die Anforderungen und Massnahmen nach diesem Gesetz sowie die vereinbarten zusätzlichen Anforderungen der Leistungsbezügerinnen berücksichtigen und umsetzen. Die internen Leistungserbringerinnen fallen alle unter den Anwendungsbereich

dieses Gesetzes und müssen es deshalb für ihre Tätigkeiten anwenden. Externe Leistungserbringerinnen dagegen gelten als Dritte im Sinne von Artikel 9 und müssen vertraglich verpflichtet werden, die Massnahmen dieses Gesetzes einzuhalten.

Jede Leistungserbringerin steht in der Pflicht, seine Netzwerke zu überwachen. Anomalien, Angriffe und Störungen müssen frühzeitig entdeckt und beurteilt werden, um darauf reagieren zu können. Bei Verdacht auf Gefährdung oder bei konkreten Verletzungen der Informationssicherheit kann es vorkommen, dass die elektronischen Aktivitäten bestimmter interner oder externer Mitarbeitender (oder Maschinen) detailliert geprüft werden müssen. Ist in diesem Zusammenhang die namentliche Identifizierung einer Person erforderlich, dann sind die Vorschriften des RVOG über die Bearbeitung von Personendaten, die im Rahmen der Benutzung der Informatikinfrastruktur anfallen, sinngemäss anwendbar. Die bestehenden sogenannten Forensikprozesse der Bundesverwaltung stützen sich heute bereits auf diesen Bestimmungen, wenn eine personenbezogene Auswertung der Daten erforderlich ist.

4. Abschnitt: Personelle Massnahmen

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

Personen, die Zugang zu Informationen, Informatikmitteln oder Infrastrukturen des Bundes haben, müssen bestimmte Anforderungen erfüllen. Es liegt in der Verantwortung des Arbeit- beziehungsweise des Auftraggebers, dafür zu sorgen, dass die Arbeit- bzw. Auftragnehmerinnen und -nehmer diese Anforderungen erfüllen.

- Bei der Auswahl der anzustellenden oder zu beauftragenden Personen müssen die Auswahlkriterien dem Schutzbedarf der Informationen beziehungsweise der Kritikalität der Informatikmittel entsprechen. Die Arbeitgeber sind für ihre Personalentscheide verantwortlich. Die Unterstellung einer Person unter die PSP entbindet sie nicht von dieser Verantwortung.
- Die Verwaltung des Zugangs zu Informationssystemen, Räumlichkeiten und Infrastrukturen erfolgt zunehmend elektronisch. Personen, die auf Ressourcen des Bundes zugreifen wollen, müssen sich elektronisch identifizieren lassen (Authentisierung), damit über ihre Zugangsberechtigung entschieden werden kann. Je nach Kritikalität des Zugangs werden stärkere oder schwächere Authentisierungssysteme eingesetzt. Beispielsweise wird zusätzlich zu einem Passwort eine Smartcard oder die Überprüfung eines biologischen Merkmals (Fingerabdruck, Augenscan usw.) verlangt.
- Die verpflichteten Behörden und Organisationen müssen ihre Angestellten und Auftragnehmer ausreichend ausbilden. Im Bereich der Informationssicherheit genügt eine einmalige Ausbildung nicht. Die Arbeit- und Auftragnehmerinnen und -nehmer müssen regelmässig geschult und sensibilisiert werden. Besondere Aufmerksamkeit ist der Schulung der Vorgesetzten sowie derjenigen Personen, die eine sicherheitsempfindliche Tätigkeit ausüben, zu schenken.

– Angestellte des Bundes müssen aufgrund der Artikel 22 BPG und 320 StGB das Amtsgeheimnis wahren. Bei Dritten, die für den Bund Aufträge ausführen sollen, muss die Geheimhaltungspflicht schriftlich im Vertrag festgehalten werden und bei ihrer Nichteinhaltung mit klaren Folgen verbunden sein, weil diese Dritten nicht unter den Anwendungsbereich von Artikel 320 StGB fallen. Es ist weiter darauf hinzuweisen, dass eine vertraglich vereinbarte Geheimhaltungspflicht den offenbarenden Beamten nicht zu rechtfertigen vermag, wenn die schriftliche Einwilligung der vorgesetzten Stelle nach Artikel 320 Absatz 2 StGB intern nicht vorliegt. Betreffend Amtsgeheimnisverletzung: Vgl. Erläuterungen zur Änderung von Artikel 320 StGB.

Die Verwendung von biometrischen Verifikationsmethoden zur Authentisierung von Personen kann zusätzliche Sicherheit bringen. Dabei geht es nicht darum, eine Person aus einer beliebigen Anzahl Personen zu identifizieren, sondern nur darum zu prüfen, ob eine bestimmte Person, die Zugang zu Ressourcen des Bundes verlangt, wirklich diejenige ist, die sie zu sein behauptet. Die verpflichteten Behörden sollen von dieser Möglichkeit für den Zugang zu ihren Ressourcen Gebrauch machen können. Sie kommen heute in gewissen Bereichen bereits zum Einsatz. Aus Datenschutzgründen sind die biometrischen Daten nach Wegfall der Zugangsberechtigung zwingend zu vernichten.

Art. 21 Restriktive Erteilung von Berechtigungen

Artikel 21 stellt einen zentralen Grundsatz der Informationssicherheit auf. Wer für eine Bundesbehörde arbeitet oder einen Auftrag ausführt, braucht zur Aufgabenerfüllung unter Umständen einen Zugang zu bestimmten Informationen, Informatikmitteln oder Räumlichkeiten. Die Arbeit- und Auftragnehmerinnen und -nehmer sollen nur diejenigen Berechtigungen erhalten, die sie zur Erfüllung ihrer Aufgaben tatsächlich benötigen. Das Risiko eines Missbrauchs kann wesentlich reduziert werden, wenn eine Person nicht ohne Grund Informationen eines anderen Bereichs bearbeiten kann. Es kommt vor, dass ehemalige Angestellte oder Auftragnehmerinnen und Auftragnehmer nach Beendigung des Arbeitsverhältnisses, des Vertrags oder einer besonderen Aufgabe nicht aufgefordert werden, ihren Schlüssel oder ihren Badge zurückzugeben, oder dass ihr Benutzerkonto nicht gesperrt wird. Solche *ungültige* Berechtigungen können in der Folge benutzt werden, um gegen die Interessen des Arbeit- oder Auftraggebers zu handeln. Wenn eine Anstellung, ein Vertrag oder eine Aufgabe beendet ist, müssen die entsprechenden Berechtigungen entzogen werden. Besteht Grund zur Annahme, dass eine Gefährdung der Informationssicherheit vorliegt, müssen die Berechtigungen sofort gesperrt oder entzogen werden. Beide Massnahmen sollen insbesondere dazu beitragen, das Risiko einer Innentat zu reduzieren.

5. Abschnitt: Physischer Schutz

Art. 22 Grundsatz

Bei den physischen Schutzmassnahmen geht es darum, die Risiken durch physische Bedrohungen zu reduzieren. Zu diesen Risiken gehören unter anderem menschliche Handlungen (z. B. Spionage, Diebstahl, Vandalismus oder Sabotage). Dazu gehören aber auch Elementarschäden (z. B. Hitze, Feuer, Wasser, Staub, Vibrationen usw.). Artikel 22 legt den Grundsatz fest, dass die verpflichteten Behörden und Organisationen den physischen Schutz ihrer Informationen und Informatikmittel gewährleisten müssen. Zu verhindern ist insbesondere der unberechtigte Zugang zu den Informationen oder Informatikmitteln etwa durch Zugangskontrollen, Videokameras, Schliesssysteme, Sicherheitsbehältnisse, Aktenvernichtungsgeräte usw. Gegen Elementarschäden werden beispielsweise Brandmeldeanlagen und automatische Löschanlagen eingesetzt. Die Massnahmen des physischen Schutzes betreffen sowohl Informationen und Informatikmittel, die sich in den Räumlichkeiten der betroffenen Behörde oder Organisation befinden, als auch solche, die öffentlich zugänglich sind. Es handelt sich beim zweiten Fall einerseits um Informationen und Informatikmittel, die von ihrem üblichen Standort (Büro) mitgenommen werden und die anschliessend – ausserhalb des üblichen Sicherheitsperimeters – geschützt werden müssen. Es handelt sich aber auch um Informationen und Einrichtungen, Verkabelungen und Versorgungsleitungen, die nicht unter der ständigen Kontrolle der Behörde oder Organisation stehen. Besondere Aufmerksamkeit muss beispielsweise Zugangspunkten wie Anlieferungs- und Ladezonen geschenkt werden.

Art. 23 Sicherheitszonen

Die Ausscheidung dieser Räume bzw. Bereiche als Sicherheitszone stellt eine physische Massnahme der Informationssicherheit dar, die bereits heute beim Bund teilweise ergriffen wird, insbesondere zum Schutz von Serverräumen oder von bestimmten Führungsräumen. Eine Sicherheitszone muss vordefiniert werden, identifizierbar sein und entsprechend geschützt werden. Das Ausführungsrecht des Bundesrats wird voraussichtlich zwei Arten von Sicherheitszonen definieren, je nach Kritikalität der Informationen oder Informatikmittel. Die Massnahmen in den Sicherheitszonen der jeweiligen Stufen werden risikogerecht auszugestalten sein. Im Gegensatz zur Gesetzgebung anderer Länder oder internationaler Organisationen sowie zur Gesetzgebung über den Schutz militärischer Anlagen (s. auch Abs. 4) besteht für die verpflichteten Behörden und Organisationen aber keine Pflicht, solche Bereiche als Sicherheitszone zu bezeichnen. Über ihre tatsächliche Einrichtung entscheidet die Behörde oder Organisation nach einer Risikobeurteilung.

Absätze 2 und 3 regeln die besonderen Befugnisse der Behörde oder Organisation, die eine Sicherheitszone einrichtet:

– Das Mitführen bestimmter Gegenstände in eine Sicherheitszone kann eingeschränkt werden. Das Mitführen von Bild- oder Tonaufnahmegeräten (inkl. Smartphones oder Notebooks mit entsprechenden Funktionen) ist in der Regel nur mit besonderer Bewilligung erlaubt.

- Bereiche der Sicherheitszone, die für die Informationssicherheit besonders wichtig sind (z. B. die Zutrittszone zu einem besonderen Serverraum, der Administratorarbeitsplatz oder der Archivraum mit «geheim» klassifizierten Informationen), können mittels Videoaufnahmegeräten überwacht werden.
- Beim Ein- oder Ausgang kann die Behörde oder Organisation Taschen- oder Personenkontrollen durchführen lassen. Damit soll verhindert werden, dass Personen ohne Bewilligung Geräte in die Sicherheitszone mitnehmen oder Informationen (z. B. mit einem USB-Memorystick) entwenden.
- Zur Durchsetzung der Vorschriften sollen auch Bürokontrollen möglich sein. Bei den Bürokontrollen wird unter anderem die Einhaltung der sogenannten *Clean Desk Policy* überprüft (es dürfen keine schutzwürdigen Informationen auf dem Schreibtisch oder anderswo herumliegen, der PC muss gesperrt oder ausgeschaltet sein, Datenträger müssen unter Verschluss gehalten werden, die Schubladen müssen geschlossen sein, der Abfallkorb darf keine klassifizierten Informationen enthalten usw.). Die Kontrolle darf auch in Abwesenheit der betroffenen Personen, beispielsweise während der Nacht, stattfinden.
- Die Behörde oder Organisation kann eine störende Fernmeldeanlage betreiben, wenn die Sicherheitszone besonders kritisch ist. Der tatsächliche Bedarf sowie die Bedingungen für den Betrieb einer solchen Störanlage werden nach dem FMG beurteilt.

6. Abschnitt: Identitätsverwaltungs-Systeme

Art. 24 Einsatz von Identitätsverwaltungs-Systemen

Im Mittelpunkt eines umfassenden Identitätsverwaltungs-Systems stehen zentralisierte Identitätsverwaltungs-Systeme. Die Absätze 1 und 2 beschreiben in groben Zügen den Zweck und die Funktionsweise der zentralen Identitätsverwaltungs-Systeme, um eine Basis für die restlichen Regelungen bereitzustellen. Die verpflichteten Behörden erhalten die Kompetenz, derartige Systeme für die zentrale Kontrolle von Personen, Maschinen und Systemen, die Zugang zu Informationssystemen und anderen Ressourcen verlangen, zu betreiben. Dabei wird absichtlich offen gelassen, wie viele solche zentralen Identitätsverwaltungs-Systeme eingesetzt werden. Für die Bundesverwaltung wird der Bundesrat entscheiden, welche Stellen oder Verwaltungseinheiten solche Systeme betreiben. Es ist beispielweise denkbar, dass für die Bundesverwaltung vorerst mehrere solcher Identitätsverwaltungskreise gebildet werden und dass diese dann mit der Zeit teilweise konsolidiert werden. Für jedes System muss eine verantwortliche Stelle bezeichnet werden. Da es den verpflichteten Behörden überlassen ist, wie viele solche Systeme sie betreiben und wie die entsprechenden Kreise organisiert sind, können die verantwortlichen Stellen im Gesetz nicht genannt werden.

Art. 25 Datenaustausch und -abgleich

Es gibt drei klar unterscheidbare Fälle, bei denen ein Identitätsverwaltungs-System Personendaten mit anderen Systemen austauscht:

- Beim Aufbau eines neuen Identitätsverwaltungs-Systems bezieht dieses die notwendigen Identitätsdaten der Mitarbeitenden des abzudeckenden Bereichs aus den entsprechenden Mitarbeiter- und Benutzerverzeichnissen. Im späteren Betrieb müssen periodisch Mutationen von diesen Systemen an das Identitätsverwaltungs-System gemeldet werden.
- Ein weiterer Anlass ist der Anschluss einer Fachanwendung, die bisher die Authentifizierung der Benutzerinnen und Benutzer selbstständig durchgeführt hat. In diesem Fall werden die für die Authentifikation verwendeten Daten an das zentrale Identitätsverwaltungs-System übertragen und dort in die bestehenden Daten eingetragen. In diesem Moment werden auch die Anforderungen nach Absatz 2 überprüft. Die weiteren Mutationen an den Benutzerdaten werden normalerweise von der Fachanwendung an das Identitätsverwaltungs-System gemeldet. Je nach konkreter organisatorischer Ausgestaltung ist aber für bestimmte Benutzerkreise auch eine zentrale Benutzerverwaltung denkbar.
- Die häufigste Übermittlung von Daten geschieht im laufenden Betrieb bei jeder Anmeldung (Login) einer Benutzerin oder eines Benutzers. Das Identitätsverwaltungs-System authentifiziert die Benutzerin oder den Benutzer, komplettiert die von der Fachanwendung verlangten Identitätsdaten aus seinem Verzeichnis (z. B. die Zugehörigkeit zu einer Amtsstelle) oder aus externen Quellen (z. B. die Funktion als Urkundsperson oder Ärztin/Arzt) und stellt diese Daten der Fachanwendung in der Form von Bestätigungen zur Verfügung, damit diese über die konkreten Zugriffsberechtigungen befinden kann.

Art. 26 Verwendung der AHV-Versichertennummer

Für ein Identitätsverwaltungs-System ist es unumgänglich, dass die zu erfassenden Personen fehlerfrei identifiziert werden. Keine Person darf wegen der Übereinstimmung von Erkennungsmerkmalen mit einer anderen verwechselt oder gar – im Bereich der Daten – zusammengeführt werden. Es darf aber auch keine Person wegen nicht erkannter Übereinstimmung doppelt geführt werden. Dieses Problem stellt sich sowohl beim Aufbau und der Nachführung des Benutzerverzeichnisses, wie auch beim einzelnen Zugriff bzw. bei der Weitermeldung der zugreifenden Person vom Identitätsverwaltungs-System zur Fachanwendung. Der beste verfügbare Personenidentifikator für eine solche fehlerfreie Identifizierung ist die AHV-Versichertennummer nach Artikel 50*c* AHVG. Sie deckt fast alle in den hier vorgesehenen Identitätsverwaltungs-Systemen vorkommenden Personen ab. Artikel 50*e* Absatz 1 AHVG verlangt für die systematische Verwendung der AHV-Versichertennummer ausserhalb der Sozialversicherung des Bundes eine formellgesetzliche Regelung von Verwendungszweck und Nutzungsberechtigten.

Für die Kommunikation zwischen dem Identitätsverwaltungs-System und den Fachanwendungen oder anderen Ressourcen wird auf die AHV-Versichertennummer

verzichtet. Sie lässt sich hier ohne übermässige Einschränkungen oder Mehrkosten durch sektorielle Personenidentifikatoren ersetzen. Bei der Pflege des Benutzerverzeichnisses der Identitätsverwaltungs-Systeme, sei es bei der Datenübernahme aus Mitarbeiter- und Benutzerverzeichnissen, beim Anschluss von bisher autonomen Fachanwendungen oder bei der direkten Eingabe von neuen Benutzerinnen und Benutzern, soll hingegen die AHV-Versichertennummer *temporär* für die Gewährleistung einer fehlerfreien Zuordnung verwendet werden. Für diesen Vergleich wird aus der AHV- Versichertennummer mit einem nicht umkehrbaren Verfahren ein spezifischer, sektorieller Personenidentifikator gebildet. Dieser abgeleitete Personenidentifikator wird einerseits für den Vergleich verwendet und andererseits im Identitätsverwaltungs-System für spätere Abgleiche gespeichert. Mit diesem Verfahren kann die Qualität der Daten der Identitätsverwaltungs-Systeme auf einem hohen Niveau gehalten werden, was sonst nur mit unverhältnismässig grossem Aufwand möglich wäre. Zudem ist die Verwendung der AHV- Versichertennummer gleich mehrfach eingeschränkt:

- Sie kann nur verwendet werden, wenn das Daten liefernde System selbst die AHV- Versichertennummer enthält, bzw. führen darf.
- Sie wird nur kurzfristig für die Ableitung verwendet und im Identitätsverwaltungs-System nicht gespeichert.
- Sie wird nur bei der Übernahme oder Registrierung von neuen Personen verwendet, also sozusagen nur ausserhalb des Identitätsverwaltungs-Systems.

Wenn sich in einem konkreten Fall ein einfacherer Weg für einen sicheren Abgleich anbietet, beispielsweise eine interne Personalnummer, wird selbstverständlich ebenfalls auf die Verwendung der AHV- Versichertennummer verzichtet. Bei Bedarf können solche Fälle auf Verordnungsstufe festgelegt werden.

Art. 27 Ausführungsbestimmungen

Den verpflichteten Behörden werden Auftrag und Kompetenz erteilt, den Einsatz der Identitätsverwaltungs-Systeme in Ausführungsbestimmungen umfassend zu regeln.

3. Kapitel: Personensicherheitsprüfungen

1. Abschnitt: Allgemeine Bestimmungen

Art. 28 Prüfzweck und Prüfungsinhalt

Die PSP ist eine vorbeugende Massnahme zum Schutz vor «Innentäterinnen» und «Innentätern». Sie soll das Risiko einer Beeinträchtigung der Interessen nach Artikel 1 Absatz 2 identifizieren, das mit der Ausübung einer sicherheitsempfindlichen Tätigkeit durch eine bestimmte Person verbunden sein könnte. Es geht also darum, die Wahrscheinlichkeit einzuschätzen, dass eine bestimmte Person vorsätzlich oder fahrlässig die Informationssicherheit des Bundes verletzen wird. Dafür werden Daten über die Lebensführung dieser Person erhoben. Gestützt darauf wird eine Beurteilung des Risikos vorgenommen bzw. eine Prognose über ungewisse künftige

Sachverhalte gestellt. Die Risikobetrachtung basiert nicht nur auf *harten* Fakten, vielmehr liegt es in der Natur der Sache, dass die aus den erhobenen Daten gezogenen Schlussfolgerungen auch Annahmen und Vermutungen sein können (s. auch Urteil des Bundesverwaltungsgerichts A-5617/2013 vom 25. März 2013, Erwägung 3.4). Nachdem sie von der Beurteilung des Risikos durch die zuständige Fachstelle PSP Kenntnis genommen hat, entscheidet allein die verpflichtete Behörde oder Organisation, ob sie ein allfälliges erhöhtes Risiko tragen, ob sie dieses mit bestimmten Auflagen reduzieren oder ob sie es durch Nichtanstellung oder Kündigung vermeiden will.

In den Absätzen 2 und 3 werden im Allgemeinen der Prüfungsinhalt sowie die entsprechenden Schranken festgehalten, das heisst, welche Daten zur Beurteilung des Risikos bearbeitet werden dürfen sowie welche Daten zum Schutz der Persönlichkeitsrechte der zu prüfenden Personen grundsätzlich nicht bearbeitet werden dürfen. Die Praxis hat gezeigt, dass ein beispielhafter Katalog an *sicherheitsrelevanten* Daten ein wertvolles Auslegeinstrument zum materiellen Inhalt der PSP liefert. Oft hat eine Gefährdung oder Verletzung der Informationssicherheit durch eine bestimmte Person einen Ausgangspunkt, der zeitlich zurückliegt und auf bestimmte persönliche Umstände zurückzuführen ist. Persönliche, insbesondere finanzielle Schwierigkeiten oder auf Auslandreisen geknüpfte, jedoch von der Person in der Schweiz verheimlichte Beziehungen können unter Umständen Situationen schaffen, die dem Staat erheblichen Schaden zufügen. Deshalb wird im Rahmen der PSP die *Lebensführung* der zu prüfenden Person unter die Lupe genommen. Der in Absatz 2 aufgeführte Katalog der Daten über die Lebensführung ist nicht abschliessend und entspricht inhaltlich dem ersten Satz von Artikel 20 Absatz 1 BWIS. Der darin enthaltene Verweis auf «Aktivitäten, welche die innere oder die äussere Sicherheit in rechtswidriger Weise gefährden können» wird jedoch gestrichen: Einerseits sind solche Aktivitäten bereits vom Oberbegriff *Lebensführung* erfasst; andererseits wird für die Erhebung dieser Daten auch eine Bedingung gesetzt (dass diese Aktivitäten die Sicherheit rechtswidrig gefährden können), die erst im Rahmen der Beurteilung des Sicherheitsrisikos festgestellt werden kann. Im Vergleich zum geltenden Recht werden die Datenerhebungsrechte der Fachstellen PSP durch diese Streichung nicht weiter eingeschränkt. Die Schranken nach den heutigen Artikeln 3 Absatz 1 sowie 20 Absatz 1 zweiter Satz BWIS bleiben allerdings bestehen.

Art. 29 Funktionenliste

Artikel 29 regelt in Verbindung mit Artikel 30, bei welchen Personen eine PSP durchzuführen ist. Die verpflichteten Behörden (nicht die Organisationen) müssen für ihren Bereich eine Liste derjenigen Funktionen erlassen, welche die Ausübung einer sicherheitsempfindlichen Tätigkeit *erfordern* und deren Funktionsträgerinnen und Funktionsträger somit geprüft werden müssen. In Bezug auf die materiellen Voraussetzungen für den Eintrag einer Funktion in die Funktionsliste wird aber nicht einfach das heutige System übernommen. Vom Kriterium der *Regelmässigkeit*, insbesondere bei der Bearbeitung von klassifizierten Informationen, wird abgesehen (s. Ziff. 1.2.5). Entscheidend für die Unterstellung der Bundesangestellten und Angehörigen der Armee unter die PSP ist vielmehr die Frage, ob die Inhaberin oder der Inhaber einer bestimmten Funktion zur Erfüllung ihrer oder seiner Aufgaben

eine sicherheitsempfindliche Tätigkeit ausüben *muss*. Wenn eine solche Tätigkeit für die funktionsbedingte Aufgabenerfüllung *erforderlich* ist, dann – und nur dann – muss die Funktion in die Liste der zu prüfenden Funktionen aufgenommen werden.

Einige fiktive Beispiele vermögen die Umsetzung des Prinzips zu erläutern:

- Eine Mitarbeiterin des Bundesamts für Umwelt ist im Rahmen ihrer Aufgaben für die Umweltverträglichkeitsprüfung im Zusammenhang mit militärischen Bauten und Anlagen zuständig. Im Rahmen ihrer Aufgaben muss sie klassifizierte Informationen ab Stufe «vertraulich» bearbeiten und manchmal Zugang zu Schutzzonen 2 von militärischen Anlagen haben. Ihre Funktion muss in die Funktionsliste aufgenommen werden.
- Ein Mitarbeiter der EFV muss ausnahmsweise die Auswirkungen eines «vertraulich» klassifizierten Antrags an den Bundesrat beurteilen. Für solche Geschäfte sind normalerweise andere Mitarbeitende zuständig, die aber ferien- oder krankheitshalber abwesend sind. Diese Aufgabe gehört grundsätzlich nicht zu seiner Funktion, die dementsprechend nicht auf der Liste aufgeführt werden darf.
- Das Reinigungspersonal einer Behörde hat hin und wieder ungewollten Zugang zu klassifizierten Informationen, wenn es im Rahmen seiner ordentlichen Aufgaben die Büros der Bundesangestellten reinigt und letztere die Informationsträgerinnen und Informationsträger nicht vorschriftsgemäss aufbewahren oder vernichten. Es gehört aber nicht zum Aufgabenbereich des Reinigungspersonals, klassifizierte Informationen zu bearbeiten. Es darf deshalb nicht in die Liste aufgenommen werden, es sei denn, es sei für die Reinigung innerhalb einer Sicherheitszone zuständig.

Das Kriterium der *Regelmässigkeit*, auch wenn es *de facto* fast immer erfüllt sein wird, ist *de iure* irrelevant. Selbst wenn im Stellenbeschrieb nur fünf Prozent des Arbeitspensums für die Erfüllung sicherheitsempfindlicher Aufgaben vorgesehen sind, soll diese Funktion in die Liste aufgenommen werden. Dies auch dann, wenn die betroffene Funktionsinhaberin vielleicht während einer längeren Periode gar keine solchen Aufgaben erfüllen muss. Die *Eventualität* der funktionsbedingten Ausübung einer sicherheitsempfindlichen Tätigkeit ist hingegen kein Grund dafür, eine Funktion in die Funktionsliste aufzunehmen.

Die Umsetzung dieses restriktiven Ansatzes setzt voraus, dass die verpflichteten Behörden und Organisationen eine klare Übersicht über die internen und übergreifenden Geschäftsprozesse und Aufgabenbereiche haben, die notwendigerweise mit sicherheitsempfindlichen Tätigkeiten verbunden sind. Sich in diesem Bereich einen Überblick zu verschaffen und diesen zu behalten, stellt gleichzeitig eine grundsätzliche Massnahme im Bereich des Risikomanagements der Informationssicherheit dar. Die Gründe für den Eintrag einer Funktion in die Funktionsliste sollen nachweisbar sein: Die Stellenbeschreibungen der jeweiligen Funktionen sollen eine genaue Umschreibung der Aufgaben beinhalten, welche die Ausübung einer sicherheitsempfindlichen Tätigkeit erfordern. Zudem sollen die verpflichteten Behörden und Organisationen unabhängig von einer allfälligen Unterstellung unter die PSP die erforderlichen Massnahmen treffen, um den Kreis der Personen, die sicherheitsempfindliche Tätigkeiten ausüben müssen, auf das notwendige Minimum zu beschränken.

Mit dem Begriff *erlassen* wird klargestellt, dass es sich um eine formelle Rechtsetzungsdelegation an die verpflichteten Behörden handelt. Die Funktionslisten werden somit in Verordnungen oder Reglementen zu finden sein. In Bezug auf die Bundesverwaltung soll grundsätzlich am heutigen System festgehalten werden. Aufgrund der Zuständigkeitsregelungen gemäss RVOG kann der Bundesrat weiterhin die Departemente und die BK ermächtigen, ihre eigenen, detaillierten Listen zu erlassen.

Absatz 2: Einzig die verpflichteten Behörden sind nach Absatz 1 für die Beurteilung der Sicherheitsempfindlichkeit der Funktionen verantwortlich. Für die Fachstellen PSP sind die Funktionenlisten grundsätzlich verbindlich. Sie können nicht bei jeder eingeleiteten PSP prüfen, ob die Funktion tatsächlich sicherheitsempfindlich ist. Der damit verbundene Aufwand wäre unverhältnismässig. Es muss also sichergestellt werden, dass die verpflichteten Behörden die Aktualität der Funktionenlisten und damit die Übereinstimmung der aufgelisteten Funktionen mit ihrer tatsächlichen Sicherheitsempfindlichkeit gewährleisten.

Art. 30 Zu prüfende Personen

Die Absätze 1–3 legen fest, wer geprüft werden muss. Die Voraussetzungen für die Durchführung der PSP im internationalen Verhältnis werden durch die entsprechenden völkerrechtlichen Verträge geregelt. Der Grundsatz von Absatz 1 Buchstabe c gilt auch für Personen, die im Auftrag einer ausländischen Behörde oder einer internationalen Organisation eine sicherheitsempfindliche Tätigkeit ausüben sollen. Falls eine Funktion die Kriterien nach Artikel 29 erfüllt, aber noch nicht in die entsprechende Liste aufgenommen wurde, kann die Prüfung durchgeführt werden, sofern die verpflichtete Behörde zustimmt. Für die Bundesverwaltung kann der Bundesrat die Entscheidkompetenz für die Ausnahmeprüfung an die betreffende Departementsvorsteherin oder den betreffenden Departementsvorsteher delegieren. Die Liste muss danach angepasst werden. Mitglieder von Behörden, die vom Volk oder als Magistratspersonen von der Bundesversammlung gewählt werden, werden grundsätzlich für die Ausübung dieser Funktion nicht geprüft, auch wenn diese Personen im Rahmen ihrer Funktion oft die sicherheitsempfindlichsten Tätigkeiten ausüben. Diese Ausnahme ist jedoch nur auf die Funktion bezogen und entsprechend als relativ zu betrachten: Ist beispielsweise ein Mitglied der Bundesversammlung wehrpflichtig und muss es im Zusammenhang mit seiner militärischen Funktion eine sicherheitsempfindliche Tätigkeit ausüben, dann muss eine PSP durchgeführt werden. Obschon sie nicht ausdrücklich erwähnt sind, werden Magistratinnen und Magistraten, die bei den Kantonen die Funktion der Kanzlerin oder des Kanzlers wahrnehmen, auch nicht geprüft.

Art. 31 Prüfstufen

In Bezug auf die Prüfstufen enthält das BWIS keine Regelung. Das Legalitätsprinzip verlangt aber aufgrund des mit der Durchführung der PSP verbundenen tiefen Eingriffs in die Grundrechte der zu prüfenden Personen, dass die wichtigsten Modalitäten des Eingriffs auf Gesetzessebene festgehalten werden. Da die Prüfstufen für die Schwere des Eingriffs massgebend sind, müssen sie im Gesetz geregelt werden. Die Vorlage sieht neu (s. Ziff. 1.2.5) die folgenden zwei Prüfstufen vor:

– Die Grundsicherheitsprüfung gilt für sicherheitsempfindliche Tätigkeiten, bei deren vorschriftswidriger oder unsachgemässer Ausübung die Interessen nach Art. 1 Abs. 2 erheblich beeinträchtigt werden können. Es handelt sich also aufgrund des erwähnten Schadenspotenzials implizit um: (a) die Bearbeitung von «vertraulich» klassifizierten Informationen; (b) die Verwaltung, den Betrieb, die Überprüfung oder die Wartung von Informatikmitteln der Sicherheitsstufe «hoher Schutz»; und (c) den Zugang zu Sicherheitszonen, in welchen Tätigkeiten nach (a) und (b) ausgeübt werden. Für den Zugang zu Schutzzonen 2 einer militärischen Anlage ist ebenfalls eine PSP dieser Stufe erforderlich.
– Die erweiterte PSP gilt entsprechend für (a) die Bearbeitung von «geheim» klassifizierten Informationen; (b) die Verwaltung, den Betrieb, die Überprüfung oder die Wartung von Informatikmitteln der Sicherheitsstufe «sehr hoher Schutz»; und (c) den Zugang zu Sicherheitszonen, in welchen Tätigkeiten nach (a) und (b) ausgeübt werden. Für den Zugang zu Schutzzonen 3 einer militärischen Anlage ist ebenfalls eine PSP dieser Stufe erforderlich.

Massgebend für die Festlegung der Prüfstufe ist nur die tatsächliche Sicherheitsempfindlichkeit der betroffenen Funktion. Es obliegt den verpflichteten Behörden, die Prüfstufen für die entsprechenden Funktionen und Aufträge festzulegen und dafür zu sorgen, dass bei gleicher Sicherheitsempfindlichkeit externe Mitarbeitende auf derselben Prüfstufe wie interne Mitarbeitende des Bundes geprüft werden (s. Ziff. 1.1.4). Die Beurteilung durch die Linie ist für die Fachstellen PSP grundsätzlich verbindlich. Die Fachstellen PSP erheben die Daten für die verlangte Prüfstufe (Art. 35) und wenden für die Beurteilung des Risikos den Massstab der entsprechenden Prüfstufe an. Da der potenzielle Schaden, der die Durchführung einer erweiterten PSP zu rechtfertigen vermag, wesentlich höher ist als bei einer Grundsicherheitsprüfung, begründen gleiche Vorkommisse bei einer erweiterten PSP eher ein Sicherheitsrisiko als bei einer Grundsicherheitsprüfung.

2. Abschnitt: Durchführung

Art. 32 Zuständige Stellen

Absatz 1 erteilt den verpflichteten Behörden sowie den Kantonen eine formelle Kompetenz zur Festlegung der Zuständigkeiten für die Einleitung des Verfahrens und für den Entscheid über die Ausübung der sicherheitsempfindlichen Tätigkeit:

– Die Fachstellen PSP können von sich aus keine PSP einleiten und durchführen; sie benötigen immer einen entsprechenden Auftrag. Die verpflichteten Behörden müssen also je für ihren Zuständigkeitsbereich diejenigen Stellen bezeichnen, die zur Einleitung der Prüfung und der entsprechenden Auftragserteilung an die Fachstellen PSP ermächtigt sind. In der Regel ist dafür der Personaldienst zuständig, aber in manchen Verwaltungseinheiten wurde die Kompetenz anderen Funktionsträgern (z. B. den Informationssicherheitsbeauftragten) erteilt. Der Bundesrat kann auch, soweit er dies für zweckmässig erachtet, bestimmte Dritte zur Einleitung von PSP ermächti-

gen. Dies betrifft insbesondere Betriebe, die häufig sicherheitsempfindliche Tätigkeiten für den Bund ausüben und im Besitz einer BSE nach Artikel 62 sind.

– Mit der Kompetenz, über die Ausübung der sicherheitsempfindlichen Tätigkeit zu entscheiden, ist zwangsläufig auch die Verantwortung für die Bewältigung eines allfälligen Risikos verbunden. Es handelt sich also grundsätzlich um eine Personalangelegenheit, die den Regeln des Personalrechts untersteht. Abweichungen sind jedoch möglich, insbesondere wenn es darum geht, die Ausübung einer sicherheitsempfindlichen Tätigkeit an Externe zu übertragen. In diesem Zusammenhang ist darauf hinzuweisen, dass die entscheidenden Stellen häufig nicht identisch mit den einleitenden Stellen sind.

Für die Durchführung der Prüfungen setzt der Bundesrat heute zwei Fachstellen PSP ein: Die eine ist beim VBS angesiedelt. Sie ist für die Mehrheit der Prüfungen zuständig. Die andere ist der BK administrativ zugeordnet. Sie prüft das Top-Kader der Bundesverwaltung sowie die Angestellten der anderen Fachstelle PSP. Grundsätzlich sollte am heutigen System festgehalten werden. Es liegt aber in der Zuständigkeit des Bundesrats, über die Organisation und Ansiedlung der Fachstellen zu entscheiden (s. auch Art. 49 Bst. b sowie Stellungnahme des Bundesrats vom 22. April 2009 zur Empfehlung 3 des Berichts der GPK-N vom 28. Nov. 2008[28] über die Umstände der Ernennung von Roland Nef zum Chef der Armee). Die Fachstellen PSP müssen das Risiko für die Informationssicherheit möglichst objektiv, das heisst gestützt auf die erhobenen Daten, sowie nach dem Stand der Wissenschaft und Rechtsprechung beurteilen können. Entsprechend darf sich die Führungslinie nicht in das Prüfverfahren einmischen, ansonsten die Gefahr besteht, dass die PSP für persönliche oder politische Zwecke missbraucht wird. Das ISG hält deshalb fest, dass die Fachstellen PSP in ihrer Beurteilung unabhängig (weisungsungebunden) sind. Dies entspricht geltendem Recht (vgl. Art. 21 Abs. 1 BWIS).

Art. 33 Einwilligung und Mitwirkung

Die Durchführung der PSP erfordert grundsätzlich die ausdrückliche Einwilligung der betroffenen Person. Die Fachstellen PSP haben dabei eine implizite Aufklärungspflicht. In der Praxis wird diese Pflicht wahrgenommen, indem die betroffene Person vor der Prüfung ein Merkblatt erhält, das die rechtlichen Grundlagen der PSP (inkl. Datenerhebung) aufführt und das Prüfverfahren erläutert. Einzig im Bereich der Armee und des Zivilschutzes darf eine PSP ohne Zustimmung der betroffenen Person durchgeführt werden. Diese Ausnahme ist notwendig, weil andernfalls Angehörige der Armee oder des Zivilschutzes sich ihrer Dienstpflicht entziehen könnten, indem sie die Durchführung der Prüfung durch Verweigerung der Einwilligung verhindern würden.

Mit Absatz 3 wird implizit auf Artikel 13 Absatz 1 Buchstabe c VwVG verwiesen. Die entsprechende Rechtsprechung und Lehre sind anwendbar. Im Rahmen der Mitwirkungspflicht hat die zu prüfende Person an der Sachverhaltserhebung mitzu-

28 BBl **2009** 3481

wirken. Diese beinhaltet neben der Auskunftserteilung anlässlich der Befragung auch, weiterführende und für den Zweck der PSP hilfreiche Unterlagen einzureichen. Insbesondere notwendig ist die Mitwirkung zur Abklärung der persönlichen Umstände und Verhältnisse, zu welchen die Fachstellen PSP keine Anhaltspunkte haben und die für sie nicht ohne Weiteres erkennbar sind. Die befragte Person muss ihre Antworten wahrheitsgemäss erteilen. Die ganze Sicherheitsprüfung wäre illusorisch, wenn Fragen nach Alkohol- oder Betäubungsmittelmissbrauch, nach persönlichen Schulden, nach Nebenbeschäftigungen und ähnlichem unter Berufung auf die Grundrechte nicht beantwortet werden müssten und entsprechende Erkenntnisse aufgrund dessen nicht in die Beurteilung des Sicherheitsrisikos einfliessen würden (s. auch Botschaft zum BWIS, BBl *1994* II 1127, hier 1187). Zwar ist es der zu prüfenden Person insbesondere anlässlich der Befragung unbenommen, bestimmte Fragen nicht beantworten zu wollen. Es ist dann aber Aufgabe der Fachstellen, die Auskunftsverweigerung oder auch die Verweigerung, weitere Dokumente einzureichen, zu würdigen, da ein gewisser Spielraum für Fragen zur persönlichen Geheimsphäre bestehen muss. Verweigert die zu prüfende Person die Mitwirkung indes in einem Ausmass, dass eine fachgerechte Beurteilung nicht möglich ist, so stellt die Fachstelle PSP eine Feststellungserklärung (Art. 40 Abs. 1 Bst. d) aus.

Art. 34 Zeitpunkt der Personensicherheitsprüfung

Das geltende Recht (Art. 19 Abs. 3 BWIS) verlangt, dass die PSP durchgeführt wird, bevor das Amt oder die Funktion übertragen oder der Auftrag erteilt wird. Diese (an sich zweckmässige) Regelung kann jedoch in der Praxis nicht umgesetzt werden. Sie würde eine wesentliche Aufstockung der personellen Ressourcen der Fachstellen PSP erfordern. Deshalb wird in Absatz 1 die Regel für Angestellte der verpflichteten Behörden und Organisationen sowie der Kantone abgeschwächt: Es wird nur noch verlangt, dass für diese Personengruppe die PSP eingeleitet wird, bevor die Funktion übertragen wird. Den Arbeitgebern steht es selbstverständlich nach wie vor offen, auf die Erklärung der Fachstelle PSP zu warten, bevor sie die betroffene Person die sicherheitsempfindliche Tätigkeit ausüben lassen. In der Praxis werden sie wohl in der Regel im Arbeitsvertrag eine Klausel einfügen, wonach die Ausstellung einer Sicherheitserklärung mit Vorbehalt, einer Risikoerklärung oder einer Feststellungserklärung (s. Art. 40 Abs. 1 Bst. b–d) einen Grund für den Entzug der Berechtigung zur Ausübung der sicherheitsempfindlichen Tätigkeit oder sogar für eine sofortige Auflösung des Arbeitsverhältnisses darstellen kann. Zur vorläufigen Risikominderung können die Arbeitgeber einen Auszug aus dem Strafregister oder aus dem Betreibungsregister (Art. 20*a* BPG) verlangen.

Für Personen, die vom Bundesrat gewählt werden, entspricht die Regelung bisherigem Recht (Art. 19 Abs. 3 BWIS). Dasselbe gilt für Dritte, die einen sicherheitsempfindlichen Auftrag ausführen sollen: die PSP muss abgeschlossen sein, bevor die Person mit der Ausübung der sicherheitsempfindlichen Tätigkeit betraut werden darf (s. auch Ziff. 1.1.4: Bericht der GPK-S betreffend externe Mitarbeitende der Bundesverwaltung, Empfehlung 6). Der Grund für die unterschiedliche rechtliche Behandlung zwischen den internen Angestellten und den Dritten liegt beim besonderen Verhältnis der Bundesangestellten zum Bund. Von Angehörigen des Bundes kann grundsätzlich von einer erhöhten Loyalität gegenüber den Interessen des Bundes

ausgegangen werden. Zudem arbeiten Angestellte des Bundes meistens direkt beim Arbeitgeber, was eine einfachere Kontrolle ermöglicht.

Auch wenn es nicht ausdrücklich im Vertrag geregelt ist, wird im internationalen Verhältnis immer verlangt, dass die PSP abgeschlossen ist, bevor eine sicherheitsempfindliche Tätigkeit ausgeübt werden darf.

Art. 35 Datenerhebung

Die Datenerhebung orientiert sich weitgehend an der heutigen Gesetzgebung (vgl. Art. 20 BWIS). Die Absätze 1 und 2 regeln die detaillierte Datenerhebung, die aufgrund der Reduktion von drei auf zwei Prüfstufen reorganisiert wurde. In beiden Absätzen handelt es sich um *Kann*-Vorschriften. Die Fachstellen müssen also 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. Der Bundesrat wird in seinen Ausführungsbestimmungen auch festlegen können, wann welche Daten erhoben werden *müssen*.

Für die Grundprüfung können folgende Quellen konsultiert werden:

- Das Strafregister, die Akten der Strafbehörden (vgl. Art. 12 StPO), einschliesslich der Jugendstrafbehörden, und die Datensammlungen des NDB sowie der Polizei- und Sicherheitsbehörden des Bundes und der Kantone können Hinweise auf die Vertrauenswürdigkeit und die allfällige Vorbelastung einer Person enthalten. Den Fachstellen PSP wird im BPI das Recht auf den Online-Zugang zum Nationalen Polizeiindex eingeräumt. Die Daten der angeschlossenen kantonalen Polizeiorgane erschliessen sich ihr nun auf einfache und effiziente Art und Weise. Selbstverständlich sind allfällige Ergebnisse im Hinblick auf die vorgesehene Tätigkeit der geprüften Person zu gewichten und in den entsprechenden Zusammenhang zu stellen. Es liegt nicht an den Strafbehörden, zu entscheiden, welche Unterlagen für eine PSP erforderlich sind. Die Fachstelle PSP muss alle vorhandenen Akten erhalten, um sich ein abschliessendes Bild über die zu prüfende Person machen zu können.
- Die Informationen aus den Registern der Betreibungs- und Konkursbehörden werden benötigt, um die finanzielle Situation der zu prüfenden Personen im Hinblick auf ein allfälliges Sicherheitsrisiko wie beispielsweise Bestechlichkeit beurteilen zu können.
- Neu dürfen auch Unterlagen und Ergebnisse früher durchgeführter PSP beigezogen werden. Einerseits muss die Fachstelle gleiche Sachverhalte konsistent beurteilen. So dürfte im Grunde genommen eine bestimmte Person aufgrund derselben Vorkommnisse nicht anders beurteilt werden als im Rahmen einer vergangenen Prüfung der gleichen Prüfstufe. Andererseits wird dadurch die Datenerhebung erleichtert, weil bestimmte Vorkommnisse bereits anlässlich früherer Prüfungen festgestellt wurden. Aufgrund der Wiederholungsfristen kann es vorkommen, dass eine frühere Erklärung Daten enthält, die in Anwendung von Artikel 48 im System vernichtet wurden. Solche Daten dürfen selbstverständlich nicht mehr bearbeitet werden.

– Informationen aus sozialen Netzwerken, die nicht an die Allgemeinheit gerichtet, sondern nur für geschlossene Personenkreise bestimmt sind, gelten nicht als öffentlich zugänglich und dürfen nicht erhoben werden.

Bei der erweiterten PSP können zusätzlich zu den eben genannten Quellen folgende Quellen konsultiert werden:

– Daten aus den eidgenössischen und kantonalen Steuerregistern können zusätzliche Erkenntnisse über die wirtschaftliche Situation der geprüften Personen liefern, etwa bei offensichtlichen Diskrepanzen zwischen Lebenshaltung und Steuerleistung.

– Die Daten aus den Registern der Einwohnerkontrolle werden nicht immer erhoben, weil sie oft nur einen begrenzten Mehrwert haben. Sie können aber situativ für die Beurteilung der persönlichen Situation der Betroffenen wichtige Hinweise liefern.

– In der erweiterten Prüfung wird die finanzielle Situation der zu prüfenden Person detailliert geprüft. Deshalb können Daten bei Finanzinstituten und Banken, mit welchen die zu prüfende Person Geschäftsbeziehungen unterhält, systematisch erhoben werden.

– Die persönliche Befragung dient dazu, Sachverhalte anzusprechen, die aus den Registerabfragen nicht oder nur unklar hervorgehen. Diese persönliche Befragung ist nicht zu verwechseln mit der Befragung nach Absatz 3. Die Befragung nach Absatz 2 Buchstabe d kann ohne Anhaltspunkte für ein Sicherheitsrisiko durchgeführt werden und ist im Befragungsumfang nicht eingeschränkt.

Absatz 3 sieht vor, dass die Fachstellen PSP die zu prüfende Person unabhängig von der Prüfstufe persönlich befragen können, wenn sicherheitsrelevante Umstände im Rahmen der Datenerhebung entdeckt werden. Diese persönliche Befragung ist im Umfang auf die Daten eingeschränkt, die im Rahmen der betroffenen Prüfstufe erhoben werden dürfen. Eine Befragung kann auch dann stattfinden, wenn die Fachstelle PSP nicht genügend Daten über einen hinreichenden Zeitraum erheben konnte. Dies kann beispielsweise dann der Fall sein, wenn sich die zu prüfende Person vor der Prüfung längere Zeit in einem Land aufgehalten hat, in dem keine oder keine zuverlässige Datenerhebung möglich ist. Der Ausdruck *über einen hinreichenden Zeitraum* ist bewusst offen formuliert. Die heutige Regelung von Artikel 19 Absatz 3 PSPV, wonach die Fachstellen PSP mindestens auf Daten über einen Zeitraum von fünf Jahren vor Einleitung der Grundprüfung und von zehn Jahren vor Einleitung der erweiterten Prüfung zurückgreifen können müssen, wurde teilweise als unverhältnismässig und zu absolut kritisiert. Zwei Lösungsansätze sind deshalb denkbar: Entweder präzisiert der Bundesrat im Rahmen seiner Ausführungsbestimmungen den entsprechenden Ausdruck oder seine Auslegung bleibt im Ermessen der Fachstellen PSP. Zur Abklärung besonderer sicherheitsrelevanter Umstände oder zum Erhalt ergänzender Daten über einen längeren Zeitraum kann die Fachstelle PSP auch Drittpersonen befragen. Solche Befragungen dürfen nur mit dem Einverständnis der zu prüfenden Person und der betroffenen Drittpersonen durchgeführt werden, wobei das Einverständnis der betroffenen Drittperson die Pflicht zur Aus-

kunftserteilung nicht mit sich bringt. Die betroffene Drittperson kann also trotz des Einverständnisses jederzeit auf die Erteilung jeglicher Auskunft verzichten.

Dass bei Befragungen nach Absatz 2 Buchstabe d oder nach diesem Absatz höchstpersönliche Fragen gestellt werden, liegt im Sinn der Sache. Die Relevanz der Fragen ergibt sich stets aus dem Kontext der Befragung bzw. Funktion, Aufgabe und persönlichen Situation der Person. So können gewisse Fragen gezielt auf Aspekte abzielen, die für die Risikobeurteilung unabdinglich sind. Andere hingegen dienen dem Gesprächsaufbau oder der Herstellung einer Gesprächskultur. Es werden jedoch keinerlei Fragen ohne Bezug zum Auftrag gestellt. Grundsätzlich ist dabei nie gänzlich auszuschliessen, dass die Befragung durch die zu prüfende Person als unangenehm empfunden wird. Die Befragungen werden im Bewusstsein um diese Tatsache deshalb so angenehm, wie dies der Zweck der Befragungen erlaubt, durchgeführt. Nichtsdestotrotz gilt es, alle für die Beurteilung nötigen Informationen zu erheben.

Es kommt vor, dass die für die Beurteilung erforderlichen Daten nicht nur die geprüften Personen betreffen, sondern auch Drittpersonen. Dies kann beispielsweise bei Bankkontenauszügen einer verheirateten Person der Fall sein. Solche Personendaten dürfen nach Absatz 4 ebenfalls bearbeitet werden, sofern sie untrennbar mit den Daten über die zu prüfende Person verbunden und für die Beurteilung des Risikos unerlässlich sind. Der Aufwand, der mit dem jeweiligen Einholen der Einwilligung der Drittperson zur Datenbearbeitung verbunden wäre, wäre für die Fachstellen PSP unverhältnismässig gross. Aus Transparenzgründen sollen die Fachstellen PSP diese Drittpersonen aber über die Datenbearbeitung informieren. Ist die Information nicht oder nur mit unverhältnismässigem Aufwand möglich, ist Artikel 18*a* Absatz 4 Buchstabe b DSG anwendbar.

Art. 36 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. Das Gesetz muss entsprechend die erhebenden Behörden zur Gewährleistung der Amtshilfe zugunsten der Fachstellen PSP ermächtigen beziehungsweise verpflichten. Absatz 2 regelt die besonderen Modalitäten der Amtshilfe des Fedpol für ausländische Daten im Strafverfolgungsbereich. Gemäss staatsvertraglichem Recht stehen die polizeilichen Informationskanäle (Schengener Informationssystem und Europol) nur für den Informationsaustausch zwischen Strafverfolgungsbehörden zur Verfügung. Auch der Interpol-Kanal steht nur für den Informationsaustausch zwischen Strafverfolgungsbehörden offen. Da die Fachstellen PSP selbst bei grosszügiger Auslegung des Begriffs nicht als Strafverfolgungsbehörde und ihre Aufgaben nicht als Tätigkeiten im Bereich der Strafverfolgung eingestuft werden können, sondern ausschliesslich als sicherheitspolizeiliche Tätigkeiten gelten, stehen die polizeilichen Kanäle für internationale verdachtsunabhängige Anfragen im Rahmen der PSP grundsätzlich nicht zur Verfügung. Ergeben jedoch die ersten Abklärungen der Fachstelle PSP in den zur Verfügung stehenden Informationssystemen (insbesondere durch die automatisierte Abfrage der Register nach Art. 46 Abs. 6) Hinweise auf Straftaten, die in die Zuständigkeit der Bundeskriminalpolizei als Zentralstelle fallen, dann dürfen die entsprechenden Kanäle verwendet werden. In einem solchen Fall prüft die zuständige Zentralstelle (Fedpol), ob die

Daten sicherheitsrelevant sind und folglich weitergegeben werden dürfen. Um sowohl den Anfragen der Fachstellen PSP als auch den Arbeiten der Analysestellen des Fedpol eine konkrete gesetzliche Grundlage zu geben, wurde der entsprechende Absatz eingefügt.

Art. 37 Kostentragung

Die Mitwirkung von Behörden am Verfahren soll unentgeltlich stattfinden. Dies entspricht grundsätzlich geltender Praxis, mit Ausnahme der Betreibungs- und Konkursregisterauszüge aus den Kantonen, die bisher kostenpflichtig waren. Dritte, beispielsweise Banken oder Kreditinstitute, die zur Mitwirkung beigezogen werden, sollen entschädigt werden, wenn der dadurch verursachte Aufwand erheblich ist. Erheblich wird ein solcher Aufwand insbesondere dann, wenn er über die Erstellung von Kontoauszügen und dergleichen hinausgeht und besonders intensive Recherchen durch die ersuchten Dritte erfordert. Der Bundesrat wird die Voraussetzungen und die Höhe solcher Entschädigungen in den Ausführungsbestimmungen regeln.

Art. 38 Einstellung

Ein bereits eingeleitetes Prüfverfahren wird eingestellt, wenn die zu prüfende Person im Verlauf des Verfahrens ihre Einwilligung zurückzieht oder wenn sie aus einem anderen Grund für die anvisierte Funktion oder für den fraglichen Auftrag nicht mehr in Frage kommt (z. B. weil die zu prüfende Person ihren Arbeitsvertrag gekündigt hat oder die Firma, für welche die zu prüfende Person hätte tätig werden sollen, insolvent geworden ist). In diesem Fall sind sowohl die zu prüfende Person als auch die einleitende Stelle über die Einstellung des Verfahrens zu informieren und die bei der Fachstelle PSP bereits erhobenen Daten und Akten zu vernichten. Die betroffene Person gilt in der Folge als nicht sicherheitsgeprüft und darf die fragliche sicherheitsempfindliche Tätigkeit nicht ausüben bzw. die entsprechende Funktion nicht übernehmen. Die Einstellung des Verfahrens ist ein Realakt im Sinne von Artikel 25*a* VwVG.

3. Abschnitt: Beurteilung des Sicherheitsrisikos

Art. 39 Sicherheitsrisiko

Es wurde bemängelt, dass die geltende Regelung im BWIS nicht ausdrücklich erwähnt, was als Sicherheitsrisiko anzusehen ist (s. Ziff. 1.1.4: Bericht der GPK-N zur Nachkontrolle zur Inspektion über die Umstände der Ernennung von Roland Nef zum Chef der Armee, Empfehlung 1). Deshalb soll nun eine entsprechende Norm aufgenommen werden, welche die Rechtsprechung des Bundesverwaltungsgerichts und des Bundesgerichts sinngemäss wiedergibt. Es versteht sich, dass es keine rein quantitative Beurteilungsmethoden gibt, wenn es darum geht, das Risiko in Bezug auf menschliche Handlungen oder Unterlassungen einzuschätzen. Deshalb wird eine qualitative Methode angewendet, bei welcher das Vorhandensein und das Zusammenwirken von Risikofaktoren bewertet werden.

Das Risiko ist in der Lehre das Produkt der Eintrittswahrscheinlichkeit eines Ereignisses und der Auswirkungen dieses Ereignisses. Der für die Unterstellung unter die PSP massgebende Ausdruck *sicherheitsempfindliche Tätigkeit* enthält in seiner Definition die Auswirkungen, deren Eintreten vermieden werden soll. Es handelt sich dabei um eine *erhebliche bzw. schwerwiegende Beeinträchtigung der Interessen nach Artikel 1 Absatz 2*. Wenn die zu prüfende Person die Aufgaben, die ihr zugewiesen werden sollen, vorschriftskonform und sachgemäss erfüllt, so kann der Schaden ihretwegen nicht eintreten. Das zu vermeidende Ereignis ist also *e contrario* die vorschriftswidrige oder unsachgemässe Ausübung der sicherheitsempfindlichen Tätigkeit durch die betroffene Person. Ein Sicherheitsrisiko muss somit im Sinne von Absatz 1 angenommen werden, wenn die Wahrscheinlichkeit hoch ist, dass die geprüfte Person die sicherheitsempfindliche Tätigkeit vorschriftswidrig oder unsachgemäss ausüben wird und dadurch die Interessen nach Artikel 1 Absatz 2 mindestens erheblich beeinträchtigen wird.

Die Fachstellen PSP müssen sich einzig auf die Eintrittswahrscheinlichkeit des Ereignisses fokussieren. Bei der Bewertung einer solchen Wahrscheinlichkeit wird es sich zwangsläufig immer um eine Prognose über ungewisse künftige Sachverhalte handeln; diese Prognose ist mit Unsicherheiten behaftet, weil es in der Natur der Sache liegt, dass sie nicht nur auf *harten* Fakten beruht und dass es sich bei den aus den erhobenen Daten gezogenen Schlussfolgerungen auch um Annahmen und Vermutungen handeln kann. Grundlage für diese Prognose bildet die Gesamtheit aller Umstände, wie beispielsweise die Persönlichkeit der betroffenen Person, ihr Vorleben und ihre Lebensverhältnisse, soweit diese Rückschlüsse auf ihr künftiges Verhalten zulassen. In Absatz 2 werden deshalb die Risikofaktoren konkretisiert, die zur Annahme einer hohen Wahrscheinlichkeit für eine Beeinträchtigung führen. Er umschreibt persönliche Eigenschaften, die besonders risikoträchtig sind. Die Aufzählung orientiert sich inhaltlich an der heutigen Praxis der Fachstellen PSP sowie an der Rechtsprechung des Bundesverwaltungsgerichts und des Bundesgerichts. Die Umschreibungen zielen zwar im Grundsatz auf möglichst objektiv feststellbare Eigenschaften ab, doch können diese häufig nur aus Indizien oder aus dem Kontext abgeleitet werden und überschneiden sich partiell. Mit Integrität und Vertrauenswürdigkeit werden vorweg der Charakter sowie die Gewohnheiten und Beziehungen einer Person zu ihrem Umfeld anvisiert. Diese Eigenschaften sind bei der Ausübung einer sicherheitsempfindlichen Tätigkeit die Eignungserfordernisse schlechthin. Liegen diese Eigenschaften vor, kann mit hoher Wahrscheinlichkeit darauf vertraut werden, dass die mit einer solchen Tätigkeit betraute Person loyal zu ihrer Aufgabe steht und die Sicherheitsinteressen des Arbeitgebers oder der Institution wahrt. Welche der Indizien und Zusammenhänge die fehlende Vertrauenswürdigkeit einer Person, ihre mutmassliche Erpressbarkeit oder ihr beeinträchtigtes Urteils- und Entscheidungsvermögen belegen, kann auf Gesetzesebene nicht spezifiziert, sondern muss letztlich in jeder einzelnen Beurteilung ermittelt und dargelegt werden.

Nach Absatz 3 stellt die PSP auf eine objektive Gefährdung und nicht auf ein schuldhaftes Verhalten ab. Dies im Gegensatz etwa zum Strafrecht, bei dem die Schuld immer Voraussetzung für eine Strafe ist. Anders als im Strafrecht (*in dubio pro reo*) rangiert somit im Zweifel die Sicherheit des Staates bzw. das Landesinteresse vor den Interessen der betroffenen Person. Die Annahme eines Sicherheitsrisikos muss durch Fakten und tatsächliche Umstände, welche die zu beurteilende

Person betreffen, begründet werden. Reine Vermutungen, insbesondere wenn sie die politische Gesinnung der zu prüfenden Person betreffen, sind nicht zulässig.

Art. 40 Ergebnis der Beurteilung

Absatz 1 regelt die verschiedenen Erklärungen der Fachstellen PSP, in welchen das Ergebnis der Beurteilung festgehalten wird. Kann aufgrund der ungenügenden Datenerhebung im Sinne von Artikel 35 Absatz 3 eine Person nicht fachgerecht beurteilt werden, so erlässt die Fachstelle PSP eine Feststellungserklärung. Gegebenenfalls wird die betroffene Person zuerst befragt.

Die Erklärungen der Fachstellen PSP stellen rechtlich keine Verfügungen sondern Realakte im Sinne von Artikel 25*a* Absatz 1 VwVG dar. Wie das heutige BWIS (s. Art. 21 Abs. 3 BWIS) schafft das ISG einen direkten Rechtschutz für die geprüften Personen (s. Art. 45). Somit ist der Rechtsweg von Artikel 25*a* Absatz 2 VwVG nicht anwendbar (Erlass einer Verfügung). Absatz 2 sorgt deshalb für einen formellen Anspruch auf rechtliches Gehör. Faktisch heisst dies, dass beim Vorliegen eines Erklärungsentwurfs nach den Buchstaben b–d die betroffene Person in geeigneter Form über den Inhalt orientiert und ihr eine angemessene Frist zur Stellungnahme eingeräumt wird.

Art. 41 Mitteilung

Die Absätze 1 und 2 entsprechen grundsätzlich geltendem Recht (Art. 21 Abs. 2–4 BWIS). Die entscheidende Stelle erhält die Erklärung ebenfalls in ungekürzter Form. Andernfalls wäre es ihr nicht möglich, sachgemäss zu entscheiden.

Absatz 3 regelt den Fall, in welchem eine PSP eingeleitet wird, die betroffene Person aber im Zusammenhang mit einer anderen Tätigkeit nach den Buchstaben a–c ebenfalls einer Prüfung untersteht (z. B. nach Art. 20*b* BPG). In diesem Fall soll die Fachstelle PSP der jeweiligen entscheidenden Stelle die Erklärung zur Hauptprüfung mitteilen können. Die Regelung der Prüfung der Vertrauenswürdigkeit nach Artikel 20*b* BPG sowie nach Artikel 113 MG verlangt, dass beide Verfahren vereinigt werden, wenn eine Person aufgrund des vorliegenden Gesetzes ebenfalls einer PSP unterzogen wird. Mit dem Begriff *unterstehen* wird nicht verlangt, dass eine andere Prüfung eingeleitet worden ist oder unmittelbar wiederholt werden soll. Dies ist insbesondere für Prüfungen nach Artikel 113 MG wichtig, welchen alle Angehörigen der Armee unterstehen. Wird im Rahmen der PSP ein Risiko in Bezug auf die Armeewaffe festgestellt, so dürfen die Fachstellen PSP der zuständigen militärischen Behörde die Erklärung mitteilen.

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.

4. Abschnitt: Folgen der Erklärung

Art. 42 Ausübung der sicherheitsempfindlichen Tätigkeit

Absatz 1 entspricht dem heutigen Artikel 21 Absatz 4 BWIS. Es ist nicht Aufgabe der Fachstellen PSP, die Verantwortung der Linie für Personalentscheide zu übernehmen oder einzuschränken, sondern lediglich, die entscheidende Behörde über ein allfälliges Risiko zu informieren. Vor ihrem Entscheid muss die entscheidende Stelle von der Erklärung der Fachstelle PSP Kenntnis nehmen, denn nur dann kann sie ihren Entscheid unter Berücksichtigung der allfälligen Risiken treffen.

Die Auflagen nach Absatz 3 stellen risikomindernde Massnahmen dar, die meistens personalrechtlicher Natur sind. Die entscheidende Stelle kann beispielsweise verlangen, dass die betroffene Person regelmässig ihre finanzielle Lage offenlegt oder sich Drogentests unterzieht. Diese Auflagen betreffen ausschliesslich die Ausübung der sicherheitsempfindlichen Tätigkeit; andere Aufgaben sind nicht betroffen. In der Regel werden die geeignetsten Auflagen von der Fachstelle PSP empfohlen. Die entscheidende Stelle ist aber an diese Auflagen nicht gebunden und kann selber Auflagen bestimmen.

Die Mitteilung des Entscheids nach Absatz 4 erfolgt innerhalb des Informationssystems nach Artikel 46 und ist insbesondere für die Gewährung des Zutritts zu Sicherheitszonen massgebend. Die Fachstellen PSP ziehen weder Erkenntnisse aus den Entscheiden noch lassen sie sich durch diese in ihrer Praxis beeinflussen.

Art. 43 Mehrmalige Verwendung einer Erklärung

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. Voraussetzung, damit bei Vorhandensein einer noch gültigen und gleichwertigen Erklärung auf eine neue Prüfung verzichtet werden kann, ist ein strukturiertes Vorgehen bei der Durchführung der Prüfung und bei der Beurteilung des Risikos (s. Erläuterungen zu Art. 31). In der Praxis stellt diese Regelung kein Problem dar, wenn eine Sicherheitserklärung für die gleiche oder eine höhere Prüfstufe ausgestellt wurde. Probleme können sich aber beispielsweise dann ergeben, wenn einer bestimmten Person für eine höhere Prüfstufe eine Sicherheitserklärung mit Vorbehalt oder eine Risikoerklärung ausgestellt wurde. Es ist nämlich durchaus möglich, dass für die Bearbeitung von «geheim» klassifizierten Informationen ein Sicherheitsrisiko besteht, dass aber dieses Risiko in Bezug auf die Bearbeitung von als «vertraulich» klassifizierten Informationen tragbar ist. Der Bundesrat wird diese *Kann*-Vorschrift auf Verordnungsebene konkretisieren.

Art. 44 Wiederholung

Das ISG schreibt keine festen ordentlichen Wiederholungsintervalle vor. Es setzt diesbezüglich lediglich Leitplanken fest. Grund dafür ist, dass die Wiederholung inskünftig vermehrt dem tatsächlichen Sicherheitsbedarf entsprechend erfolgen soll. Die Ausführungsbestimmungen werden die Wiederholungen detailliert regeln. Der Bundesrat soll bei Angehörigen der Armee oder des Zivilschutzes auf eine Wieder-

holung verzichten dürfen, wenn beispielsweise eine Wiederholungsprüfung mit Blick auf die noch verbleibende Dienstzeit unverhältnismässig erschiene.

Absatz 3 regelt die ausserordentliche Wiederholung. Grund für eine solche vorzeitige Wiederholung ist die Entstehung neuer Risiken bei der betroffenen Person, beispielsweise die Eröffnung eines Strafverfahrens gegen sie, das einen Bezug zur sicherheitsempfindlichen Tätigkeit aufweist.

Art. 45 Rechtsschutz

Die Absätze 1 und 2 entsprechen trotz angepasster Formulierung geltendem Recht (s. Art. 21 Abs. 2 BWIS). Die Frist zur Ausübung der Einsichts- und Berichtigungsrechte wird im Vergleich zu heute von 10 auf 30 Tage erhöht. Da die geprüfte Person gestützt auf Absatz 3 30 Tage Zeit hat, um beim Bundesverwaltungsgericht Beschwerde zu führen, soll sie während dieser Zeit alle Rechte nach Absatz 1 ausüben können.

Absatz 3 entspricht ebenfalls grundsätzlich geltendem Recht (s. Art. 21 Abs. 3 BWIS), wobei eingangs erklärt wird, dass die Erklärungen der Fachstellen PSP Realakte im Sinne von Artikel 25*a* VwVG darstellen. Der heutige Artikel 22 PSPV bezeichnet die Erklärungen der Fachstellen PSP als Verfügungen im Sinne von Artikel 5 VwVG. Diese Qualifizierung ist materiell betrachtet aber unzutreffend, weil den Erklärungen nur empfehlender Charakter zukommt (s. Art. 21 Abs. 4 BWIS sowie Art. 42 ISG). Aufgrund der Schwere des Eingriffs in die Persönlichkeitsrechte der geprüften Personen wird allerdings auf den ordentlichen Rechtschutz für Realakte nach Artikel 25*a* VwVG verzichtet und an dessen Stelle ein unmittelbarer Rechtsweg an das Bundesverwaltungsgericht geschaffen.

Mit dem ISG dürfen das Bundesverwaltungsgericht und das Bundesgericht neu für ihre eigenen Angestellten oder die von ihnen beauftragten Dritten PSP einleiten. In diesen Fällen werden sie auch für den Entscheid über die Ausübung der sicherheitsempfindlichen Tätigkeit und gleichzeitig für ein allfälliges Beschwerdeverfahren zuständig sein. Damit entsteht, wie bei arbeitsrechtlichen Streitigkeiten, ein Interessenkonflikt, der mit der bewährten Regelung von Artikel 36 BPG verhindert wird.

5. Abschnitt: Bearbeitung von Personendaten

Art. 46 Informationssystem zur Personensicherheitsprüfung

Artikel 46 entspricht grundsätzlich geltendem Recht (s. Art. 144–149 MIG). Beide Fachstellen benutzen heute ein System (SIBAD), das vom VBS eingesetzt und betrieben wird. Die erhobenen Daten und insbesondere die Risikobeurteilungen stellen besonders schützenswerte Personendaten bzw. Persönlichkeitsprofile im Sinne von Artikel 3 Buchstaben c und d DSG dar. Das System wird selbstverständlich nicht nur für die PSP nach dem ISG verwendet, sondern auch für die Durchführung der Prüfungen der Vertrauenswürdigkeit nach der Spezialgesetzgebung und der Beurteilungen des Gewaltpotenzials nach dem MG. Der Bundesrat wird die Zuständigkeiten für den Datenschutz festlegen (s. Art. 49 Bst. d).

Das System verwendet zum Identitätsnachweis eine eigene Registrationsnummer. Die AHV-Versichertennummer wird nur dann vom System verwendet, wenn ein anderes System diese Nummer systematisch verwendet. Dies betrifft in erster Linie das Informationssystem PISA der Gruppe Verteidigung. Da das PISA die AHV-Versichertennummer systematisch verwendet, wird die Nummer bei der Einleitung von PSP der Armee zum Informationssystem zur PSP übertragen. Innerhalb dieses Informationssystems wird wiederum nur die systemeigene Registrationsnummer benutzt. Beim Abgleich mit dem PISA nach der Prüfung muss die Konkordanz mit der AHV-Versichertennummer aber wieder hergestellt werden.

Absatz 6: Nach Artikel 19 Absatz 3 DSG dürfen besonders schützenswerte Personendaten nur dann durch ein automatisiertes Verfahren zugänglich gemacht werden, wenn dies in einem Gesetz im formellen Sinn so vorgesehen ist. Die Effizienz des Prüfverfahrens kann gesteigert werden, indem die den Fachstellen PSP gesetzlich zustehenden Zugriffe auf Informationssysteme des Bundes automatisiert abgefragt werden. Die formell-gesetzlichen Grundlagen der drei hier aufgeführten Informationssysteme sehen bereits heute den Zugriff der Fachstellen PSP vor. Diese erhalten also dadurch nicht mehr oder erweitert Zugriff. Bis anhin mussten allerdings sämtliche Systeme durch die Mitarbeitenden der Fachstellen PSP einzeln manuell abgefragt werden. Künftig sollen lediglich Systeme, bei denen die automatisierte Abfrage einen Treffer, also eine Verzeichnung, ergeben hat, noch manuell konsultiert werden (s. auch Art. 36 Abs. 2). Dieses Vorgehen, das auf Verordnungsstufe detailliert festgelegt wird, verringert ausserdem deutlich die Fehlerquellen bei der manuellen Eingabe. Es versteht sich, dass die Kantone in ihrem kantonalen Recht den Fachstellen PSP einen entsprechenden automatisierten Zugriff auf ihre Datenbanken einräumen dürfen.

Art. 47 Zugriffsrechte und Datenbekanntgabe

Artikel 47 Absätze 1–3 entsprechen geltendem Recht (s. Art. 144–149 MIG), das aufgrund von Artikel 19 Absatz 3 DSG ausführlicher gestaltet wird. Die Listen nach Absatz 4 werden nur bei nachgewiesenem Bedarf geliefert. Die Lieferung erfolgt ausserhalb des Informationssystems.

Art. 48 Datenaufbewahrung, -archivierung und -vernichtung

Artikel 48 entspricht grundsätzlich geltendem Recht (s. Art. 144–149 MIG sowie PSPV). Absatz 1 schafft die rechtliche Grundlage für die Tonaufnahme der Befragungen. Nach Absatz 2 darf die Aufbewahrungsdauer zehn Jahre nicht überschreiten. Falls eine Person bereits mehreren Prüfungen unterzogen wurde, sind diejenigen Daten, die Prüfungen betreffen, die länger als zehn Jahre zurückliegen, zu löschen. Das Bundesarchiv beurteilt, welche Daten aus dem Informationssystem archivwürdig sind (Abs. 3). Es handelt sich insbesondere um Statistiken über die Risikofälle und über die Anzahl durchgeführter PSP. Bei einer Einstellung des Verfahrens nach Artikel 38 besteht die Möglichkeit (auch wenn dies sehr unwahrscheinlich ist), dass die betroffene Person den Erlass einer Verfügung verlangt und anschliessend beim Bundesverwaltungsgericht Beschwerde führt. Die Fachstellen dürfen die Daten also nicht sofort löschen.

6. Abschnitt: Bestimmungen des Bundesrats

Art. 49

Der Bundesrat soll ergänzendes und gesetzesvertretendes Recht erlassen dürfen. Es handelt sich dabei mithin nicht bloss um Ausführungsbestimmungen, für die der Bundesrat aufgrund von Artikel 182 BV ohne weiteres zuständig ist. Grund dafür ist die Regelung von Artikel 85 Absatz 1, wonach alle Behörden nach Artikel 2 Absatz 1 für den Vollzug dieses Gesetzes und den Erlass entsprechender Ausführungsbestimmungen zuständig sind.

- Buchstabe c: Ausländische Sicherheitsbehörden gewähren ausschliesslich sicherheitsgeprüften Personen Zugang zu klassifizierten Informationen, klassifiziertem Material und Sicherheitszonen. Die zuständige schweizerische Behörde (voraussichtlich die Fachstelle des Bundes für Informationssicherheit nach Artikel 84) muss die erforderliche Personensicherheitsbescheinigung ausstellen können. Massgebend ist der Entscheid der entscheidenden Stelle und nicht die Erklärung.
- Buchstaben d–f: Der Bundesrat muss in Anwendung von Artikel 16 Absatz 2 DSG ergänzendes Recht zur Organisation der Zuständigkeiten und Verantwortungen für den Datenschutz (inkl. Datensicherheit) im Zusammenhang mit dem Informationssystem nach Artikel 46 erlassen. Da die Daten, die im Rahmen der PSP bearbeitet werden, besonders sensibel sind, soll die Rechtmässigkeit ihrer Bearbeitung periodisch durch eine Stelle kontrolliert werden, die von den Fachstellen PSP unabhängig ist.

4. Kapitel: Betriebssicherheitsverfahren

1. Abschnitt: Allgemeine Bestimmungen

Art. 50 Verfahrenszweck

Zum Zweck des BSV, siehe Ziffer 1.2.6.

Art. 51 Betroffene Betriebe

Als *Betrieb* im Sinne des Gesetzes wird nicht unbedingt das ganze Unternehmen erfasst. Betroffen sind vielmehr nur diejenigen Teile und Personen des Unternehmens, die tatsächlich mit dem sicherheitsempfindlichen Auftrag betraut werden.

- Buchstabe a führt den Hauptanwendungsfall auf: Eine verpflichtete Behörde oder Organisation will einen sicherheitsempfindlichen Auftrag einem Unternehmen erteilen, das sich darum bewirbt. Das BSV stellt grundsätzlich eine nationale Angelegenheit dar. Deshalb müssen sich Betriebe mit Sitz im Ausland, die sich um einen Auftrag aus der Schweiz bewerben, durch denjenigen Staat prüfen lassen, in dem sich ihr Sitz befindet. Die Zuständigkeiten und Prüfmodalitäten sind Bestandteil der völkerrechtlichen Vereinbarungen nach Artikel 88.

– Buchstabe b erfasst umgekehrt den Fall von Betrieben mit Sitz in der Schweiz, die sich für einen Auftrag aus dem Ausland bewerben wollen und den dortigen Behörden eine Sicherheitserklärung der Behörden ihres Sitzstaates vorweisen müssen. Dieses Verfahren und die damit verbundene Zertifizierung stellen eine amtliche Tätigkeit dar, die nicht an die Privatwirtschaft übertragen werden kann, weil die ausländischen Behörden ausnahmslos ein amtliches «Sicherheitssiegel» des Sitzstaates des Betriebs verlangen. Da der Bund in diesen Fall kein unmittelbares Selbstinteresse an der Durchführung des Verfahrens hat, trägt der Betrieb die Kosten des Verfahrens (Abs. 3). Der Bundesrat wird die Frage der Kosten auf Verordnungsebene regeln.

In der Praxis stellt die erforderliche Zustimmung des Betriebs nie ein Problem dar, weil die Betriebe ein finanzielles Interesse an der Auftragserteilung haben.

Art. 52 Einstellung des Verfahrens

Das BSV wird nur durchgeführt, wenn bestimmte Kriterien und Voraussetzungen (z. B. Zustimmung) erfüllt werden. Erfüllt der Betrieb diese Kriterien im Laufe des BSV nicht mehr, wird das Verfahren eingestellt und sämtliche mit diesem zusammenhängenden Daten und Akten werden vernichtet. Dies kann nach Buchstabe c beispielsweise auch dann der Fall sein, wenn der Betrieb im Falle seines Konkurses oder der Zerstörung der Betriebsstätte durch einen Brand den Auftrag überhaupt nicht mehr erfüllen kann. Absatz 2 hält fest, dass die BSV durch eine *Fachstelle für Betriebssicherheit* (Fachstelle BS) durchgeführt werden. Innerhalb des Bundes soll sich also (wie bis anhin) eine einzige Stelle mit diesen Verfahren befassen. Die Fachstelle BS muss die Einstellung dem Betrieb sowie der Auftraggeberin mitteilen.

2. Abschnitt: Einleitung des Betriebssicherheitsverfahrens

Art. 53 Antrag auf Einleitung

Die Fachstelle BS wird nur auf Antrag (und nicht im Auftrag) einer verpflichteten Behörde oder Organisation tätig. Letztere sind aber verpflichtet, einen entsprechenden Antrag zu stellen, falls sie einen sicherheitsempfindlichen Auftrag an einen Betrieb vergeben wollen. Die Behörden müssen die Zuständigkeiten zur Antragsstellung bestimmen. Je nach ihren organisatorischen Bedürfnissen kann dies eine zentrale Stelle sein oder jede Stelle, die über die Kompetenz verfügt, sicherheitsempfindliche Aufträge an Unternehmen der Privatwirtschaft zu vergeben (vgl. auch Verordnung vom 24. Oktober 2012[29] über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung).

Im internationalen Verhältnis wird das Verfahren in der Regel mittels einer Anfrage seitens der ausländischen Sicherheitsbehörde (*Facility Security Clearance Information Sheet*) an die hiesige Sicherheitsbehörde und einer Bestätigung des interessier-

29 SR **172.056.15**

ten Betriebs eingeleitet. Die Anfrage wird mittels eines standardisierten Ablaufs beantwortet. Die Einzelheiten dieser Verfahren sind durch Verordnung zu regeln.

Art. 54 Prüfung des Antrags

Nach Eingang des Antrags prüft die Fachstelle BS zunächst, ob ein sicherheitsempfindlicher Auftrag vorliegt, und leitet gegebenenfalls das BSV ein. Können die Risiken für die Informationssicherheit im konkreten Fall durch andere Massnahmen hinreichend minimiert werden, kann die Fachstelle BS nach Rücksprache mit der Auftraggeberin auf die Durchführung des BSV verzichten. Damit lassen sich in diesen Fällen unwirtschaftliche und bürokratische Aufwendungen vermeiden. Wenn der Auftrag unter Aufsicht der Auftraggeberin in deren Räumlichkeiten ausgeführt wird und dem Auftragnehmer (Betrieb) keine Unterlagen ausgehändigt werden, reichen beispielsweise unter Umständen entsprechende PSP aus. Verzichtet die Fachstelle BS auf das BSV, so empfiehlt sie auch die Sicherheitsmassnahmen, die sie für zweckmässig betrachtet. In diesem Fall verfügt die Fachstelle BS über keine Durchsetzungskompetenzen mehr.

Art. 55 Festlegung der Sicherheitsanforderungen

Nach der Einleitung des Verfahrens legt die Fachstelle BS in Absprache mit der Auftraggeberin die Anforderungen an die Informationssicherheit für die Auftragserfüllung fest. Soweit bereits im Rahmen des Vergabeverfahrens die Ausübung einer sicherheitsempfindlichen Tätigkeit notwendig ist, werden auch für diese Phase die Anforderungen festgehalten. Dies ist insbesondere oft dann der Fall, wenn für die Erstellung einer Offerte während des Vergabeverfahrens die Kenntnisnahme von klassifizierten Informationen oder der Zugang zu Sicherheitszonen erforderlich ist.

3. Abschnitt: Beurteilung der Betriebe

Art. 56 Eignung

Der Begriff *Eignung* ist im Sinne der Systematik des öffentlichen Beschaffungsrechts zu verstehen. Zwar stellt die Gewährleistung der Informationssicherheit kein ausdrückliches Eignungskriterium nach Artikel 9 BöB dar, der Entwurf fügt es aber für die Ausführung sicherheitsempfindlicher Aufträge ein. Die Prüfung der sicherheitsmässigen Eignung entspricht einer Risikobeurteilung. Aus Wirtschaftlichkeits- und Datenschutzgründen soll diese Risikobeurteilung nicht bei allen Anbietern durchgeführt werden, sondern nur bei denjenigen, die für den Zuschlag in Frage kommen. Besteht nach Artikel 58 ein Risiko für die Informationssicherheit, dann ist der betroffene Betrieb nicht geeignet. Die Fachstelle BS muss für die Beurteilung der Eignung weisungsungebunden sein. Es geht hier darum, dass diese Beurteilung frei von wirtschaftspolitischen Interessen getroffen wird (vgl. Art. 32 Abs. 2).

Art. 57 Datenerhebung

Artikel 57 schafft die formell-gesetzliche Grundlage für die Datenerhebung zur Beurteilung der Eignung der Betriebe. Absatz 1 listet auf, welche Daten die Fachstelle BS zur Beurteilung der Eignung erheben kann. Die erforderlichen Daten werden im Wesentlichen beim Betrieb selbst mit dessen Einverständnis erhoben. Besonders wichtig sind auch die Ergebnisse der Abklärungen mit dem NDB. Schliesslich kann die Fachstelle BS auch Daten über die Firma aus dem Handelsregister oder im Internet erheben. Solche Recherchen können wichtige Informationen über die Vertrauenswürdigkeit der Firma liefern (s. Art. 35 Abs. 1 Bst. g für die PSP). Da sehr viele Betriebe im Ausland vernetzt sind, ist es notwendig, entsprechende Daten erheben zu können. Insbesondere nachrichtendienstliche Informationen aus dem Ausland, die vom NDB erhoben werden, können wertvolle Hinweise auf ein Sicherheitsrisiko liefern. Die Modalitäten solcher Anfragen und der Auskunftserteilung sind auf Verordnungsebene zu regeln.

Art. 58 Sicherheitsrisiko

Diese Bestimmung stellt das Pendant zur Beurteilung des Sicherheitsrisikos bei der PSP dar. Die Risikobeurteilungsmechanismen sind grundsätzlich identisch (vgl. Erläuterungen zu Art. 39). Ein Sicherheitsrisiko besteht demnach, wenn konkrete Anhaltspunkte dafür vorliegen, dass der Betrieb mit hoher Wahrscheinlichkeit den sicherheitsempfindlichen Auftrag vorschriftswidrig oder unsachgemäss ausführen wird. Dies kann beispielsweise dann der Fall sein, wenn die erhobenen Daten zeigen, dass der Betrieb Straftaten begangen hat, die für die Informationssicherheit relevant sind. Dies kann auch dann zutreffen, wenn der Betrieb aus einer einzelnen Person besteht (Einzelfirma) oder wenn für die Auftragserfüllung bestimmte Personen unentbehrlich sind (z. B. weil es sich bei diesen Personen um Fachleute handelt, die nicht ersetzt werden können, oder weil sie den Betrieb führen und der Auftrag ohne ihren Einsatz nicht erfüllt werden kann). Die Ausstellung einer Risikoerklärung im Rahmen der PSP für diese Betriebsangehörigen kann zur Folge haben, dass der Betrieb als Ganzes als Sicherheitsrisiko beurteilt werden muss. Mit dem BSV soll aber vor allem verhindert werden, dass sicherheitsempfindliche Informationen oder praktische Angriffsvektoren auf kritische Informatikmittel des Bundes Betrieben zugänglich gemacht werden, die aufgrund ihrer Eigentums- und Rechtsverhältnisse, ihrer Organisationsstrukturen oder ihrer Geschäftsbeziehungen beispielsweise von ausländischen Nachrichtendiensten oder Organisationen mit kriminellem Hintergrund gesteuert oder massgebend beeinflusst werden (*Foreign Ownership, Control or Influence*) (s. auch Ziff. 1.2.6).

Absatz 3 hält fest, dass das erwähnte Risiko durch die tatsächlichen Umstände begründet sein muss. Unerheblich ist dabei, ob den Betrieb selbst oder seine Angehörigen irgendein Verschulden trifft, beispielsweise wenn die Firma, welcher der Betrieb gehört, von Personen mit nachrichtendienstlichem oder kriminellem Hintergrund gesteuert oder beeinflusst wird (vgl. Erläuterungen zu Art. 39 Abs. 3).

Art. 59 Eröffnung der Beurteilung und Ausschluss aus dem Vergabeverfahren

Die Fachstelle BS eröffnet dem betreffenden Betrieb ihre Beurteilung in Bezug auf die Eignung. Ist der Betrieb mit der Risikobeurteilung nicht einverstanden, kann er gegen diese Verfügung Beschwerde beim Bundesverwaltungsgericht erheben (Art. 70 Abs. 1 Bst. d). Die Auftraggeberin kann das Submissionsverfahren bzw. ihre Vertragsverhandlungen mit allen Betrieben, bei denen kein Sicherheitsrisiko erkennbar ist, weiterführen. Sie ist nicht zur Beschwerde berechtigt und wird deshalb über die Beurteilung nur informiert. Erkennt die Fachstelle BS in Bezug auf einen Betrieb untragbare Sicherheitsrisiken, darf die Auftraggeberin diesem hingegen weder den Zuschlag erteilen noch den Vertrag mit einem solchen Betrieb abschliessen. Sie schliesst den betreffenden Betrieb als sicherheitsmässig ungeeignet aus dem Vergabeverfahren aus. Im Gegensatz zur PSP ist beim BSV die Auftraggeberin grundsätzlich an die Beurteilung der Fachstelle BS gebunden. Ein Unternehmen oder Betrieb, dem eine BSE ausgestellt wird, erhält ein staatliches Sicherheitssiegel. Die Integrität dieses Siegels kann nur dann gewahrt werden, wenn der Entscheid über die Eignung von Fachspezialisten getroffen wird. Die Fachstelle BS erlässt aus diesen Gründen eine anfechtbare Verfügung.

Absatz 3 räumt eine Ausnahme zum Grundsatz von Absatz 2 für den Fall ein, dass es für den Auftrag keine echte Alternative zu einem Betrieb gibt, bei dem ein Risiko für die Informationssicherheit des Bundes besteht. Dies betrifft vor allem Dienstleistungen im Informatikbereich, denn hier haben einige Firmen eine quasi monopolistische Marktstellung. Muss ein solcher Betrieb wegen mangelnder Alternative beauftragt werden, darf ihm auf keinen Fall eine schweizerische Sicherheitsbescheinigung ausgestellt werden. Entsprechend wird das BSV eingestellt und die Verantwortung für die Überprüfung der Sicherheitsmassnahmen der Auftraggeberin übertragen. Diese verfügt von Gesetzes wegen über analoge Durchsetzungsrechte wie die Fachstelle BS im Rahmen des BSV.

4. Abschnitt: Sicherheitskonzept

Art. 60 Zuschlag und Sicherheitskonzept

Sobald die Auftraggeberin den Zuschlag erteilt hat, informiert sie die Fachstelle BS. Diese leitet die weiteren Schritte des Verfahrens ein. Die Gewährleistung der Informationssicherheit beim Betrieb verlangt die Umsetzung entsprechender organisatorischer, personeller, technischer und physischer Massnahmen. In einem Sicherheitskonzept beschreibt deshalb der Betrieb, wie er die von der Fachstelle BS definierten Anforderungen an die Informationssicherheit umsetzen wird (s. auch Art. 55). In der Regel haben die Betriebe in verschiedensten Bereichen bereits Sicherheitsmassnahmen getroffen, die durch die Fachstelle BS nur noch überprüft und wo nötig ergänzt werden müssen. Alle Massnahmen werden im Konzept festgehalten. Die notwendigen Daten zur Kontrolle und Genehmigung des Sicherheitskonzepts erhebt die Fachstelle BS direkt beim Betrieb.

Art. 61 Personensicherheitsprüfungen

Die Personen des Betriebs werden gestützt auf Artikel 30 Absatz 1 Buchstabe c oder Artikel 30 Absatz 2 überprüft. Die Prüfstufe richtet sich nach Artikel 31. Bei der Prüfstufe darf kein Unterschied zwischen internen und externen Mitarbeitenden gemacht werden. Die Fachstelle BS entscheidet im Anschluss an die PSP verbindlich, ob die geprüfte Person mit der sicherheitsempfindlichen Tätigkeit betraut werden darf. Wird das BSV in Anwendung von Artikel 59 Absatz 3 eingestellt, ist die Auftraggeberin zuständig.

5. Abschnitt: Betriebssicherheitserklärung

Art. 62 Erteilung der Betriebssicherheitserklärung

Die Erteilung bzw. Nichterteilung der BSE stellt – anders als die Sicherheitserklärung im Bereich der PSP – eine Verfügung nach Artikel 5 VwVG dar, weil sie für die Beteiligten unmittelbare Rechtswirkungen entfaltet. In der bisherigen Praxis kam es nur selten vor, dass ein Betrieb die Sicherheitsmassnahmen nicht umgesetzt hat oder ihm die BSE nicht erteilt wurde. Kommt dies aber tatsächlich vor, muss die Fachstelle BS dem Betrieb eine Nachfrist gewähren, um seinen Pflichten nachzukommen, bevor die Verweigerung der BSE verfügt werden darf. Ist der Betrieb mit der Verfügung der Fachstelle BS nicht einverstanden, steht ihm die Beschwerde an das Bundesverwaltungsgericht offen (Art. 70 Abs. 1 Bst. d). Die Verfügung wird auch der Auftraggeberin mitgeteilt, weil sie den Betrieb, dem die BSE verweigert wird, nicht mit dem sicherheitsempfindlichen Auftrag betrauen darf (s. Art. 63). Zu diesem Zeitpunkt hat die Auftraggeberin möglichweise bereits viel Geld in das Projekt investiert. Sie ist (im Gegensatz zu Art. 59 Abs. 1) deshalb ebenfalls zur Beschwerde berechtigt.

Mit der Befristung der Geltungsdauer der BSE auf fünf Jahre soll sichergestellt werden, dass regelmässig eine Neubeurteilung der sicherheitsmässigen Eignung vorgenommen wird. Mit dieser kann wesentlichen Änderungen beim Betrieb, die einen Einfluss auf die Informationssicherheit haben, Rechnung getragen werden.

Art. 63 Ausführung des sicherheitsempfindlichen Auftrags

Die Auftraggeberin ist an den Entscheid der Fachstelle BS gebunden. Sie darf einen Betrieb, dem die BSE verweigert wird, nicht mit einem sicherheitsempfindlichen Auftrag betrauen (s. Art. 62 Abs. 2). Umgekehrt sind Betriebe mit einer gültigen BSE berechtigt, sicherheitsempfindliche Aufträge auszuführen, wenn sie den entsprechenden Zuschlag erhalten und der Vertrag zustande kommt. Die BSE muss vorliegen, bevor die Auftraggeberin den Betrieb den Auftrag ausführen lässt. Diese Regelung entspricht dem Grundsatz von Artikel 34 Absatz 3 im Bereich der PSP.

Art. 64 Pflichten des Betriebs

Betriebe mit einer BSE sind zur Mitwirkung und Zusammenarbeit verpflichtet. Ihre wichtigste Pflicht besteht darin, die Massnahmen des Sicherheitskonzepts laufend umzusetzen. Sie müssen zudem der Fachstelle BS alle Änderungen melden, die für

die Wahrung der Informationssicherheit bei der Erfüllung des sicherheitsempfindlichen Auftrages wesentlich sind. Zu melden sind beispielsweise neue Mitarbeitende, die mit sicherheitsempfindlichen Tätigkeiten betraut werden sollen, damit bei ihnen eine PSP durchgeführt wird. Weiter muss der Betrieb unverzüglich informieren, wenn sich ein sicherheitsrelevanter Vorfall ereignet hat.

Art. 65 Kontrollen und Schutzmassnahmen

Die Fachstelle BS muss die Einhaltung der auftragsrelevanten, im Sicherheitskonzept vorgesehenen Sicherheitsmassnahmen im Betrieb überwachen. Die Überprüfung kann naturgemäss auch unangemeldet erfolgen. Sie darf nur in Begleitung bzw. in Anwesenheit einer zum Betrieb gehörenden Person, in der Regel mit dem Sicherheitsbeauftragten, durchgeführt werden. Die Fachstelle BS kann, wenn konkrete Anhaltspunkte für eine Gefährdung der Informationssicherheit vorliegen, die erforderlichen Schutzmassnahmen treffen. Sie kann beispielsweise die sofortige Einschliessung oder Rückgabe bestimmter Unterlagen oder Materialien verfügen. Falls die Informationssicherheit anderweitig nicht gewährleistet werden kann, ist sie gar befugt, bestimmte Unterlagen oder Materialien sicherzustellen. Dies gilt auch für Fälle, in denen nach dem Konkurs eines Betriebs noch vorhandene Unterlagen oder Informatikmittel rasch aus der Konkursmasse ausgeschieden werden müssen.

Art. 66 *Vereinfachtes Verfahren bei der Vergabe weiterer sicherheitsempfindlicher Aufträge*

Betriebe mit einer gültigen BSE gelten grundsätzlich als sicher. Ihre Eignung wird nicht neu beurteilt. In derartigen Fällen muss jedoch geprüft werden, ob das bestehende Sicherheitskonzept angepasst werden muss. Dies wäre beispielsweise dann der Fall, wenn der betreffende Betrieb bis anhin «nur» «vertraulich» klassifizierte Informationen bearbeiten musste, nun aber neu auch «geheim» klassifizierte Informationen bearbeiten muss. Es kommt ein vereinfachtes Verfahren zur Anwendung, das der Bundesrat auf Verordnungsebene regeln wird.

Art. 67 Internationale Betriebssicherheitsbescheinigung

Betriebe mit Sitz in der Schweiz, die sich für einen sicherheitsempfindlichen Auftrag aus dem Ausland bewerben, müssen den dortigen Behörden immer häufiger eine Sicherheitserklärung der Schweizer Behörden vorweisen. Artikel 67 schafft die nötige Grundlage für die Ausstellung entsprechender Bescheinigungen, die den Schweizer Firmen Zugang zu Aufträgen im Ausland eröffnen können.

Art. 68 Widerruf der Betriebssicherheitserklärung

Der Widerruf der BSE im Verlauf der Ausführung eines Auftrags ist äusserst selten. Kommt es jedoch dazu, so wird eine entsprechende Verfügung erlassen, gegen welche die Beschwerde an das Bundesverwaltungsgericht offensteht. Das Beschwerderecht steht auch der Auftraggeberin zu, da ein Widerruf auch für sie nachteilig sein kann. Sie kann beispielsweise ein erhebliches finanzielles Interesse daran haben, dass die BSE nicht widerrufen wird. Die Auftraggeberin muss jedoch dem

Betrieb unverzüglich die Auftragsausführung entziehen, um das Risiko zu vermeiden. Dem Betrieb steht kein Anspruch auf finanzielle Entschädigung zu. Die bisher geleisteten Arbeiten müssen jedoch vergütet werden. Die Anwendung von Artikel 59 Absatz 3 (Auftragserteilung an einen ungeeigneten Betrieb) bleibt vorbehalten, weil es möglich ist, dass die Auftraggeberin keine wirtschaftlich vertretbare Alternative zum betroffenen Betrieb hat. In diesem Fall werden die Kontroll- und Durchsetzungsbefugnisse der Fachstelle BS der Auftraggeberin übertragen.

6. Abschnitt: Wiederholung des Verfahrens und Rechtsschutz

Art. 69 Wiederholung des Verfahrens

Während des Wiederholungsverfahrens wird die Auftragserfüllung nicht gestoppt. Ist der Auftrag fast erfüllt und wurden dem Betrieb keine neuen sicherheitsempfindlichen Aufträge erteilt, wird die Fachstelle BS aus Gründen der Verfahrensökonomie das Verfahren nicht wiederholen. Besteht konkreter Grund zur Annahme, dass in Folge wesentlicher Änderungen beim Betrieb neue Sicherheitsrisiken entstanden sind, ist das Verfahren ebenfalls zu wiederholen.

Art. 70 Rechtsschutz

Den Organen des Betriebs werden grundsätzlich dieselben Rechte wie im Rahmen der PSP (s. Art. 45) gewährt. Gegen die Verfügungen der Fachstelle BS kann beim Bundesverwaltungsgericht Beschwerde geführt werden. Mit dieser Norm wird implizit festgehalten, dass vorliegend die Ausnahmebestimmung von Artikel 32 Absatz 1 Buchstabe a des Verwaltungsgerichtsgesetzes (grundsätzliche Unzulässigkeit der Beschwerde gegen Verfügungen auf dem Gebiet der inneren und äusseren Sicherheit des Landes) nicht zur Anwendung kommt. Beruht jedoch eine Verfügung der Fachstelle BS auf nachrichtendienstlichen Informationen, die nicht an den Betrieb oder an die Öffentlichkeit gelangen sollen, so finden die entsprechenden Verfahrensbestimmungen Anwendung (Art. 27 und 28 VwVG).

7. Abschnitt: Bearbeitung von Personendaten

Art. 71 Informationssystem zum Betriebssicherheitsverfahren

Die heutige Rechtsgrundlage für das seit Jahren existierende System (Art. 150 ff. MIG) soll aus systematischen Gründen in das ISG verschoben werden. Weil das System besonders schützenswerte Personendaten enthalten kann, bedarf es einer formell-gesetzlichen Grundlage (Art. 17 Abs. 2 DSG).

Art. 72 Zugriffsrechte und Datenbekanntgabe

Die Auftraggeberinnen erhalten Zugang zu den Daten, die sie betreffen, sowie zur Liste mit allen Betrieben, die über eine BSE verfügen. Dies ermöglicht es ihnen, sich rasch einen Überblick darüber zu verschaffen, ob ein Betrieb bereits über eine

BSE verfügt. Der Bundesrat kann in seinem Ausführungsrecht bestimmte Betriebe ermächtigen, selbst PSP für ihren Bereich einzuleiten. In diesem Fall müssen diese Betriebe Zugang zu bestimmten Daten des Informationssystems erhalten. Bereits mit dem heutigen System können zudem die Sicherheitsbeauftragen gewisser Betriebe den Prüfungsentscheid und die Prüfstufe der Mitarbeitenden ihres Betriebs abrufen.

Art. 73 Datenaufbewahrung, -archivierung und -vernichtung

Die Regelung der Datenaufbewahrung, -archivierung und -vernichtung entspricht *mutatis mutandis* der für die PSP vorgeschlagenen Regelung (s. Art. 48).

8. Abschnitt: Bestimmungen des Bundesrats

Art. 74

Die Erläuterungen zu Artikel 49 im Bereich der PSP gelten hier auch für das BSV.

5. Kapitel: Kritische Infrastrukturen

Die Artikel 75–81 regeln die Aufgaben und Kompetenzen des Bundes bezüglich der Unterstützung der KI-Betreiberinnen im Bereich der Informationssicherheit. Die Teilnahme der KI-Betreiberinnen an der öffentlich-privaten Partnerschaft mit dem Bund und der Bezug der Dienstleistungen des Bundes erfolgt auf freiwilliger Basis. Zur NCS, siehe Ziffer 1.1.2 und 1.2.7.

Art. 75 Aufgaben des Bundes

Das gesamtgesellschaftliche Interesse am zuverlässigen Funktionieren der KI spiegelt sich in der ersten Bestimmung dieses Kapitels: Der Bund will mit der Unterstützung der KI-Betreiberinnen gewährleisten, dass Netz- und Systemunterbrüche sowie Missbräuche selten, von kurzer Dauer, beherrschbar und von geringem Schadensausmass sind. Es geht dabei um die technische Funktionalität der Informationsinfrastrukturen, mithin des Internets, und dass Informatikmittel nicht ohne Wissen und Willen der berechtigten Nutzer durch Dritte verwendet werden. Diese Unterstützung umfasst insbesondere die in Absatz 2 aufgeführten Dienstleistungen. Sie kann demgegenüber nicht herangezogen werden, um inhaltsbezogenen Missbrauch wie Urheberrechtsverletzungen oder Ehrverletzungsdelikte zu bekämpfen.

Nach Absatz 3 führt der Bund einerseits einen nationalen Frühwarndienst, der die Bedrohungslage im Bereich der Informationssicherheit laufend analysiert und Informationen über identifizierte Bedrohungen und Gefahren zuhanden der KI-Betreiberinnen aufbereitet, um deren Informationssicherungs- und Risikomanagementprozess zu unterstützen. Andererseits betreibt er eine Anlaufstelle für präventive und reaktive Massnahmen im Bereich der technischen Informationssicherheit, die technische Analysen – zum Beispiel von Schadsoftware – vornehmen und Empfehlungen für konkrete technische Massnahmen zur Absicherung von Informatikmit-

teln, Abwehr von Gefahren oder Erkennung von Vorfällen abgeben kann. Die mit Aufgaben nach Absatz 3 beauftragten Stellen dürfen zur Erkenntnisgewinnung beispielsweise verwundbare Informatikmittel (Honeypots) in Netzwerken betreiben sowie infizierte Informatikmittel unter Beobachtung laufen lassen, um die Funktions- und Verhaltensweisen von Schadsoftware und Angreifern zu analysieren.

Nach Absatz 4 sorgt der Bundesrat dafür, dass ein sicherer Informationsaustausch zwischen Bund und KI-Betreiberinnen sowie zwischen den KI-Betreiberinnen selbst stattfinden kann. Dieser Absatz begründet keine eigenständige Kompetenz zur Datenbearbeitung, sondern bietet die gesetzliche Grundlage für das Bereitstellen einer sicheren Informationsaustauschplattform. Bedrohungen, Gefahren und Verwundbarkeiten betreffen häufig nicht nur ein einzelnes Ziel, sondern mehrere in einem bestimmten Sektor tätige Organisationen, möglicherweise auch sektorübergreifend alle KI-Betreiberinnen. Die Inanspruchnahme der Dienstleistungen nach Artikel 75 und die Teilnahme an der öffentlich-privaten Partnerschaft beruht dennoch vollständig auf Freiwilligkeit. Der Grundsatz des Handelns in Eigenverantwortung der KI wird also implizit wiederholt. Durch einen permanenten Informationsaustausch sollen Transparenz und Vertrauen geschaffen werden. Dadurch gewinnen nicht nur die KI-Betreiberinnen an Knowhow, sondern auch die Bundesbehörden in ihrer Eigenschaft als Inhaberinnen und Betreiberinnen von KI. Sie können wichtige Informationen zur Beurteilung ihrer eigenen Risiken und zur Abwehr von Gefahren erhalten.

Bei den zuständigen Stellen handelt es sich heute um MELANI, die das ISB mit dem NDB gemeinschaftlich betreibt. In Anbetracht der Organisationsautonomie des Bundesrats sollen diese Stellen nicht im Gesetzestext, sondern auf Verordnungsebene bezeichnet werden (Abs. 5). Diese Stellen sollen gegenüber den KI-Betreiberinnen weiterhin einheitlich auftreten. Es steht dem Bundesrat demgegenüber frei, wie er diese Stellen intern organisieren und wo er sie ansiedeln will.

Art. 76 Bearbeitung von Personendaten

Zur Erfüllung ihrer Aufgaben nach Artikel 75 müssen die zuständigen Stellen des Bundes Informationen bezüglich Bedrohungen und Gefahren sowie Indikatoren für Vorfälle im Bereich der Informationssicherheit bearbeiten und sie mit den Betreiberinnen von KI austauschen können. Solche Informationen bestehen vorwiegend aus Adressierungselementen nach Artikel 3 Buchstabe f FMG (z. B. IP-Adressen, E-Mail-Adressen, Domainnamen). Diesen Adressierungselementen ist inhärent, dass sie sich auf bestimmte oder bestimmbare Personen beziehen, respektive auf Geräte oder Fernmeldeanschlüsse, die wiederum einer bestimmten oder bestimmbaren Person zugeordnet werden können. Endkunden beziehen Adressierungselemente überdies meistens von Fernmelde- oder anderen Dienstanbieterinnen, die ihrerseits aufgrund des Adressierungselements – in der Regel durch Konsultation von öffentlichen Verzeichnissen – bestimmt werden können. Entsprechend können Adressierungselemente als Personendaten betrachtet werden, für deren Bearbeitung durch Bundesorgane eine gesetzliche Grundlage nötig ist (Art. 4 Abs. 3 und 17 Abs. 1 DSG). Die Qualifizierung von Adressierungselementen ist in Lehre und Praxis umstritten und kann in konkreten Fällen – nicht zuletzt aufgrund der teils stark divergierenden administrativen Vergabeprozesse und Verzeichnispflichten bei

ausländischen Adressierungselementen – sehr unterschiedlich beurteilt werden. Deshalb ist im ISG die Auslegung, ob Adressierungselemente Personendaten sind, bewusst weit gefasst, um die Rechtmässigkeit der Datenbearbeitung zu gewährleisten und den mit der Bearbeitung beauftragten Stellen Rechtssicherheit zu bieten.

Absatz 1 sieht entsprechend vor, dass die Stellen nach Artikel 75 Absatz 5 die nötigen Adressierungselemente sowie die damit zusammenhängenden Personendaten bearbeiten dürfen. Die Bearbeitung von Daten nach diesem Kapitel ist nicht mit personen- und gesprächsinhaltsbezogenen geheimen Überwachungsmassnahmen nach der StPO oder dem BÜPF vergleichbar. Bei den hier angesprochenen Daten handelt es sich typischerweise um Programmanweisungen in Form von Computer(schad)codes und Adressierungselementen, die im Zusammenhang mit einem Vorfall (z. B. Missbrauch eines Informatikdiensts oder Infektion eines Informatikmittels mit Schadsoftware) in Erscheinung getreten sind und MELANI gemeldet wurden. Durch Austausch solcher Daten soll festgestellt werden können, ob schutzwürdige Systeme von KI-Betreiberinnen Verbindungen mit diesen Adressierungselementen hatten (Abgleich mit Log-Daten aus den internen Netzwerken der KI-Betreiberinnen), da dies als *Hin*weis (nicht *Be*weis) auf eine Verletzung der Informationssicherheit dient. Solchen Hinweisen muss dann durch weitere Abklärungen in den eigenen Systemen nachgegangen werden, um zum Beispiel Infektionen mit Schadsoftware im eigenen Netzwerk zu entdecken.

In Absatz 2 wird im Sinne von Artikel 17 Absatz 2 DSG den zuständigen Stellen die Kompetenz zur Bearbeitung von Adressierungselementen und zusammenhängenden Personendaten eingeräumt, die als besonders schützenswert betrachtet werden können.

- Buchstabe a: Angriffe auf Informatikmittel und -systeme sind meistens finanziell motiviert. Es kommt jedoch oft vor, dass Personen nicht primär mit Bereicherungsabsicht, sondern aus religiösen, weltanschaulichen oder politischen Gründen einen Angriff planen oder durchführen. Dies ist zum Beispiel der Fall bei sogenannten «Hacktivisten», die Informatikdienstleistungen unterbrechen, finanzielle Schäden verursachen oder vertrauliche Daten von Angriffsopfern veröffentlichen, um öffentlich Aufmerksamkeit für ihre politischen Anliegen zu erlangen. Da die Absicht hinter einem Angriff für die Einschätzung einer Bedrohung und des damit einhergehenden Risikos wesentlich sein kann, soll MELANI Angaben bezüglich der Gesinnung bearbeiten dürfen, wenn dies zur Bewertung von konkreten Bedrohungen und Gefahren erforderlich ist.
- Buchstabe b: Angriffe gegen Informatikmittel und -Infrastrukturen werden in der Regel strafrechtlich verfolgt. Stehen Personendaten im Zusammenhang mit einer strafrechtlichen Verfolgung, gelten sie nach Artikel 3 Buchstabe c Ziffer 4 DSG als besonders schützenswerte Personendaten, für deren Bearbeitung die Bundesorgane eine formell-gesetzliche Grundlage benötigen. Da jedoch mit einer Strafanzeige allein die Gefahr zumindest kurzfristig nicht gebannt wird, ist die Information der KI-Betreiberinnen bezüglich dieser Angriffsvektoren essenziell, damit diese ihre Systeme schützen und allenfalls bereits erfolgte Angriffe erkennen können. Auch wenn der Umstand nicht kommuniziert wird, dass betreffend ein Adressierungselement ein Ver-

fahren eingeleitet oder eine Sanktion verhängt wurde, kann eine Informationsempfängerin oder ein Informationsempfänger aus der Angabe, dass ein Adressierungselement für kriminelle Zwecke verwendet wurde, schliessen, dass ein entsprechendes Verfahren läuft. Die hier gewährte Kompetenz soll verhindern, dass dieser Austausch nicht mehr stattfinden kann, sobald eine Strafanzeige bezüglich eines Adressierungselements erfolgt oder ein administratives Verfahren eingeleitet wird.

Absatz 3 ermöglicht die Datenbearbeitung, ohne dass betroffene Personen über die Bearbeitung informiert werden. Das Regime der Vergabe von Adressierungselementen ist in vielen Fällen mehrstufig. An der Vergabe von Internet-Domainnamen sind beispielsweise eine Vielzahl von Personen beteiligt, die typischerweise durch Konsultation von öffentlichen Verzeichnissen (WHOIS-Abfragen) bestimmt werden können: Registrierungsstelle, Registrar, Registrant, technischer Kontakt, administrativer Kontakt. Ist die Internet-Domain aktiv, steht sie zudem in Verbindung mit einer IP-Adresse und den aufgrund dieser Adresse (wiederum durch Konsultation von öffentlichen Verzeichnissen) bestimmbaren Personen. Es ist nicht verhältnismässig, bei jeder Bearbeitung eines Domainnamens alle damit zusammenhängenden und bestimmbaren natürlichen und juristischen Personen zu informieren – vielfach werden jedoch gewisse betroffene Personen gezielt kontaktiert, damit sie Massnahmen zur Gefahrenabwehr, zur Unterbindung weiteren Missbrauchs oder zur Wiederherstellung des rechtmässigen Zustandes ergreifen können. Die Identifikation der (End-)Benutzerin oder des (End-)Benutzers ist demgegenüber insbesondere bei im Ausland registrierten Adressierungselementen regelmässig nicht möglich oder mit erheblichem Aufwand verbunden. Sie ist aber für die Gefahrenabwehr durch passive Schutzmassnahmen nicht nötig. Wenn keine Identifikation stattfindet, kann die Datenbearbeitung der betroffenen Person weder ersichtlich gemacht, noch kann sie über die Bearbeitung informiert werden.

Liegt hingegen nach Absatz 4 der Verdacht vor, dass ein (Schweizer) Adressierungselement oder ein dieses Adressierungselement verwendendes Gerät von Unberechtigten missbraucht wird, soll die rechtmässige Nutzerin oder der rechtmässige Nutzer des Adressierungselements identifiziert und über den Missbrauch informiert werden. Die Identifikation und Information muss jedoch nicht zwangsläufig durch die zuständigen Behörden erfolgen: Beispielsweise kann im Fall von dynamischen IP-Adressen die vermittelnde Fernmeldedienstanbieterin informiert werden, damit diese die entsprechenden Angaben den betroffenen Kundinnen und Kunden weiterleiten kann. Den Kundinnen und Kunden wird dadurch ermöglicht, Massnahmen zur Unterbindung weiteren Missbrauchs zu ergreifen und bei Vorliegen einer Straftat diese anzuzeigen und gegebenenfalls einen Strafantrag zu stellen.

Die vorliegende Bestimmung ist entsprechend als *Lex Specialis* zu Artikel 4 Absatz 4 und Artikel 18*a* DSG zu sehen.

Art. 77 Zusammenarbeit im Inland

Artikel 77 erlaubt den zuständigen Stellen, zur Erfüllung ihrer Aufgaben die definierten Arten von Daten KI-Betreiberinnen bekanntzugeben, damit diese sich schützen können. Weiter dürfen sie Daten an Anbieterinnen und Betreiberinnen von

Informatikdiensten bekanntgeben, damit diese nach einem Missbrauch ihrer Systeme sowie derjenigen ihrer Kundinnen und Kunden weitere Missbräuche verhindern können.

Absatz 3 räumt den KI-Betreiberinnen sowie den Anbieterinnen und Betreiberinnen von Informatik- und Kommunikationsdiensten das Recht ein, Informationen, die im Zusammenhang mit Gefahren und Vorfällen im Bereich der Informationssicherheit stehen, freiwillig an die Stellen nach Artikel 75 zu melden. Sie dürfen zur Abwehr von Gefahren und entsprechend zur Verhinderung von Schäden Angaben über von ihnen erbrachte Dienstleistungen, Vermittlungen und andere Vorgänge machen. Diese Bestimmung ermöglicht die rechtmässige Bearbeitung entsprechender Personendaten und weiterer Angaben. Ein Anwendungsfall dieser Bestimmung ist, wenn bei einem Speicheranbieter (Hosting-Provider) ein Steuerserver (Command & Control Server) festgestellt wird, mit welchem ein Netzwerk von mit Schadsoftware infizierten Heimcomputern (Bot-Netz) gesteuert wird. Diesfalls könnte der Hosting-Provider Protokoll-Dateien an MELANI liefern, aus welchen die IP-Adressen der infizierten Heimcomputer ersichtlich sind. Diese würden dann an die entsprechenden Fernmeldedienstanbieterinnen weitergegeben, damit diese ihre Kundinnen und Kunden informieren können. Weiter könnte der Hosting-Provider Konfigurationsdateien und Kommunikationsmuster des Steuerservers liefern, welche die Erkennung weiterer Bot-Netze ermöglichen. Auf polizeiliche Untersuchungen und gerichtliche Verfahren finden die jeweiligen Regeln für die Beweiserhebung Anwendung. Strafverfolgungsbehörden können keine Daten bei MELANI herausverlangen, sondern müssen sie bei der ursprünglichen Datenhalterin oder beim ursprünglichen Datenhalter beweiskräftig erheben. Erlaubt die Datenlieferantin explizit eine Weitergabe, kann MELANI die Daten selbstständig den zuständigen Strafverfolgungsbehörden bekanntgeben.

Art. 78 Internationale Zusammenarbeit

Der Schutz kritischer Infrastrukturen vor Gefahren im Bereich der Informationssicherheit ist eine Aufgabe, die kein Unternehmen und kein Land allein lösen kann. Die globale Natur des Internets führt dazu, dass Vorfälle typischerweise nicht lokal oder national beschränkt sind, sondern KI-Betreiberinnen in verschiedenen Ländern betreffen. In dieser Hinsicht haben viele Staaten ein gemeinsames Interesse und kooperieren bereits heute freiwillig bei der Erkennung und Behebung von Vorfällen. Es besteht keine Pflicht zur Lieferung bestimmter Daten. Daran ändert dieses Gesetz nichts. Artikel 78 erteilt MELANI lediglich eine explizite Kompetenz zu internationaler Zusammenarbeit und entsprechendem Datenaustausch. Auch wenn in diesem Rahmen regelmässig Daten ausgetauscht werden, kann in jedem Einzelfall auf eine Bekanntgabe verzichtet werden, wenn diese als nicht mit Artikel 6 DSG vereinbar oder als unverhältnismässig beurteilt wird. Ausländische Stellen müssen die ausschliesslich bestimmungsgemässe Verwendung der erhaltenen Daten gewährleisten. Im internationalen Verhältnis hat sich das so genannte *Traffic Light Protocol* etabliert, gemäss dem beim Datenaustausch Anweisungen mitgeliefert werden, an wen die Daten weitergegeben werden dürfen (z. B. nur an den Energiesektor).

Der zwischenbehördlichen Informationsaustauch umfasst in erster Linie Adressierungselemente. Dabei ist zu vermerken, dass MELANI ihren internationalen Part-

nern nur äusserst selten Adressierungselemente mitteilt, die sich auf Personen, Firmen oder Informatikmittel in der Schweiz beziehen. Bedrohungen und Gefahren, die aus der Schweiz hervorgehen, wird nämlich im Rahmen der Zusammenarbeit im Inland begegnet. Der Informationsaustausch umfasst aber auch andere Informationen, die für die Gewährleistung der Informationssicherheit bei den KI wesentlich sind (z. B. Beschreibungen und Einschätzungen von Bedrohungen, Anweisungen zur technischen Erkennung und Behebung von Vorfällen, konkrete Vorfallanalysen und Sicherheitsempfehlungen, Analysen betreffend Sicherheitslücken und Verwundbarkeiten). Zumal der Zweck der internationalen Zusammenarbeit dem Schutz und der Gefahrenabwehr dient, stellt Absatz 3 klar, dass für rechtliche Verfahren die Bestimmungen über die Amts- und Rechtshilfe gelten. Damit wird festgehalten, dass dieses Gesetz nicht zur Umgehung von entsprechenden Voraussetzungen verwendet werden kann.

Art. 79 Informationssystem zur Unterstützung von kritischen Infrastrukturen

Um eine möglichst hohe Sicherheit sowie Nachvollziehbarkeit der Datenbearbeitung gewährleisten zu können, ist der Einsatz eines spezifischen Informationssystems angezeigt. Der Austausch von Informationen kann jedoch auch über andere Kanäle erfolgen, z.B. über eine verschlüsselte Mail-Nachricht oder ein persönliches Treffen. Die Auflistung der im Informationssystem enthaltenen Informationen illustriert, dass es sich dabei nicht unbedingt um Personendaten handelt und auch Adressierungselemente nicht grundsätzlich nach Personen erschlossen sind. Jedoch können insbesondere Anweisungen zur technischen Erkennung von Vorfällen Adressierungselemente enthalten, bei welchen durch Konsultation von öffentlichen Verzeichnissen mit diesen Adressierungselementen in Verbindung stehende Personen bestimmt werden können. Obwohl es sich bei diesen Personen häufig nicht um die Endnutzerinnen und Endnutzer der Adressierungselemente handelt, sind sie aufgrund der Adressierungselemente bestimmbar und diese entsprechend als Personendaten zu qualifizieren.

Art. 80 Datenaufbewahrung und -archivierung

Personendaten sollen nur so lange aufbewahrt werden, wie dies für die Erkennung von Vorfällen und die Abwehr von Gefahren zweckmässig ist. Die Festlegung der maximalen Aufbewahrungsdauer auf fünf Jahre setzt einen grundsätzlichen zeitlichen Rahmen. In den meisten Fällen sind bearbeitete Daten sehr kurzlebig und können kurz nach der Bearbeitung wieder gelöscht werden. Demgegenüber können vereinzelte Angaben zu Angriffsvektoren über mehrere Jahre Gültigkeit haben. Die Zweckmässigkeit einer andauernden Datenbearbeitung kann jeweils bei den Kontrollen nach Artikel 81 Buchstabe d durch eine externe Stelle überprüft werden.

Art. 81 Bestimmungen des Bundesrats

Der Bundesrat soll auf Verordnungsstufe die Aufgabenteilung und die Zusammenarbeit der Stellen nach Artikel 75 Absatz 5 regeln. Im NDG sind Kompetenzen des NDB im Bereich des Schutzes der KI vorgesehen. Die entsprechende Aufgabenteilung, die Zusammenarbeit und der Informationsaustausch müssen im Detail vom

Bundesrat festgelegt werden. Um Transparenz zu schaffen und Rechtssicherheit zu gewährleisten, regelt der Bundesrat die Datenbearbeitung sowie den Austausch von Daten zwischen diesen Stellen, deren Bekanntgabe an KI-Betreiberinnen sowie ausländische und internationale Stellen wie auch die dabei zu berücksichtigende Datensicherheit. Er sorgt auch für eine periodische externe Kontrolle der Rechtmässigkeit der Datenbearbeitung. Die Kontrollinstanz kann der Bundesrat frei wählen, sofern diese über die nötige Unabhängigkeit gegenüber MELANI verfügt.

6. Kapitel: Organisation und Vollzug

1. Abschnitt: Organisation

Art. 82 Informationssicherheitsbeauftragte

Zur Rolle der Informationssicherheitsbeauftragten siehe Ziffer 1.2.9. Das ISG greift aufgrund des überwiegenden Bedarfs nach einer integralen Steuerung der Umsetzung des Gesetzes in die Organisationsautonomie der Behörden ein: Es verlangt, dass die Behörden, die Departemente und die BK für ihren Zuständigkeitsbereich eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten und eine Stellvertretung bezeichnen. Da einerseits eine wirksame integrale Steuerung der Informationssicherheit sowohl politisches, rechtliches, organisatorisches als auch technisches Wissen voraussetzt und andererseits durch die Informationssicherheitsbeauftragten sehr viele Aufgaben wahrgenommen werden müssen, verlangt die praktische Umsetzung, dass mindestens zwei Personen pro Behörde diese Aufgaben wahrnehmen. Es wird jedoch nicht verlangt, dass beide Personen in vollem Umfang dafür eingesetzt werden.

Der Bundesrat selbst muss ebenfalls eine Beauftragte oder einen Beauftragten bezeichnen. Hingegen soll die Aufsichtsbehörde der Bundesanwaltschaft aufgrund ihres begrenzten Personalbestands nicht dazu verpflichtet werden. Die eidgenössischen Gerichte werden nicht einzeln aufgeführt, weil es unverhältnismässig wäre, von den personell ebenfalls relativ kleinen Gerichten solche Stellen zu verlangen. Das ISG lässt es also zu, dass die eidgenössischen Gerichte für alle Gerichte beispielsweise eine einzige Stelle bezeichnen oder einen anderen Ansatz wählen, der die Behördenautonomie wahrt. Die Bundesämter und die dezentrale Bundesverwaltung werden durch das Gesetz ebenfalls nicht verpflichtet, Beauftragte zu bezeichnen. Der Bundesrat muss im Rahmen der Erfüllung seiner Organisationspflicht auf Verordnungsebene entscheiden, wie die Informationssicherheit bis auf diese Stufe organisiert und gesteuert werden soll.

Absatz 2 umschreibt in allgemeiner Form den Aufgabenbereich und die Zuständigkeit der Informationssicherheitsbeauftragten:

– Buchstabe a betont, dass die Entscheidkompetenzen und die Verantwortung für die Entscheidungen im Bereich der Informationssicherheit nach wie vor bei der Linie, also bei den zuständigen Behörden und den ihnen nachgeordneten Stellen liegen sollen. Die Informationssicherheitsbeauftragten sollen die Linie aber fachlich beraten und unterstützen.

- Buchstabe b legt fest, dass die Informationssicherheitsbeauftragten im Auftrag ihrer Behörde oder Organisation die Informationssicherheit sowie das entsprechende Risikomanagement fachtechnisch steuern müssen.
- Buchstabe c sieht vor, dass die Informationssicherheitsbeauftragten eine allgemeine Pflicht zur Überprüfung der Einhaltung der Vorschriften dieses Gesetzes haben, dass sie ihrer Behörde Bericht erstatten und bei Handlungsbedarf Antrag stellen müssen. Dazu gehört auch die Liste der Funktionen, die eine sicherheitsempfindliche Tätigkeit einschliessen. Audits und Kontrollen sind immer ein heikles Thema. Ihre Durchführung muss grundsätzlich von der Linie angeordnet werden. Die Informationssicherheitsbeauftragten sollen zu diesem Zweck ihrer Behörde oder Organisation jährlich einen Auditplan vorlegen, in dem die Auditprioritäten und die dafür erforderlichen Ressourcen ausgewiesen werden.
- Buchstabe d hält fest, dass die Informationssicherheitsbeauftragten sicherheitsrelevante Vorfälle sowohl der Fachstelle des Bundes für Informationssicherheit, der Konferenz der Informationssicherheitsbeauftragten als auch den Stellen, welche die Aufgaben bezüglich Informationssicherheit bei KI wahrnehmen, melden können. Es wird also im behördenübergreifenden Rahmen aufgrund der Behördenautonomie auf eine Melde*pflicht* verzichtet. Der Bundesrat kann für die Bundesverwaltung und die Armee auf Verordnungsebene eine Meldepflicht vorsehen, wenn er dies für notwendig hält.

Die Informationssicherheitsbeauftragten müssen in ihrer Stellung und ihrer Aufgabenerfüllung unabhängig sein und dürfen keinen materiellen Interessenkonflikten ausgesetzt werden. Eine fehlende Funktionstrennung führt in der Praxis immer wieder zu Problemen beim Vollzug der Sicherheitsvorgaben. So ist beispielsweise heute noch die Mehrheit der Informatiksicherheitsbeauftragten den Informatikleitungen unterstellt. Dabei verfolgen die Informatikverantwortlichen oft andere Prioritäten als die Sicherheit und aufgrund der Dringlichkeit oder der Kosten wird in Projekten regelmässig auf die Umsetzung der erforderlichen Sicherheitsmassnahmen verzichtet. Die Informationssicherheitsbeauftragten sollten auch nicht mit dem unmittelbaren Betrieb von Informatikmitteln beauftragt oder als Leiterinnen und Leiter von Projekten, die nicht primär die Informationssicherheit betreffen, eingesetzt werden, denn genau bei solchen Aufgabenkumulationen kollidieren die anders gelagerten Anforderungen des Betriebs regelmässig mit einer möglichst objektiven Beurteilung der Risiken. Mit dieser Regelung wird auch der Empfehlung 7 des Berichts der GPDel über die Informatiksicherheit beim NDB Rechnung getragen (s. Ziff. 1.1.4).

Die genaue Ansiedlung der Funktion ist den Behörden, den Departementen und der BK überlassen. Die Praxis zeigt jedoch, dass die Informationssicherheitsbeauftragten am effektivsten sind, wenn sie relativ nah an der Behördenleitung angesiedelt werden, weil sie so am besten die Geschäftsprozesse überblicken und die Geschäftsanforderungen beurteilen können. Es wäre zudem wünschenswert, die Informationssicherheitsbeauftragten so anzusiedeln, dass sie eine enge Koordination mit den bestehenden Risikomanagerinnen, Risikomanagern, Datenschutzberaterinnen, Datenschutzberatern, Sicherheitsbeauftragten (Objektsicherheit), Öffentlichkeitsberaterinnen und Öffentlichkeitsberatern sicherstellen können.

Art. 83 Konferenz der Informationssicherheitsbeauftragten

Zur Rolle der Konferenz siehe Ziffer 1.2.9. Nebst den verpflichteten Behörden sollen auch die Departemente, die BK und die Kantone vertreten sein. So kann sichergestellt werden, dass der Gesetzesvollzug auch innerhalb der Bundesverwaltung und in der Zusammenarbeit mit den Kantonen möglichst einheitlich erfolgt. Einsitz soll auch die oder der EDÖB nehmen, um die nötige Koordination mit dem Datenschutz systematisch und bereits bei der Erstellung der Vorgaben zu gewährleisten. Die Konferenz wird insbesondere für die Beurteilung der Vollzugstauglichkeit, Wirksamkeit und Wirtschaftlichkeit von vorgeschlagenen standardisierten Massnahmen (Art. 86) sorgen. Nur so können einheitliche Lösungen gefunden sowie die erforderliche Akzeptanz geschaffen werden. Die Fachstelle des Bundes für Informationssicherheit soll die Konferenz bei allen wichtigen Belangen der Informationssicherheit (z. B. in Fragen der Informationssicherheitsstrategie) einbeziehen. Die Konferenz soll auch dazu dienen, Trends und Risiken zu erkennen und vorausschauend entsprechende Massnahmen zu konzipieren. Sie kann für ihre Abklärungen und ihre Meinungsbildung auch unabhängige Expertinnen und Experten beiziehen.

Art. 84 Fachstelle des Bundes für Informationssicherheit

Zur Rolle der Fachstelle des Bundes für Informationssicherheit siehe Ziffer 1.2.9. Im behördenübergreifenden Rahmen verfügt die Fachstelle über keine Weisungs- und Durchsetzungsbefugnisse, weil solche Kompetenzen die zwingend einzuhaltende Vollzugsautonomie der verpflichteten Behörden verletzen würden.

- Buchstabe a: Die im Gesetz genannten Stellen können bei allen mit dem Vollzug verbundenen Fragen (inkl. PSP) die fachliche Unterstützung der Fachstelle anfordern. Die Fachstelle gilt somit als «Kompetenzzentrum» für die Informationssicherheit.
- Buchstabe b: Bei neuen Gefahren und Bedrohungen sowie bei der Entdeckung neuer Schwachstellen und Lücken soll die Information aller Beteiligten rasch und zielgerichtet erfolgen. Bei operativen Bedrohungen im technischen Bereich übernimmt MELANI diese Aufgabe für ihren Kundenkreis.
- Buchstabe c: Audits und Kontrollen sind grundsätzlich Sache der Behörden und Organisationen. Insbesondere für technische Sicherheitsaudits bei kritischen Bereichen ist jedoch hohes Fachwissen erforderlich, das nicht alle verpflichteten Behörden für sich beschaffen sollten: Die Bereitstellung eines Expertenpools ist wirtschaftlicher. Die Fachstelle darf von sich aus keine solchen Überprüfungen durchführen, sondern nur im Auftrag einer Behörde. Die Fachstelle soll nach Konsultation der Konferenz jährlich einen strategischen Prüfplan erstellen bzw. anpassen und ihn den zuständigen Behörden zur Genehmigung unterbreiten. Im strategischen Prüfplan werden die Auditprioritäten und die gegebenenfalls dafür erforderlichen Ressourcen ausgewiesen.
- Buchstabe d: Im Bereich der Technik kommen regelmässig neuartige Technologien zum Einsatz. Die Risiken, die mit dem Einsatz solcher neuartiger Mittel (Hard- und Software) verbunden sind, sind oft unklar. Für Technolo-

gien, die besonders wichtig sind oder die einen breiten Anwendungsbereich haben können, sollen die Behörden der Fachstelle die Durchführung einer Risikoanalyse beantragen können. Die Konferenz soll anschliessend die Ergebnisse prüfen.

– Buchstabe e: Es geht hier um eine operationelle Massnahme zur Standardisierung von Prozessen, Mitteln, Einrichtungen, Gegenständen und Dienstleistungen. Im Bereich der Informatik haben beispielsweise die Leistungserbringerinnen ein Interesse daran, zu wissen, ob die technischen Lösungen, die sie entwickeln, die Anforderungen des Bundes erfüllen. Ist das der Fall, so können sie sie für andere Projekte oder Informatikmittel wesentlich einfacher einsetzen. Dasselbe gilt auch für Gegenstände oder Dienstleistungen, die dem physischen Schutz dienen. Die Verantwortung, auch wenn die Anforderungen erfüllt sind, bleibt jedoch immer bei der Behörde oder Organisation, die solche Mittel einsetzt. Diese Kompetenz ist auch für das internationale Verhältnis erforderlich: Die Fachstelle soll die heute fehlende, international übliche Rolle der *National Accreditation Authority* wahrnehmen (s. Ziff. 5.2). So wird die Fachstelle amtlich bestätigen können, dass eingesetzte Mittel z. B. den Anforderungen der EU genügen.

– Buchstabe f: Bei übergreifenden Projekten wird die Federführung einer bestimmten Behörde oder Organisation übertragen. Da die Sicherheitsinteressen und -bedürfnisse der betroffenen Behörden und Organisationen oft unterschiedlich sind, muss sichergestellt werden, dass die Belange der Informationssicherheit professionell koordiniert werden. Die Fachstelle sollte diese Aufgabe übernehmen können, wenn es sich dabei um wichtige behördenübergreifende Projekte mit wesentlichem Bezug zur Informationssicherheit handelt.

– Buchstabe g: Da das entsprechende Fachwissen für den Bund in der vorgesehenen Fachstelle zusammengefasst werden soll, soll sie auch die Ansprechstelle des Bundes für die inländischen, ausländischen und internationalen Stellen im Bereich der Informationssicherheit sein. Sie wird auch die erforderlichen Rollen im internationalen zwischenbehördlichen Rahmen wahrnehmen (s. Ziff. 5.2). Andere Behörden oder Organisationen (z. B. EDA, NDB oder BAKOM) werden aber weiterhin Fachkontakte in diesem Bereich pflegen dürfen.

– Buchstabe h: Der Bundesrat muss regelmässig über den Stand der Informationssicherheit informiert werden, sodass er deren Wirksamkeit und Wirtschaftlichkeit beurteilen kann und entsprechend die Aufsichtsorgane der Bundesversammlung orientieren kann (s. Art. 89 Abs. 2).

Absätze 2–3: Der Bundesrat wird auch eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten einsetzen. Um allfällige Zuständigkeitskonflikte zu vermeiden soll diese Person gleichzeitig Chefin oder Chef der Fachstelle sein. Der Bundesrat wird zudem festlegen, welche Aufgaben die Fachstelle selbst oder in Zusammenarbeit mit anderen Bundesstellen erfüllen soll. Er wird auch über ihre Ansiedelung entscheiden. Schliesslich wird der Bundesrat auch entscheiden, ob

er der Fachstelle zusätzliche Aufgaben oder Durchsetzungsbefugnisse für die Bundesverwaltung und die Armee erteilen will.

2. Abschnitt: Vollzug

Art. 85 Ausführungsbestimmungen

Zum Vollzug siehe auch Ziffer 1.2.8. Die Behörden werden den Ausführungsbestimmungen des Bundesrats nicht unterstellt. Im Gegenzug müssen sie die für den Vollzug erforderlichen Ausführungsbestimmungen für ihren Bereich selbst erlassen. Mit dem zweiten Satz in Absatz 1 wird das Verhältnis zu Artikel 15 Absatz 2 RVOG geregelt. In Zusammenhang mit Artikel 70 ParlG sorgt Absatz 2 für eine klare Vollzugskompetenz bei der Bundesversammlung. In Absatz 3 wird das sogenannte *Opting-out* festgelegt. Die Ausführungsbestimmungen werden in Zusammenarbeit mit der Konferenz der Informationssicherheitsbeauftragten vorbereitet. Der Bundesrat wird zudem die anderen Behörden und die Kantone anhören, bevor er seine Ausführungsbestimmungen erlässt.

Art. 86 Standardanforderungen und -massnahmen

Da ein wichtiges Ziel dieses Gesetzes darin besteht, behördenübergreifend möglichst einheitliche Sicherheitsstandards zu erreichen, wird der Bundesrat beauftragt, standardisierte Anforderungen und Massnahmen nach dem Stand von Wissenschaft und Technik festzulegen. Es handelt sich dabei nicht um grundsätzliche organisatorische Anforderungen und Massnahmen, die auf Verordnungsebene festgelegt werden, sondern vorab um Anforderungen untergeordneter oder technischer Natur, beispielsweise:

- Standard für die Erhebung des Schutzbedarfs von Informationen in Bezug auf die vier Kriterien von Artikel 6 Absatz 2;
- Standardmethode für die Risikobewertung sowie Standards für organisatorische, personelle, technische und bauliche Massnahmen (Art. 8);
- Standards für bestimmte Prozesse und Mittel zum Schutz klassifizierter Informationen (Art. 11–15);
- Standards für den Grundschutz, für die Erstellung von Informationssicherheitskonzepten sowie für die Sicherheit von Informatikmitteln der Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz» (Art. 16–19).

Viele andere Länder und internationale Organisationen haben bereits Standards für ihren Bereich bestimmt. Die Bundesbehörden werden also nicht das Rad neu erfinden müssen. Es ist in diesem Zusammenhang auch wichtig, dass die Schweiz sich an solchen Standardisierungsprozessen aktiv beteiligt.

Der Bundesrat soll die Erarbeitung und Verabschiedung der Standards wenn nötig an untergeordnete Stellen delegieren können, um nicht mit dem Erlass von operativtechnischen Sicherheitsmassnahmen belastet zu sein. Da Sicherheitsmassnahmen grundsätzlich von der Linie beschlossen werden müssen, kann eine Delegation an

die Generalsekretärenkonferenz (Art. 53 RVOG) eine besonders geeignete Lösung sein. Eine Delegation kann überdies auch die Fachstelle des Bundes für Informationssicherheit, aber auch beispielsweise das Fedpol im Bereich des Objektschutzes betreffen. Die Leistungserbringerinnen des Bundes sollten ebenfalls technische Sicherheitsstandards erarbeiten können und diese gegebenenfalls zwecks Standardisierung durch die Fachstelle auf ihre Eignung für den Bund prüfen lassen (s. Art. 84 Abs. 1 Bst. e). Eine solche Delegation durch den Bundesrat soll aber nicht allzu umfassend erfolgen. Bestimmte technische Massnahmen können erhebliche finanzielle Folgen nach sich ziehen, die nicht von untergeordneten Stellen beschlossen werden sollten. Der Bundesrat soll also auch bei einer allfälligen Delegation sicherstellen, dass er die weitreichenden und kostspieligsten Massnahmen selbst beschliesst.

Die Standards sind für die anderen verpflichteten Behörden nicht verbindlich, weil sie vom Bundesrat festgelegt werden. Da die Konferenz bei der Ausarbeitung der Standards aber massgebend mitwirken wird, sollte der bloss empfehlende Charakter der Standards in der Praxis die Anwendung derselben durch die anderen Behörden und durch die Kantone nicht verhindern.

Art. 87 Kantone

Zur Zusammenarbeit zwischen Bund und Kantonen siehe Ziffer 1.2.2. Nach Artikel 3 sind die Kantone verpflichtet, einen gleichwertigen Schutz zu gewährleisten, wenn sie klassifizierte Informationen des Bundes bearbeiten oder auf seine Informatikmittel zugreifen. Sie müssen entsprechend sicherstellen, dass ihre Massnahmen tatsächlich geeignet dafür sind, das erforderliche Sicherheitsniveau zu erreichen. Der Umfang dieser Prüfung ist auf die Sicherheit bei der Bearbeitung von klassifizierten Informationen und beim Zugriff auf Informatikmittel des Bundes beschränkt. Für diese Kontrolle sind die Kantone selbst zuständig. Es wird von ihnen allerdings verlangt, dass sie die Fachstelle des Bundes für Informationssicherheit über die Ergebnisse ihrer Prüfungen orientieren. Ferner soll sichergestellt werden, dass der Informationsaustausch zwischen Kantonen und Bund systematisch und effizient stattfindet und die Umsetzung der Massnahmen nach diesem Gesetz koordiniert erfolgt. Von den Kantonen wird nicht erwartet, dass sie sich neu organisieren oder neue Strukturen schaffen. Sie werden zudem an der Ausarbeitung der Vollzugserlasse zum Gesetz sowie der Standards nach Artikel 86 direkt mitwirken.

Obschon die Kantone selbst für ihre Informationssicherheit zuständig sind, verfügt der Bund über besondere Instrumente und Fähigkeiten, auf welche die Kantone für ihre eigenen Bedürfnisse zugreifen dürfen sollen. Der Aufbau entsprechender Instrumente und Fähigkeiten auf kantonaler Ebene wäre wirtschaftlich betrachtet nicht sinnvoll. Betroffen sind insbesondere die PSP. Angestellte der Kantone, die sicherheitsempfindliche Tätigkeiten des Bundes ausüben, werden gestützt auf Artikel 30 Absatz 1 Buchstabe b sicherheitsüberprüft. Die entsprechenden Kosten trägt wie heute der Bund. Das BSV sowie die vorgesehenen Auditfähigkeiten der Fachstelle des Bundes für Informationssicherheit stossen bei den Kantonen ebenfalls auf Interesse. Der Bundesrat soll deshalb ermächtigt werden, in Zusammenarbeit mit den Kantonen festzulegen, in welchem Umfang und auf welche Ressourcen des Bundes die Kantone sollen zugreifen dürfen. Sofern die Kantone die Dienstleistun-

gen des Bundes für ihre eigenen Bedürfnisse in Anspruch nehmen, sollen sie den Bund dafür kostendeckend entschädigen.

Art. 88 Völkerrechtliche Verträge

Die völkerrechtlichen Verträge im Bereich der Informationssicherheit enthalten vorweg technische Regelungen über die wechselseitige Anerkennung nationaler Vorschriften und Abläufe (z. B. das PSP-Verfahren oder das BSV), Konkordanzlisten über die Anwendung von Klassifizierungen, Sicherheitsstandards im Bereich der Informatik oder Kommunikationssicherheit sowie Regelungen über die Durchführung gegenseitiger Kontrollen. Es kann zudem erforderlich sein, dass zum Schutz von Informationen, die dem Bund von anderen Staaten oder internationalen Organisationen zur Verfügung gestellt werden, Vereinbarungen zu treffen sind, die in einzelnen Punkten (z. B. Voraussetzungen für die Klassifizierung, für den Zugang zu oder die Bearbeitung von klassifizierten Informationen oder für die Erteilung der Sicherheitserklärungen) von den gesetzlichen Vorschriften abweichen. Der Lieferant der Informationen kann in solchen Fällen von den empfangenden Bundesbehörden verlangen, dass ein strengerer oder ein weniger strenger Schutz seiner Informationen vereinbart wird. Aus Gründen der Verwaltungsökonomie soll der Bundesrat ermächtigt werden, solche Informationssicherheitsabkommen direkt abzuschliessen.

Zur Minimierung der Risiken im Bereich der Informationssicherheit ist eine zunehmende internationale Vernetzung und Zusammenarbeit erforderlich. Die Umsetzung der NCS verlangt deshalb, dass der Austausch von Erfahrungen, Forschungs- und Entwicklungsarbeiten, vorfallbezogenen Informationen sowie Ausbildungs- und Übungstätigkeiten verstärkt wird (s. auch Ziff. 1.1.2). Der Bundesrat soll auch ermächtigt werden, völkerrechtliche Verträge zum Austausch von Informationen über Gefährdungen, Schwachstellen und Vorfälle, insbesondere bei KI, abzuschliessen. Es handelt sich hier ebenfalls um untergeordnete organisatorische und technische Angelegenheiten (z. B. Zusammenarbeit mit anderen staatlichen CERT, s. Art. 78).

Art. 89 *Evaluation*

Eine Evaluation soll fünf Jahre nach Inkrafttreten des Gesetzes durchgeführt werden. Die Berichterstattung soll jährlich auf der Basis der Berichterstattung der Fachstelle des Bundes (s. Art. 84 Abs. 1 Bst. h) stattfinden. Die Bundesversammlung muss die Kommission bestimmen, welche die Berichte des Bundesrats behandeln soll.

7. Kapitel: Schlussbestimmungen

Art. 90 Änderung anderer Erlasse

Siehe Ziffer 2.3.

Art. 91 Übergangsbestimmungen

Der Übergang in das neue Recht muss so gestaltet werden, dass er möglichst wirtschaftlich und nach Prioritäten erfolgt. So wäre es unverhältnismässig zu verlangen, dass die Klassifizierung aller Informationen innerhalb einer bestimmten Frist überprüft wird. Dies trifft ebenfalls im Bereich der Informatik zu: Ein sofortige Anpassung aller Systeme an die neuen Vorschriften wäre zwar aus Sicherheitssicht zu empfehlen. Der finanzielle und personelle Aufwand, der damit verbunden ist, wäre jedoch völlig unverhältnismässig. Deshalb legt das Gesetz fest, dass in einem ersten Schritt die Sicherheitseinstufung der Informatikmittel stattfinden muss. Diese Massnahme muss innerhalb von zwei Jahren erfolgen, damit die kritischsten Informatikmittel rasch identifiziert werden. Die Nachrüstung von Informatikmitteln ist oft aufwendig und wesentlich teurer, als wenn die Sicherheit von Anfang an implementiert wird. Ist der Aufwand zur Verbesserung eines Systems unverhältnismässig im Vergleich zur erwarteten Informationssicherheit, dann müssen die Risiken transparent ausgewiesen und getragen werden. Vier weitere Jahre sollen genügen, um bei Bedarf die erforderlichen Anpassungen an den Systemen selbst bzw. an den bestehenden Informationssicherheits- und Datenschutzkonzepten vorzunehmen, wobei die kritischsten Systeme zuerst behandelt werden sollten. Voraussetzung für diese Anpassungen ist das Vorliegen der Standards nach Artikel 86, die entsprechend zuerst festgelegt werden müssen.

Die Übergangsregelung für die PSP und das BSV dient einerseits der Transparenz gegenüber den Personen und Firmen, die in Besitz einer entsprechenden Erklärung sind, andererseits aber auch dem ordentlichen, risikogerechte Einstieg in das neue Recht. Die Gültigkeit der Betriebssicherheitserklärungen beträgt bereits fünf Jahre. Die Lage bei den PSP ist leicht komplizierter, da die Erklärungen kein formelles Ablaufdatum haben (die Prüfung wird lediglich nach einer bestimmten Frist wiederholt). Die vorgeschlagene Regelung bietet sowohl den einleitenden Stellen als auch den Fachstellen PSP Kontinuität. Sie gibt ferner dem Bundesrat genügend Spielraum, um zuerst die kritischsten Funktionen neu prüfen zu lassen.

2.2 Koordination mit anderen Erlassen

Der vorliegende Gesetzesentwurf ist mit folgenden hängigen Gesetzesentwürfen zu koordinieren:

Nachrichtendienstgesetz

Tritt das NDG vor dem vorliegenden Gesetz in Kraft, so ist Artikel 51 Absatz 4 NDG mit Inkrafttreten des vorliegenden Gesetzes gemäss dem vorliegenden Gesetz zu ändern.

Tritt das NDG nach dem vorliegenden Gesetz in Kraft, so ist die Änderung von Artikel 51 Absatz 4 NDG gemäss vorliegendem Gesetz erst auf denselben Zeitpunkt in Kraft zu setzen.

Unabhängig davon, ob das NDG oder das vorliegenden Gesetz zuerst in Kraft tritt, lautet mit Inkrafttreten der später in Kraft tretenden Änderung sowie bei gleichzeitigem Inkrafttreten Artikel 367 Absatz 2 Buchstabe i, Absatz 2bis Buchstabe b und Absatz 4 des Strafgesetzbuches wie folgt:

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

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

i. die für die Durchführung der Personensicherheitsprüfungen zuständigen Fachstellen nach Artikel 32 Absatz 2 ISG[30] (Fachstellen PSP);

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

b. die Fachstellen PSP;

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

Strafregistergesetz

Tritt das Strafregistergesetz (StReG) vor dem vorliegenden Gesetz in Kraft, entfallen die im vorliegenden Gesetz enthaltenen Änderungen von Artikel 365 Absatz 2 Buchstabe d sowie 367 Absätze 2 Buchstabe i, 2bis Buchstabe b und 4 StGB. Stattdessen sind Artikel 46 Absatz 6 Buchstabe a ISG, Artikel 46 Buchstabe e StReG und Artikel 51 Buchstabe f StReG mit Inkrafttreten des vorliegenden Gesetzes wie folgt zu ändern:

Art. 46 Abs. 6 Bst. a ISG

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

a. Strafregister-Informationssystem VOSTRA nach dem Strafregistergesetz vom 17. Juni 2016[31];

Art. 46 Bst. e StReG

Folgende angeschlossene Behörden können durch ein Abrufverfahren in alle im Behördenauszug 2 erscheinenden Daten (Art. 38) Einsicht nehmen, soweit dies für die Erfüllung der nachstehend genannten Aufgaben notwendig ist:

30 SR …; BBl **2017** 2953 3097
31 SR …; BBl **2016** 4871

e.	die Fachstellen für Personensicherheitsprüfungen nach Artikel 32 Absatz 2 des Informationssicherheitsgesetzes vom …[32] (ISG):	1. für die Beurteilung des Risikos im Rahmen von Personensicherheitsprüfungen nach dem ISG, 2. für Beurteilungen des Gefährdungs- und Missbrauchspotenzials nach dem Militärgesetz vom 3. Februar 1995[33], 3. für weitere Beurteilungen des Risikos im Rahmen der in der Spezialgesetzgebung vorgesehenen Prüfungen;

Art. 51 Bst. f StReG

Aufgehoben

Tritt das Strafregistergesetz nach dem vorliegenden Gesetz in Kraft, so sind Artikel 46 Absatz 6 Buchstabe a ISG, Artikel 46 Buchstabe e StReG und Artikel 51 Buchstabe f StReG gemäss oben stehendem Wortlaut zu ändern. Hingegen entfällt die im Strafregistergesetz vorgesehene Änderung von Artikel 20*a* BPG; die nach dem vorliegenden Gesetz vorgesehene Änderung von Artikel 20*a* BPG bleibt also in Kraft.

Energiegesetz

Tritt das Energiegesetz vor dem vorliegenden Gesetz in Kraft so erhält Artikel 20*a* StromVG mit Inkrafttreten des vorliegenden Gesetzes die Fassung gemäss dem vorliegenden Gesetz.

Tritt das Energiegesetz nach dem vorliegenden Gesetz in Kraft so entfällt die im Energiegesetz vorgesehene Änderung des Artikels 20*a* StromVG; d. h. die nach dem vorliegenden Gesetz vorgesehene Änderung des Artikels 20*a* StromVG bleibt in Kraft.

2.3 Änderung anderer Erlasse

Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit

Art. 2 Abs. 4 Bst. c sowie Art. 19–21

Die PSP soll neu schwergewichtig im ISG geregelt werden. Die entsprechenden Bestimmungen des BWIS müssen daher aufgehoben werden.

Art. 24a Abs. 7 erster Satz

Zur Beurteilung des Sicherheitsrisikos im Rahmen einer PSP nach dem ISG, einer Prüfung der Vertrauenswürdigkeit nach der Spezialgesetzgebung sowie zur Beurtei-

32 SR …; BBl **2017** 2953 3097
33 SR **510.10**

lung des Gewaltpotenzials im Sinne von Artikel 113 MG müssen die Fachstellen PSP auf die Daten der Hooligandatenbank des Fedpol Zugriff haben.

Nachrichtendienstgesetz

Art. 51 Abs. 4 Bst. d

Die Fachstellen PSP können Daten beim NDB erheben (Art. 35 Abs. 1 Bst. c). Der INDEX NDB dient dazu, festzustellen, ob der NDB Daten zu einer bestimmten Person, Organisation, einem Gegenstand oder einem Ereignis bearbeitet. Alle in IASA NDB und IASA-GEX NDB (s. Art. 49 und 50 NDG) erfassten Personen sind hier abrufbar. Konkret werden hier die wichtigsten Identifikationsdaten erfasst, beispielsweise bei Personen der Name, das Geburtsdatum, die Nationalität usw. Der INDEX NDB dient damit der Koordination der nachrichtendienstlichen Tätigkeiten von Bund und Kantonen, aber auch der Koordination von nachrichtendienstlichen Tätigkeiten mit sicherheits- und kriminalpolizeilichen Tätigkeiten. Die Fachstellen PSP haben keinen direkten Zugang zu Informationen, die über die Identifikationsdaten hinausgehen. Ist eine bestimmte Person im INDEX NDB registriert, so muss die zuständige Fachstelle PSP den NDB um die Lieferung der nötigen Daten ersuchen (s. Art. 46 Abs. 6 ISG sowie Art. 49 ff NDG).

Bundespersonalgesetz

Art. 20a

Die Erhöhung des Schwellenwerts für die Durchführung von PSP soll dazu dienen, diese Massnahme nur noch für Tätigkeiten einzusetzen, die tatsächlich eine erhöhte Sicherheitsempfindlichkeit vorweisen. Es besteht jedoch die Gefahr, dass der Schwellenwert für die PSP in der Praxis herabgesetzt wird bzw. die Anforderungen an die Notwendigkeit einer PSP reduziert werden, wenn die verpflichteten Behörden und Organisationen keine anderen Instrumente zur Verfügung haben, um die Vertrauenswürdigkeit von Bewerberinnen und Bewerbern sowie von Angestellten zu prüfen. Der neue Artikel 20*a* BPG soll den Arbeitgebern entsprechende Mittel anbieten. Auszüge sollen jedoch nicht standardmässig verlangt werden, sondern nur dann, wenn dies für die Wahrung der Interessen der Arbeitgeber unumgänglich ist. Der Bundesrat wird dazu Ausführungsrecht erlassen.

Art. 20b

Die PSP nach dem ISG dürfen nur zur Identifizierung von erheblichen Risiken für die Informationssicherheit durchgeführt werden. Es verbleiben aber weitere Tätigkeiten im Aufgabenbereich der Bundesbehörden, die zwar keinen unmittelbaren Bezug zur Informationssicherheit haben, bei denen aber wesentliche Interessen des Bundes erheblich beeinträchtigt werden können. Personen, die solche Tätigkeiten ausüben, sollen auf ihre Vertrauenswürdigkeit hin geprüft werden dürfen. Mit der Einfügung einer neuen Bestimmung über die Prüfung der Vertrauenswürdigkeit in

Artikel 20*b* BPG soll ein identifizierter Prüfbedarf für bestimmte Bundesangestellte abgedeckt werden.

- Es handelt sich primär um das diplomatische und konsularische Personal des EDA. Es kann aber auch das Personal anderer Departemente betroffen sein, das ähnliche Funktionen wahrnimmt (z. B. beim SECO).
- Die Prüfung kann für Amtsdirektorinnen und -direktoren gelten, aber auch beispielsweise für Angestellte, die Entscheidungskompetenzen bei der Vergabe wesentlicher öffentlicher Aufträge haben, oder Personen, die besonders empfindliche Aufgaben im Zusammenhang mit dem Finanzhaushalt erfüllen.

Die Bestimmung erfasst nicht alle Arbeitgeber im Sinne von Artikel 3 BPG. So ist zum Beispiel die Aufsichtsbehörde über die Bundesanwaltschaft nicht aufgeführt, weil keine Angestellte der Aufsichtsbehörde die Voraussetzungen von Artikel 20*b* Absatz 1 BPG erfüllen. Für die dezentralisierten Verwaltungseinheiten und die anderen eidgenössischen Gerichte wird der Bundesrat nach Konsultation der betroffenen Organisationen auf Verordnungsebene entscheiden, ob und inwiefern ihr Personal einer Vertrauenswürdigkeit unterzogen werden darf (siehe Verweis auf die Zuständigkeit des Bundesrats in Art. 3 Abs. 2 und 3 BPG). Die Prüfung soll zudem nur bei ausgewiesenem Bedarf, d. h. bei der Möglichkeit eines erheblichen Schadens, angeordnet werden. Die vorliegende Bestimmung darf nicht dazu dienen, die vom Bundesrat verlangte Reduzierung der Anzahl durchgeführter PSP zu umgehen. Es ist nicht sinnvoll, für die Prüfung der Vertrauenswürdigkeit ein besonderes Verfahren oder weitere Fachstellen einzuführen, da die abzuklärenden Fragen vom Grundsatz her die gleichen sind, wie bei der Informationssicherheit. Für die Prüfung soll daher auf die Regelung im ISG zurückgegriffen werden. Mit der Übernahme des Verfahrens werden insbesondere auch der Grundsatz des Einverständnisses der betroffenen Person mit der Durchführung der Prüfung, die Grundsätze der Datenerhebung, die Funktionslisten, die Prüfstufen und die Regelungen über die Folgen der Beurteilung zur Anwendung kommen. Die für diese Prüfung notwendigen Funktionslisten sollen durch die Fachstelle des Bundes für Informationssicherheit – in Zusammenarbeit mit dem EPA für die Bundesverwaltung und mit den zuständigen Stellen der anderen Bundesbehörden – erstellt und nachgeführt werden.

Zivilprozessordnung

Zur Änderung von Artikel 166 Absatz 1 Buchstabe c der Zivilprozessordnung: siehe Erläuterungen zu Artikel 320 Ziffer 1 StGB.

Bundeszivilprozess

Zur Änderung von Artikel 42 Absatz 3 des Bundeszivilprozesses: siehe Erläuterungen zu Artikel 320 Ziffer 1 StGB.

Strafgesetzbuch

Art. 320 Ziff. 1

Outsourcing ist in der IKT heute in vielen Bereichen nicht nur allgemein üblich, sondern geradezu zwingend, weil das spezialisierte Knowhow von Hardware- und Software-Herstellern oft unentbehrlich ist. Auch Bund und Kantone ziehen in der IKT zahlreiche externe Dienstleistungserbringer bei (vgl. dazu Art. 10*a* DSG). Gerade in Datenbanken ist häufig eine kaum bestimmbare Menge an verschiedenen geheimnisgeschützten Informationen gespeichert. Selbst wenn das Prinzip der Datensparsamkeit und weitere technische oder organisatorische Massnahmen (Anonymisierung der Daten, Kontrolle der Mitarbeitenden usw.) eingehalten werden, erhalten die mit technischen Aufgaben betrauten Personen (oft unvermeidbar) *Zugang zu amtsgeheimnisgeschützten Informationen*.

Externe Hilfspersonen im Bereich IKT, die Dienstleistungen für die Verwaltung erbringen (z. B. Wartung von Datenbanken), sind nach *Artikel 320 StGB* nicht verpflichtet, Amtsgeheimnisse zu wahren, die sie in Ausübung ihrer Tätigkeit wahrnehmen. Diese verwaltungsexternen IKT-Mitarbeitenden sind grundsätzlich *keine funktionellen Beamtinnen und Beamten* im Sinne von Artikel 110 Ziffer 3 StGB[34] und fallen somit nicht in den Täterkreis von *Artikel 320 Ziffer 1 StGB* (Sonderdelikt).[35] Eine strafrechtliche Handhabe besteht nur, wenn sich die externen Hilfspersonen als Gehilfinnen und Gehilfen oder Anstifterinnen und Anstifter am Sonderdelikt der Beamtin oder des Beamten beteiligen oder solche Informationen weitergeben und damit ein anderes Delikt begehen; zu denken ist dabei an verbotene Handlungen für einen fremden Staat (Art. 271 StGB) oder politischen oder wirtschaftlichen Nachrichtendienst (Art. 272 bzw. 273 StGB). Es besteht somit – anders als beim Schutz von Berufsgeheimnissen (Art. 321 StGB), der auch die Hilfspersonen der Geheimnisträgerinnen und Geheimnisträger erfasst – eine *Schutz- bzw. Strafbarkeitslücke im Bereich Amtsgeheimnisse*, soweit es um eine reine Hilfstätigkeit von Externen geht.

Die Offenbarung von Amtsgeheimnissen[36] ist nach *Artikel 320 Ziffer 2 StGB* nicht strafbar, wenn sie mit schriftlicher *Einwilligung* der vorgesetzten Behörde erfolgt. Weil Artikel 320 StGB nicht nur *Dienstgeheimnisse* erfasst, sondern auch *Privatgeheimnisse*[37] (z. B. Gesundheitsdaten in einem Personendossier oder Fabrikations- und Geschäftsgeheimnisse bei einer öffentlichen Ausschreibung), muss die für die Einwilligung zuständige Behörde bei der *Interessenabwägung* sorgfältig prüfen, welche Interessen durch eine Offenbarung tangiert sind. Je nach Art und Gewicht

34 Weber Rolf H., Outsourcing von Informatik-Dienstleistungen in der Verwaltung, in: Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht, 100. Jahrgang (1999), S. 97 ff., Ziff. 2.2.1. Vgl. auch (e contrario) BGE **135** IV 198, E. 3.3.

35 Oberholzer Niklaus in: Niggli/Wiprächtiger (Hrsg.), Basler Kommentar Strafrecht I, Basel 2013, Art. 110 Abs. 3 N 13 ff. Umfangreiche Kasuistik bei Trechsel Stefan/ Vest Hans in Trechsel/Pieth (Hrsg.), Schweizerisches Strafgesetzbuch Praxiskommentar, Zürich/St. Gallen 2013, Art. 110 Abs. 3 N 13.

36 Das Verschaffen einer Möglichkeit der Kenntnisnahme genügt, vgl. Oberholzer Niklaus in: Niggli/Wiprächtiger (Hrsg.), Basler Kommentar Strafrecht II, Basel 2013, Art. 320 N 10.

37 Oberholzer Niklaus in: Niggli/Wiprächtiger (Hrsg.), Basler Kommentar Strafrecht II, Basel 2013, Art. 320 N 3 und 8.

des in Frage stehenden Geheimhaltungsinteresses ist die Einwilligung zu erteilen oder zu verweigern.[38] Falls das Geheimhaltungsinteresse nicht mindestens teilweise dienstlicher, sondern ausschliesslich privater Natur ist, scheidet die Einwilligung der vorgesetzten Behörde nach Artikel 320 Ziffer 2 StGB als Rechtfertigungsgrund prinzipiell aus.[39] Die erforderlichen Einwilligungen sind im IKT-Bereich auch aus praktischen Gründen (unbestimmbare Zahl an Geheimnisträgern bzw. -herren) nicht einholbar, wenn z. B. nach einem Absturz einer Datenbank unverzüglich externer technischer Support notwendig ist. Wenn aber keine gültige Einwilligung vorliegt, machen sich die verwaltungsinternen Mitarbeitenden strafbar, falls sie externen Dienstleistern Zugang zu Amtsgeheimnissen ermöglichen. Es besteht de lege lata somit auch ein *Strafbarkeitsrisiko* für die verwaltungsinternen Mitarbeitenden.

Der Bundesrat ist der Ansicht, dass der Gesetzgeber diese Probleme rasch lösen sollte. Er sieht jedoch davon ab, die *Einwilligung* der vorgesetzten Behörde gesetzlich auf reine Privatgeheimnisse zu erstrecken. Auch dann könnte – wie *de lege lata* – die Pflicht zur Wahrung der Amtsgeheimnisse bei externen Dienstleistern lediglich indirekt, auf vertraglichem Weg (mittels Konventionalstrafen) abgesichert werden. Zudem würde damit die Rechtsstellung der Privaten tendenziell ausgehöhlt. Auch eine Erweiterung der *Legaldefinition* des Beamten in Artikel 110 Ziffer 3 StGB ist nicht sachgerecht, da dies Auswirkungen auf alle Amtsdelikte hätte. Externe Hilfspersonen, die nicht unter den funktionellen Beamtenbegriff fallen, üben jedoch keine Funktion im Dienst der Öffentlichkeit aus und treten nach aussen nicht als Repräsentantinnen und Repräsentanten der staatlichen Verwaltung in Erscheinung. Sie sollen deshalb nicht generell für sämtliche Amtsdelikte verantwortlich sein können.

Der Bundesrat zieht es vor, den *Täterkreis* von *Artikel 320 Ziffer 1 StGB* um die Hilfspersonen zu *erweitern* und damit den *Schutz von Amtsgeheimnissen* zu *verstärken*. Nicht zuletzt mit Blick auf die bestehende Regelung bei den Berufsgeheimnissen (Art. 321 StGB) ist es angezeigt, Hilfspersonen strafrechtlich ebenfalls zur Wahrung des Amtsgeheimnisses zu verpflichten.[40] Damit ist auch das Strafbarkeitsrisiko der internen Mitarbeitenden eliminiert, wenn sie Amtsgeheimnisse ohne Einwilligung, aber dienstlich bedingt externen Hilfspersonen zugänglich machen.

Soll eine externe Hilfsperson nach Artikel 320 Ziffer 2 StGB vom Amtsgeheimnis entbunden werden, muss die vorgesetzte Behörde des verwaltungsinternen Auftraggebers schriftlich einwilligen. Die Situation ist damit vergleichbar mit den Hilfsper-

38 Trechsel Stefan/Vest Hans, in: Trechsel/Pieth (Hrsg.), Schweizerisches Strafgesetzbuch Praxiskommentar, Zürich/St. Gallen 2013, Art. 320 N 11. Zur strukturell ähnlichen Einwilligung der vorgesetzten Behörde beim Berufsgeheimnis vgl. Stratenwerth Günter/Bommer Felix, Schweizerisches Strafrecht Besonderer Teil II, Bern 2013, § 61 N 23. Zum prozessualen Gegenstück der materiellen Strafnorm vgl. Art. 170 Abs. 3 StPO, dazu Donatsch Andreas in: Donatsch/Hansjakob/Lieber (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung, Zürich etc. 2014, Art. 170 N 14. Für die spiegelbildliche Interessenabwägung beim Recht auf Zugang zu amtlichen Dokumenten vgl. Art. 7 (insb. Abs. 3) des Bundesgesetzes über das Öffentlichkeitsprinzip der Verwaltung (BGÖ) vom 17. Dezember 2004 (SR **152.3**).

39 Zur Reichweite der Einwilligung vgl. Stratenwerth Günter, Schweizerisches Strafrecht Allgemeiner Teil I, Bern 2011, § 10 N 5, 13 und Stratenwerth Günter/Bommer Felix, Schweizerisches Strafrecht Besonderer Teil II, Bern 2013, § 61 N 10 f.

40 Zu den Hilfspersonen von Berufsgeheimnisträgern vgl. Oberholzer Niklaus in: Niggli/Wiprächtiger (Hrsg.), Basler Kommentar Strafrecht II, Basel 2013, Art. 321 N 10.

sonen von Berufsgeheimnisträgerinnen und Berufsgeheimnisträgern nach Artikel 321 StGB. Nur die verwaltungsinterne, vorgesetzte Behörde kann die für eine Einwilligung erforderliche Interessenabwägung unter Berücksichtigung der massgebenden Kriterien sachgerecht vornehmen.

Für die Verletzung des Dienstgeheimnisses nach *Artikel 77 MStG* gelten die vorstehenden Erläuterungen analog. Als Folge der Änderung im materiellen Recht muss der Personenkreis für das *Zeugnisverweigerungsrecht aufgrund eines Amtsgeheimnisses* in Artikel 170 StPO, Artikel 77 MStP, Artikel 166 der *Zivilprozessordnung*[41] und (kraft Verweis in Art. 16 Abs. 1 VwVG) in Artikel 42 des Bundesgesetzes über den *Bundeszivilprozess*[42] ebenfalls entsprechend ergänzt werden.

Art. 365 Abs. 2 Bst. d

Da die PSP neu nicht mehr im BWIS sondern im ISG geregelt werden sollen, müssen die Bestimmungen über die zugriffsberechtigten Stellen sowie den Zweck der Datenerhebung entsprechend angepasst werden.

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

Zu Absätzen 2 und 2bis siehe die Erläuterungen zu Artikel 365 Absatz 2 Buchstabe d. Gemäss aktueller Praxis haben die Fachstellen PSP auch Zugang zu Daten über hängige Strafverfahren, obschon sie nicht in der Aufzählung von Artikel 367 Absatz 4 StGB enthalten sind. Wie bereits in der Botschaft zum Strafregistergesetz ausgeführt wurde[43], beruht dies auf einem gesetzgeberischen Versehen, das korrigiert werden muss. Denn Artikel 20 Absatz 2 Buchstabe d BWIS berechtigt diese Fachstellen bereits heute, bei den zuständigen Strafverfolgungsorganen Auskünfte über laufende Strafverfahren einzuholen. Dies können sie aber nur, wenn sie wissen, ob überhaupt ein Strafverfahren hängig ist. Diese Information erhalten die Fachstellen durch Konsultation von VOSTRA. Aus diesem Grund ist Artikel 367 Absatz 4 StGB zu aktualisieren (durch Erwähnung von Bst. i).

Strafprozessordnung

Zur Änderung von Artikel 170 Absatz 1 StPO: siehe Erläuterungen zu Artikel 320 Ziffer 1 StGB.

Militärstrafgesetz

Zur Änderung von Artikel 77 MStG: siehe Erläuterungen zu Artikel 320 Ziffer 1 StGB.

41 SR **272**
42 SR **273**
43 BBl **2014** 5713, 5810

Militärstrafprozess

Zur Änderung von Artikel 77 Absatz 2 MStP: siehe Erläuterungen zu Artikel 320 Ziffer 1 StGB.

Bundesgesetz über die polizeilichen Informationssysteme des Bundes

Art. 15 Abs. 4 Bst. f und Art. 17 Abs. 4 Bst. l

Neu erhalten die Fachstellen PSP Zugriff nur auf den Nationalen Polizeiindex (s. Art. 46 Abs. 6 ISG). Der Zugriff auf RIPOL (Art. 15 BPI) kann aufgehoben werden.

Militärgesetz

Art. 14

Entsprechend dem vorgeschlagenen Artikel 20*b* BPG sieht das ISG vor, dass der Bundesrat im Rahmen seiner Ausführungsbestimmungen zum MG zwei Aufgabenbereiche einer Prüfung der Vertrauenswürdigkeit unterstellen kann:

- Es handelt sich in Buchstabe a vor allem um Angehörige der Armee, die im Rahmen von regelmässigen Auslandeinsätzen die Schweiz hoheitlich vertreten oder die Aufgaben im Bereich der militärischen Diplomatie erfüllen.
- Buchstabe b betrifft nur Angehörige der Armee, die im Rahmen ihrer Dienstpflicht die finanziellen Interessen des Bundes erheblich beeinträchtigen könnten.

Die vorliegende Bestimmung darf nicht dazu dienen, die vom Bundesrat verlangte Reduzierung der Anzahl durchgeführter PSP zu umgehen. In der Praxis soll sie somit nur ausnahmsweise zur Anwendung kommen.

Art. 113 Abs. 6

Es handelt sich hier um eine formelle Anpassung von Absatz 6. Dieser muss auf das vorliegende Gesetz verweisen und nicht auf das BWIS.

Art. 150 Abs. 4 Aufhebung

Die Kompetenz zum Abschluss von Staatsverträgen zur Wahrung der militärischen Geheimhaltung ist neu in Artikel 88 ISG enthalten.

Bundesgesetz über die militärischen Informationssysteme

Art. 14 Abs. 1 Bst. i

Mit der Einführung der Prüfung der Vertrauenswürdigkeit nach Artikel 14 MG muss eine Grundlage für die Bearbeitung der Prüfungsergebnisse im PISA geschaffen werden. Im PISA sollen ausschliesslich Prüfungsergebnis und -datum sowie der Entscheid bearbeitet werden.

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

Neu werden die Informationssysteme zur PSP und zum BSV im ISG geregelt.

Kernenergiegesetz

Art. 5 Abs. 3 und Abs. 3bis

Der geltende Artikel 5 Absatz 3 KEG sieht bereits heute vor, dass die Sicherungsmassnahmen soweit erforderlich klassifiziert werden müssen. Die Änderung soll sicherstellen, dass die Klassifizierung dieser Massnahmen sowie die Bearbeitung der klassifizierten Informationen sich nach den Vorschriften des ISG richten.

Stromversorgungsgesetz

Art. 20a

In seiner Botschaft vom 4. September 2013[44] zum ersten Massnahmenpaket der Energiestrategie 2050 (Revision des Energierechts) und zur Volksinitiative «Für den geordneten Ausstieg aus der Atomenergie (Atomausstiegsinitiative)» hat der Bundesrat die Einführung einer PSP für gewisse Angestellte der nationalen Netzgesellschaft vorgeschlagen. Die vorliegende Änderung hat nur zum Ziel, diesen Vorschlag an die Terminologie und Systematik des ISG anzupassen.

Nationalbankgesetz

Art. 16, Sachüberschrift und Abs. 5

Aufgrund ihrer geld- und währungspolitischen Aufgaben soll die Nationalbank als verpflichtete Behörde gelten.

3 Auswirkungen

3.1 Auswirkungen auf den Bund

Der Bund investiert jährlich insgesamt über 800 Millionen Franken in seine Informatik. Die Gefahren für Informationen und Informatikmittel sind mit der Entwicklung zu einer Informationsgesellschaft komplexer und dynamischer geworden. Das Schadensausmass, das durch den Ausfall oder die Störung von Informatikmitteln oder den Diebstahl oder Missbrauch von Informationen verursacht werden kann, ist entsprechend gewachsen. Informationssicherheit hat zum Ziel, möglichst effektiv und wirtschaftlich die Eintrittswahrscheinlichkeit und gegebenenfalls das Ausmass eines solchen – auch finanziellen – Schadens zu reduzieren. Das Gesetz und seine Ausführungsbestimmungen werden eine nachhaltige Verbesserung der Informati-

44 BBl **2013** 7561

onssicherheit im Bund bewirken. Das ISG regelt vorwiegend das Management der Informationssicherheit und wird dessen Effizienz erhöhen. Ein effizientes Management verbessert die Sicherheit erfahrungsgemäss oft effektiver, wirtschaftlicher und nachhaltiger als blosse Investitionen in technische Massnahmen. Die Praxis hat zudem gezeigt, dass eine Optimierung des Managements – insbesondere wenn letzteres auf ein effektives Risikomanagement gestützt ist – mittelfristig sogar zu Kosteneinsparungen beitragen kann.

Der Entwurf sieht zudem mehrere organisatorische Massnahmen vor, die im Vergleich zu heute nicht nur einen besseren Schutz bewirken werden, sondern auch zu Kosteneinsparungen führen sollen, sofern sie konsequent umgesetzt werden. So soll beispielsweise die Erhöhung der Schwellenwerte für die Klassifizierung die Anzahl klassifizierter Informationen und somit den entsprechenden Aufwand reduzieren. Bei den PSP werden gleichzeitig die Unterstellungskriterien verschärft und die Anzahl Tätigkeiten reduziert, für deren Ausübung eine PSP erforderlich und zulässig ist. Es sollen also inskünftig deutlich weniger PSP durchgeführt werden. Ferner werden die Standardisierung, der verbesserte Informationsaustausch zwischen den Bundesbehörden und deren Unterstützung durch die Fachstelle des Bundes für Informationssicherheit dazu beitragen, dass das Rad nicht bei jedem Projekt neu erfunden wird. Die Neuregelung wird schliesslich die internationale Zusammenarbeit im Sicherheitsbereich erleichtern und den Datenschutz beim Bund verbessern.

Die finanziellen und personellen Auswirkungen des Entwurfs einerseits und die entsprechende Reduktion der erwähnten Risiken sowie die aufwandreduzierenden Auswirkungen andererseits müssen also immer abgewogen werden.

3.1.1 Finanzielle Auswirkungen

Die finanziellen Auswirkungen des Gesetzes hängen fast vollständig vom Sicherheitsniveau ab, dass die Behörden erreichen wollen (Art. 7 Abs. 2) und können deshalb erst im Rahmen der Ausarbeitung des Ausführungsrechts abgeschätzt werden. Auf diese Kosten hat das Gesetz selbst wenig Einfluss.

Die Kosten der Neuorganisation nach dem Stand von Wissenschaft und Technik (Art. 7 Abs. 1) variieren je nach Organisationsmodell stark. Den Entscheid über das Organisationsmodell werden die verpflichteten Behörden nach einer Kosten-Nutzen-Analyse im Rahmen des Vollzugs treffen. Eine Minimalvariante, bei welcher die bestehenden Prozesse auf wesentliche Lücken geprüft werden und zwischen den Behörden und Organisationen untereinander harmonisiert werden, könnte grundsätzlich mit den bestehenden Ressourcen umgesetzt werden. Eine Maximalvariante – die Umsetzung eines ISMS nach dem Standard DIN ISO/IEC Norm 27 001 durch alle verpflichteten Behörden und Organisationen – würde nach Einschätzung von Fachexperten Projektkosten (Beratungsaufwand) von ungefähr 8–12 Millionen Franken nach sich ziehen. Zwischen diesen beiden Varianten bestehen weitere Umsetzungsansätze, für die je nach Umfang und Sicherheitsbedarf mehr oder weniger Beratungsaufwand anfallen würde. Für das Management und den Betrieb der Organisation sind die Informationssicherheitsbeauftragten zuständig. Allfällige Auditkosten müssen im Rahmen des ordentlichen Budgets geplant und getragen werden.

Die Wirksamkeitsprüfungen (Art. 18 Abs. 3) könnten je nach Organisationsmodell (siehe Ziffer 3.1.2) jährliche Kosten von 1,5 bis 1,8 Millionen Franken für externe Audits nach sich ziehen. Erfahrungsgemäss entsprechen die Auditkosten in der Regel zwischen 0,5 und 2 Prozent der gesamten Investitionskosten für zu auditierende Systeme.

Mit Beschluss vom 12. Dezember 2013 hat das Parlament einen Verpflichtungskredit für das Programm IAM Bund (Art. 24–27) gesprochen. Die Mittel sind im Budget und Finanzplan des Bundes enthalten.

Für die Erhebung von Daten bei Finanzinstituten und Banken im Rahmen von erweiterten PSP (Art. 35 Abs. 2 Bst. c in Verbindung mit Art. 37 Abs. 2) ist mit jährlichen Kosten von 10 000 bis 20 000 Franken zu rechnen.

3.1.2 Personelle Auswirkungen

Insgesamt könnten für die Fachorgane der Informationssicherheit zwischen 13,5 und 14,5 zusätzliche Stellen erforderlich sein. Der Bundesrat wird beim Erlass des Vollzugsrechts über die zusätzlich einzusetzenden personellen Ressourcen entscheiden. Diese zusätzlichen Stellen sollen aber mittelfristig grösstenteils durch eine entsprechende Reduzierung im Bereich PSP kompensiert werden. Der personelle Mehrbedarf für die Informationssicherheitsbeauftragten kann zurzeit noch nicht sachgemäss abgeschätzt werden, weil er von der Regelung der internen Organisation (zentraler oder dezentraler Ansatz) abhängt. Es ist jedoch denkbar, dass ein zusätzlicher Aufwand von zwischen zwei bis sieben Stellen anfallen wird, der aber je nach Organisationsmodell mehr oder weniger intern kompensiert werden kann. Die geschätzten personellen Auswirkungen lassen sich wie folgt erläutern:

Fachstellen PSP

Die Fachstellen PSP führen jährlich zwischen 75 000 und 80 000 Prüfungen durch. Inbegriffen sind nicht nur die PSP nach dem BWIS, sondern auch die Prüfungen nach dem KEG (500 Prüfungen) und die Beurteilungen des Gewaltpotenzials von Stellungspflichtigen nach Artikel 113 MG (40 500 Prüfungen). Dafür setzt der Bundesrat heute insgesamt 61 Stellen ein: 27 unbefristete und 30 bis Ende 2017 befristete Stellen beim VBS sowie vier unbefristete Stellen bei der BK. Die Mehrheit der befristeten Stellen beim VBS (16 Stellen) wurde Ende 2012 zum Abbau der pendenten potenziellen Risikofälle bewilligt. Zehn neue auf zwei Jahre befristete Stellen wurden Ende 2015 vom VBS bewilligt. Bereits heute zeigt sich aber, dass trotz dieser zusätzlichen Stellen die Ressourcen der Fachstelle PSP VBS nicht genügen, um alle durchzuführenden Prüfungen zu bewältigen. Die Gesamtkosten der PSP (Personal- und Verwaltungsgemeinkosten sowie Informationssystem) für das Jahr 2015 betragen 12,5 Millionen Franken. Überdies entspricht der Verwaltungsaufwand für die Einleitung der PSP sowie für die Erstellung und Anpassung der Funktionslisten nach Angaben der Departemente und der BK insgesamt zehn Vollzeitstellen. Der Bundesrat will eine deutliche Reduzierung der Anzahl PSP erzielen und mittelfristig den damit verbundenen Personal- und Verwaltungsaufwand im Vergleich zu heute um mindestens zwölf Stellen kürzen. Auf die Anzahl Prüfungen

nach dem KEG, dem StromVG und Artikel 113 MG hat die Vorlage dagegen keinen Einfluss.

Fachstelle BS

Heute verfügen ungefähr 550 Betriebe mit Sitz in der Schweiz über eine BSE. Zur Durchführung des BSV bei militärisch klassifizierten Aufträgen setzt das VBS 2,2 Stellen (zwei Stellen für Sicherheitsspezialistinnen und -spezialisten und 20 Stellenprozent für die Einleitung von PSP) ein. Die Erweiterung des BSV auf den zivilen Bereich und auf die anderen Bundesbehörden wird voraussichtlich zu einer Zunahme der zu betreuenden Betriebe von circa 30 Prozent führen. Die Anpassungen am heutigen Verfahren werden zudem einen leicht erhöhten personellen Aufwand verursachen. Es wird damit gerechnet, dass für das BSV insgesamt 1,5 zusätzliche Stellen erforderlich sein werden. Ohne diese Ressourcen muss auf das einheitliche BSV verzichtet werden.

MELANI

Die Ressourcen von MELANI wurden im Rahmen der Umsetzungsplanung zur NCS behandelt. Es sind keine zusätzlichen personellen Ressourcen erforderlich.

Informationssicherheitsbeauftragte

Die Rolle der Informationssicherheitsbeauftragten fasst die bisherigen Rollen der Informationsschutz- und der Informatiksicherheitsbeauftragten zusammen. Die Informationssicherheitsbeauftragten erhalten zudem zusätzliche Zuständigkeiten im Bereich PSP und BSV sowie weitere Aufgaben (z. B. Steuerung der Informationssicherheit und des entsprechenden Risikomanagements sowie Durchführung von Audits). Für die Beurteilung der dafür nötigen personellen Ressourcen sind die Ausführungsbestimmungen massgebend. Die interne Fachorganisation in den Departementen (zentraler oder dezentraler Ansatz) kann die Ressourcenlage ebenfalls massgeblich beeinflussen. Erfahrungsgemäss könnte ein zusätzlicher personeller Aufwand von zwei bis acht Stellen erforderlich sein, der je nach Organisationsmodell mehr oder weniger intern kompensiert werden kann. Die verpflichteten Behörden werden im Rahmen des Vollzugs über diese Ressourcen entscheiden.

Fachstelle des Bundes für Informationssicherheit

Für eine minimale Erfüllung ihrer Aufgaben nach Artikel 84 sowie die Ausarbeitung der Standards nach Artikel 86 wird die Fachstelle des Bundes für Informationssicherheit gemäss Expertenbeurteilung insgesamt 22 Stellen benötigen. Diese verteilen sich wie folgt: Leitung Fachstelle (inkl. Stellvertretung): 1,2 Stellen; Sekretariat: 1,1 Stellen; Koordination Fachorgane: eine Stelle; Ausbildung und Sensibilisierung: eine Stelle; Risiko- und Anforderungsmanagement: vier Stellen; Audits und Reporting: zwei Stellen; Technische Audits: fünf Stellen; Kryptologie: 3,5 Stellen; Recht und politische Geschäfte: zwei Stellen; Internationale Beziehungen: 1,2 Stellen. Diese Stellen sollen gestaffelt kompensiert bzw. besetzt werden (im ersten Jahr 11 Stellen; zwischen dem zweiten und dritten Jahr 11 Stellen). Von diesen 22 Stellen werden 7,2 Stellen mit Ressourcen kompensiert, die bereits heute durch das EFD und das VBS für die departementsübergreifende Steuerung der Informatiksicherheit bzw. für die koordinierte Umsetzung der ISchV eingesetzt werden. Zwei bis drei

weitere Stellen (vor allem im Bereich Recht und internationale Beziehungen) werden vom VBS an das zuständige Departement übertragen. Insgesamt könnten also etwa zwölf bis dreizehn zusätzliche Stellen nötig sein. Der Bundesrat wird sich bemühen, soweit möglich diese allfälligen Personalbedürfnisse intern oder durch Effizienzgewinne zu kompensieren.

Diese zusätzlichen Stellen werden vorwiegend für drei neue oder erweiterte Aufgaben eingesetzt, die nachfolgend näher begründet werden:

– *Risiko- und Anforderungsmanagement:* Es geht einerseits darum, die Standards auszuarbeiten und diese anschliessend zu pflegen. Standardisierte Anforderungen und Massnahmen können zu Kosteneinsparungen im Rahmen von Projekten führen. Sie sind auch für den einheitlichen Vollzug wichtig. Andererseits soll auch die Unterstützung der Behörden (und der Kantone) bei der Steuerung ihrer Informationssicherheit und des entsprechenden Risikomanagements sichergestellt werden. Ohne die vier zusätzlichen Stellen müsste auf die Standardisierung verzichtet werden.

– *Technische Audits:* Es handelt sich hier um eine neue Aufgabe, die sowohl die Prüfung der Eignung (Art. 84 Abs. 1 Bst. e) als auch die periodischen Wirksamkeitsprüfungen (Art. 18 Abs. 3) einschliesst. Die Prüfung der Eignung ist im internationalen Verhältnis (s. Ziffer 5.2) und für die operationelle Standardisierung bei den Leistungserbringerinnen (s. Erläuterungen zu Art. 84 Abs. 1 Bst. e) notwendig. Die Wirksamkeitsprüfung ist die einzige Massnahme, die den effektiven Stand der technischen Informationssicherheit belegen kann. Die heutigen Rechtsgrundlagen sehen die neue Sicherheitsstufe «sehr hoher Schutz», für welche diese Prüfung vorbehalten ist, nicht vor. Von Fachexperten wird aber geschätzt, dass der Bund zehn bis zwanzig Systeme mit sehr hohem Schutzbedarf einsetzt. Derartige Systeme sind meistens sehr komplex. Der Auditaufwand ist entsprechend gross. Modelliert wurde mit zwölf bis sechzehn Systemen, die alle vier Jahre nach dem Stand der Lehre auditiert werden. Dafür benötigt der Bund entweder elf zusätzliche Stellen (eine Stelle für die Auditleitung, eine Stelle für die Sachbearbeitung und drei Auditgruppen mit je drei Auditoren), acht Stellen (Auditleitung, Sachbearbeitung und zwei Auditgruppen) mit einem Budget für externe Expertinnen und Experten von 750 000 bis 900 000 Franken, fünf Stellen (Auditleitung, Sachbearbeitung und eine Auditgruppe) mit einem Budget für externe Experten von 1,5 bis 1,8 Millionen Franken oder zwei Stellen (nur Auditleitung und Sachbearbeitung) mit einem Budget für externe Expertinnen und Experten von 2,25 bis 2,7 Millionen Franken. Zur Realisierung vorgeschlagen wird die Variante mit fünf Stellen, weil damit sichergestellt wird, dass der Bund intern über das erforderliche Fachwissen verfügt, und dass die Bundesbehörden regelmässig über den Auditaufwand entscheiden können, weil die entsprechenden Ressourcen beantragt werden müssen. Zudem ist fraglich, ob der Bund mehr Expertinnen und Experten überhaupt finden könnte.

  Ohne diese fünf zusätzlichen Stellen müsste entweder die Variante mit nur zwei zusätzlichen Stellen und entsprechendem Budget gewählt werden oder auf diese Aufgaben verzichtet werden. In diesem Fall würden die Anforde-

rungen im internationalen Verhältnis nicht erfüllt und die operationale Standardisierung bei den Leistungserbringerinnen könnte nur mit zusätzlichem externem Aufwand erreicht werden. Zudem könnte der Stand der Informationssicherheit bei den kritischsten Informatikmitteln des Bundes nicht fachgerecht beurteilt werden.

– *Kryptologie:* Die Verwendung von kryptologischen Massnahmen ist eine unabdingbare Schutzmassnahme für Informationen mit erhöhtem Schutzbedarf an Vertraulichkeit und Integrität. Der Einsatz der Kryptologie verlangt einerseits, dass klare Anforderungen vorliegen, andererseits aber auch, dass der Beschaffungsprozess begleitet wird, die Kryptokonzepte fachgerecht überprüft werden und die kryptologischen Komponenten periodisch gepflegt werden. Sowohl die Anforderungen als auch die erwähnten Fähigkeiten fehlen beim Bund weitgehend. Das VBS hingegen setzt 7,5 Stellen (4,5 bei der FUB und 3 bei der Armasuisse) zur Erfüllung dieser Aufgaben zugunsten des Departements und der Armee ein. Expertinnen und Experten schätzten, dass zur Erfüllung entsprechender Aufgaben bei allen Informatikmitteln mit sehr hohem Schutz und bei behördenübergreifenden Informatikmitteln mit hohem Schutz 3,5 zusätzliche Stellen nötig sind. Ohne diese zusätzlichen Ressourcen müsste auf die Begleitung und Überprüfung der kryptologischen Massnahmen ausserhalb des VBS verzichtet werden.

3.2 Auswirkungen auf Kantone und Gemeinden sowie auf urbane Zentren, Agglomerationen und Berggebiete

Die Auswirkungen auf die Kantone können erst beim Erlass der Ausführungsbestimmungen endgültig abgeschätzt werden. Die Anwendung des ISG auf die Kantone ist allerdings beschränkt und wird vor allem projekt- oder applikationsbezogen erfolgen. Die Kantone werden bei der Gestaltung der Ausführungsbestimmungen und Standards überdies eng mitwirken können, sodass sie die Wirtschaftlichkeit der Massnahmen früh beurteilen und darauf Einfluss nehmen können. Der Bund wird wie heute die Kosten der PSP für kantonale Angestellte tragen, die sicherheitsempfindliche Aufgaben des Bundes erfüllen müssen. Betroffen sind ungefähr 400 PSP jährlich. Die Kantone werden auch von der Unterstützung der Fachstelle des Bundes für Informationssicherheit profitieren. Sie werden hingegen verpflichtet, die Wirksamkeit der getroffenen Schutzmassnahmen periodisch zu überprüfen. Hierfür sollten sie jedoch keine neue Organisation aufbauen müssen, sondern ihre bestehenden Aufsichtsstrukturen benutzen. Im Rahmen der PSP soll die Erhebung von Betreibungs- und Konkursregisterauszügen aus den Kantonen zukünftig zwar unentgeltlich erfolgen (zurzeit kosten diese Erhebungen den Bund jährlich 250 000 Franken). Da diese Daten im Rahmen des Programms eSchKG[45] inskünftig jedoch über eine Schnittstelle elektronisch erhoben werden, wird der Erhebungsaufwand für die Kantone entfallen. Insgesamt ist absehbar, dass die Neuregelung einen eher

45 Informationen zum Projekt eSchKG finden hier: www.bj.admin.ch > Staat & Bürger > Rechtsinformatik > Projekt eSchKG

moderaten zusätzlichen Aufwand für die Kantone verursachen wird, der teilweise durch die effektiven Unterstützungsmassnahmen des Bundes kompensiert werden soll.

Das Gesetz hat grundsätzlich keine Auswirkungen auf urbane Zentren, Agglomerationen und Berggebiete.

3.3 Auswirkungen auf die Volkswirtschaft

Dritte werden nur vom Gesetz erfasst, wenn sie im Rahmen eines Vertrags mit Informationen oder Informatikmitteln des Bundes umgehen sollen. Betriebe, die sich für zivile Aufträge des Bundes bewerben, die eine sicherheitsempfindliche Tätigkeit einschliessen, werden neu dem BSV unterstellt. Mit dieser Unterstellung ist zwar ein geringer zusätzlicher administrativer Aufwand verbunden. Umgekehrt wird dadurch jedoch die Wettbewerbsfähigkeit von Schweizer Unternehmen verbessert, weil das Gesetz die Grundlage für die Abgabe behördlicher Sicherheitserklärungen zugunsten Privater schafft, die sich für ausländische oder internationale klassifizierte Aufträge bewerben und dafür eine nationale Sicherheitsbescheinigung.

Dritte, beispielsweise Banken oder Kreditinstitute, die im Rahmen der PSP zur Mitwirkung beigezogen werden, sollen nur entschädigt werden, wenn der dadurch verursachte Aufwand erheblich ist. Erheblich wird ein solcher Aufwand insbesondere dann, wenn er beispielsweise über die Erstellung von Kontoauszügen hinausgeht und besonders intensive Recherchen erfordert. Diese Mitwirkung ist nur für die höchste Prüfstufe vorgesehen. Der damit verbundene Aufwand soll gering bleiben.

3.4 Auswirkungen auf die Gesellschaft

Die Gesellschaft ist in zweifacher Hinsicht betroffen. Einerseits werden der Datenschutz und die Datensicherheit verbessert. Andererseits werden die Grundsätze der Klassifizierung offengelegt und die Kriterien verschärft, sodass insgesamt weniger klassifiziert wird. Dies ist insbesondere in Bezug auf das Öffentlichkeitsprinzip wichtig, dessen Wirkung durch das Gesetz keinesfalls beeinträchtigt werden darf.

3.5 Auswirkungen auf die Umwelt

Das Gesetz hat keine Auswirkungen auf die Umwelt.

3.6 Andere Auswirkungen

Die Vorlage setzt formal keine direkten internationalen Verpflichtungen um. Praktisch wird es die internationale Zusammenarbeit erleichtern, indem es die im internationalen Verhältnis üblichen Zuständigkeiten klar definiert (s. Ziff. 5.2).

4 Verhältnis zur Legislaturplanung und zu nationalen Strategien des Bundesrates

4.1 Verhältnis zur Legislaturplanung

Die Vorlage geht hervor aus der in der Botschaft vom 25. Januar 2012[46] zur Legislaturplanung 2011–2015 und im Bundesbeschluss vom 15. Juni 2012[47] über die Legislaturplanung 2011–2015 angekündigten Massnahme «Aktualisierung und Umsetzung der Strategie für eine Informationsgesellschaft» in der Schweiz.

4.2 Verhältnis zu nationalen Strategien des Bundesrates

4.2.1 Strategie für eine Informationsgesellschaft in der Schweiz

Zur Strategie: siehe Ziffer 1.1.1. Das ISG wurde im Vorhabenkatalog Informationsgesellschaft 2011–2015 (Stand November 2013) unter dem Handlungsfeld «Sicherheit und Vertrauen» aufgenommen. Es wird klare Grundlagen für die Sicherheitsanforderungen in den Projekten, die vom Bund durchgeführt werden, schaffen.

4.2.2 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

Zur NCS: siehe Ziffer 1.1.2; zum Verhältnis zwischen NCS und ISG: siehe Ziffer 1.2.7; zur Unterstützung der KI-Betreiber: siehe Artikel 75–81.

4.2.3 Nationale Strategie zum Schutz kritischer Infrastrukturen

Die Nationale Strategie vom 27. Juni 2012[48] zum Schutz kritischer Infrastrukturen (SKI-Strategie) hat zum Ziel, die Resilienz der Schweiz im Bereich der KI zu verstärken. Die Strategie bezeichnet dazu verschiedene Massnahmen in zwei Bereichen. Der Selbstschutz wird verbessert, indem die zuständigen Stellen integrale Schutzkonzepte erarbeiten und umsetzen. Darin werden infrastrukturspezifische Risiken identifiziert und reduziert. Im infrastrukturübergreifenden Bereich werden die Zusammenarbeit der Akteure (Behörden, Betreiberinnen) aus den verschiedenen KI-Sektoren verbessert und die Verletzlichkeit von Gesellschaft, Wirtschaft und Staat durch schwerwiegende Ausfälle verringert. Zu diesem Zweck werden Planungen zur Schadensbewältigung bei schwerwiegenden Ausfällen und zur subsidiären Unterstützung der KI-Betreiberinnen bei solchen Ereignissen erarbeitet. Der Bun-

46 BBl **2012** 481, hier 454, 602 und 609
47 BBl **2012** 7155, hier 7157
48 BBl **2012** 7715

desrat will die KI-Betreiberinnen in ihren eigenen Schutzbestrebungen unterstützen. Dabei soll auch die grösstmögliche Resilienz im Hinblick auf die Informationssicherheit erreicht werden. So sieht beispielsweise die Massnahme 7 der SKI-Strategie die Schaffung von formell-gesetzlichen Grundlagen zur Sicherheitsüberprüfung von ausgewähltem Personal der KI-Betreiberinnen vor. Das ISG unterstützt somit auch die Umsetzung der SKI-Strategie.

5 Rechtliche Aspekte

5.1 Verfassungs- und Gesetzmässigkeit

Nach Artikel 42 BV benötigt der Bundesgesetzgeber für seine Regelungen eine (ausdrückliche oder implizite) Verfassungsgrundlage. Für die Vorlage bestehen hinreichende Verfassungsgrundlagen. Formal handelt es sich bei diesem Erlass vorweg um übergreifende Organisationsbestimmungen für die Bundesbehörden. Das Organisationsrecht des Bundes wird zwar als Gesetzgebungskompetenz beim Katalog der Kompetenzausscheidung zwischen Bund und Kantonen in der BV nicht ausdrücklich erwähnt, doch führt Artikel 164 Absatz 1 Buchstabe g BV bei den Zuständigkeiten der Bundesversammlung «die Organisation und das Verfahren der Bundesbehörden» unter den Gegenständen auf, die in der Form des Bundesgesetzes zu erlassen sind (s. etwa den Ingress zum ParlG). Im Weiteren wird in der geltenden Organisationsgesetzgebung auch etwa auf Artikel 173 Absatz 2 BV verwiesen, welcher der Bundesversammlung alle Geschäfte zuweist, die in die Zuständigkeit des Bundes fallen und keiner anderen Behörde zugewiesen sind (siehe etwa den Ingress (mit Fussnote 1) zum RVOG oder zum BGÖ).

Inhaltlich sollen die Regelungen primär der Wahrung der Sicherheit des Landes im Innern und gegen aussen dienen sowie die Entscheidungs- und Handlungsfähigkeit der Behörden schützen. Insofern stützen sich die Regelungen auch auf Artikel 54 Absätze 1 und 2 BV (Beziehungen zum Ausland und Wahrung der äusseren Sicherheit) sowie auf Artikel 57 Absatz 1 BV, der den Bund und die Kantone beauftragt, «… im Rahmen ihrer Zuständigkeiten für die Sicherheit des Landes …» zu sorgen.

Nicht unter die erwähnten Ziele fallen die Bestimmungen zum BSV, soweit sie für Betriebe vorgesehen sind, die eine Betriebssicherheitserklärung benötigen, um sich für klassifizierte Aufträge ausländischer oder internationaler Behörden bewerben zu können. Diese Regelung wird durch Artikel 101 BV abgedeckt, der die Grundlage für die Förderung der Aussenwirtschaft bildet. Die Bestimmungen zum Schutz der KI können sich sowohl auf die Grundlagen im Bereich der inneren und äusseren Sicherheit als auch auf die Kompetenzen des Bundes im Bereich der Landesversorgung (Art. 102 BV) abstützen. Für die Armee kann auf Artikel 60 BV verwiesen werden, der die Organisation der Armee zur Bundessache erklärt.

5.2 Vereinbarkeit mit internationalen Verpflichtungen der Schweiz

Die Schweiz unterhält mit verschiedenen Staaten und internationalen Organisationen Informationsschutzabkommen (ISA; siehe SR *0.514.XXX*). Mit diesen Staatsverträgen hat sich die Schweiz zur Einhaltung gewisser Standards zum Schutz von Informationen dieser Staaten und Organisationen verpflichtet. Neben der EU hat die Schweiz auch ISA mit der ESA (*European Space Agency*) und der NATO abgeschlossen. Diese Verträge enthalten einheitliche Schutzmechanismen für das Bearbeiten von klassifizierten Informationen oder die gegenseitige Anerkennung von Sicherheitsbescheinigungen. So wird jeweils die für die Umsetzung der Sicherheitsmassnahmen zuständige Stelle genannt (*National Security Authority*). Im Bereich der Kommunikationssicherheit werden nationale Anlaufstellen verlangt, die einheitliche Standards festlegen und die Eignung der Systeme bestätigen (*Security Accreditation Authority*). Die Fachstelle des Bundes für Informationssicherheit wird diese Aufgaben für die Schweiz übernehmen.

Die internationalen Verpflichtungen der Schweiz im Bereich der Informationssicherheit stehen dem vorliegenden Gesetz nicht entgegen.

5.3 Erlassform

Der Bundesrat ist bereits in seinem Beschluss vom 12. Mai 2010 (s. Ziff. 1.1.4) davon ausgegangen, dass die wesentlichen Regelungen über die Informationssicherheit in der Form eines Bundesgesetzes festgelegt werden müssen. Einerseits handelt es sich um Organisations- und Verfahrensregelungen für die Bundesbehörden (Art. 164 Abs. 1 Bst. g BV), die infolge der Notwendigkeit der einheitlichen Geltung auch behördenübergreifende Wirkungen entfalten müssen. Den Kantonen werden ebenfalls Informationssicherheitspflichten auferlegt. Andererseits handelt es sich um Bestimmungen, die insbesondere im Bereich der PSP und des BSV erhebliche Eingriffe in grundrechtlich geschützte Positionen zur Folge haben (Art. 164 Abs. 1 Bst. b und c BV) oder für die aus Datenschutzgründen eine Verankerung auf formell-gesetzlicher Ebene unumgänglich ist (Art. 17 Abs. 2 DSG). Zum gesetzgeberischen Nachteil des einheitlichen Geltungsbereichs, siehe Ziffer 1.3: Vollzug.

5.4 Unterstellung unter die Ausgabenbremse

Die Vorlage untersteht nicht der Ausgabenbremse nach Artikel 159 Absatz 3 Buchstabe b BV, da sie weder Subventionsbestimmungen noch die Grundlage für die Schaffung eines Verpflichtungskredits oder Zahlungsrahmens enthält.

5.5 Einhaltung der Grundsätze der Subventionsgesetzgebung

Die Vorlage sieht keine Finanzhilfen oder Abgeltungen im Sinne des Subventionsgesetzes vom 5. Oktober 1990[49] vor.

5.6 Delegation von Rechtsetzungsbefugnissen

Rechtsetzungsbefugnisse können durch Bundesgesetz übertragen werden, soweit dies nicht durch die Bundesverfassung ausgeschlossen wird (Art. 164 Abs. 2 BV). Aufgrund des Geltungsbereichs, der alle Bundesbehörden erfasst, kann der Vollzug des Gesetzes nicht nach dem «ordentlichen» Schema erfolgen, wonach der Bundesrat grundsätzlich allein für das Ausführungsrecht zuständig ist. Zur Wahrung von deren Vollzugsautonomie sieht die Vorlage vor, dass die verpflichteten Behörden die nötigen Ausführungsbestimmungen selbst erlassen (Art. 85 Abs. 1). Diese Delegation bezieht sich auf das ganze Gesetz, sofern dieses die Rechtsetzungsbefugnis nicht ausdrücklich an den Bundesrat delegiert. Der Entwurf delegiert nachfolgende Rechtsetzungsbefugnisse an den Bundesrat:

- Artikel 2 Absätze 3 und 4: er legt fest, welche Einheiten der dezentralen Bundesverwaltung und Organisationen nach Artikel 2 Absatz 4 RVOG das Gesetz anwenden müssen;
- Artikel 12 Absatz 3: er regelt die Entklassifizierung von Archivgut;
- Artikel 32 Absatz 2: er muss die Fachstellen PSP einsetzen;
- Artikel 44 Absatz 2: er kann für Funktionen der Armee und des Zivilschutzes von der Wiederholung der PSP absehen;
- Artikel 49: er erlässt ergänzendes Recht zu den PSP und zum Datenschutz;
- Artikel 74: er erlässt ergänzendes Recht zum BSV, zum entsprechenden Datenschutz und regelt die Organisation der Fachstelle BS;
- Artikel 75 Absatz 5: er bezeichnet die Stellen, die für die Aufgaben zur Unterstützung der KI im Bereich der Informationssicherheit zuständig sind;
- Artikel 81: er erlässt ergänzendes Recht zur Informationssicherheit bei KI und zum entsprechenden Datenschutz;
- Artikel 84 Absatz 3: er regelt die Organisation der Fachstelle des Bundes für Informationssicherheit und kann ihr weitere Aufgaben zuweisen;
- Artikel 85 Absatz 1: er kann den Erlass von Ausführungsbestimmungen für Bundesratsgeschäfte der BK übertragen;
- Artikel 86: er legt Standardmassnahmen nach dem Stand von Wissenschaft und Technik fest. Er kann diese Aufgabe delegieren;

[49] SR **616.1**

- Artikel 87 Absatz 4: er entscheidet, auf welche Ressourcen des Bundes die Kantone für ihre eigenen Bedürfnisse zugreifen dürfen; er legt die Gebühren fest;
- Artikel 88: er kann völkerrechtliche Verträge selbständig abzuschliessen;
- Artikel 14 Absatz 2 MG: er legt die zu prüfenden Funktionen fest;
- Artikel 20*a* Absatz 2 StromVG: er legt fest, welche Personengruppen auf ihre Vertrauenswürdigkeit hin geprüft werden müssen.

5.7 Datenschutz

Für die Erfüllung der Aufgaben nach dieser Vorlage ist die Bearbeitung von Personendaten in den nachfolgenden Bereichen erforderlich:

- Artikel 19 Absatz 2: Die Bearbeitung von Personendaten im Rahmen der Überwachung der Netzwerke durch die Leistungserbringerinnen stützt sich auf bestehendes Recht (Art. 57*i*–57*q* RVOG).
- Artikel 20 Absatz 2: Für die Verwendung von biometrischen Daten zur Verifizierung der Identität von Personen, die Zugang zu Informationen, Informatikmitteln und Räumlichkeiten des Bundes benötigen, wird eine formellgesetzliche Grundlage im Sinne von Artikel 17 Absatz 2 DSG geschaffen.
- Artikel 24–27: Zum Einsatz von Informationssystemen zur zentralen Kontrolle von Identitäten werden ausführliche formell-gesetzliche Grundlagen im Sinne von Artikel 17 Absatz 2 DSG geschaffen. Da die Verantwortung für den Datenschutz möglicherweise geteilt wird, werden die verpflichteten Behörden (vor allem der Bundesrat) gestützt auf Artikel 16 Absatz 2 DSG die Verantwortung für den Datenschutz regeln. Der Einsatz solcher Systeme wird den operativen Datenschutz und die Datensicherheit verbessern.
- Artikel 28–49: Für die PSP ist die Bearbeitung von besonders schützenswerten Personendaten (Art. 3 Bst. c DSG) erforderlich. Das Ergebnis der PSP entspricht zudem einem Persönlichkeitsprofil (Art. 3 Bst. d DSG). Für die Bearbeitung dieser Daten schafft das ISG eine ausführliche formellgesetzliche Grundlage im Sinne von Artikel 17 Absatz 2 DSG. Da der Bundesrat mindestens zwei Fachstellen PSP einsetzen wird, muss er die Verantwortung für den Datenschutz noch im Detail regeln (Art. 16 Abs. 2 DSG). Insgesamt ist die Neuregelung in Bezug auf den Datenschutz wesentlich besser und verhältnismässiger als das heutige Recht (Art. 19–21 BWIS sowie Art. 144–149 MIG). Der Bundesrat will zudem die Anzahl Personen, die der PSP unterstehen, verringern, was die Bearbeitung von Personendaten entsprechend reduzieren wird.
- Artikel 50–74: Für die Durchführung von BSV ist die Bearbeitung von besonders schützenswerten Personendaten (Art. 3 Bst. c DSG) erforderlich. Für die Bearbeitung dieser Daten schafft das ISG eine ausführliche formellgesetzliche Grundlage im Sinne von Artikel 17 Absatz 2 DSG.

- Artikel 75–81: Zur Unterstützung der KI im Bereich der Informationssicherheit muss MELANI regelmässig Personendaten (Adressierungselemente) bearbeiten, die in bestimmten Fällen als besonders schützenswerte Personendaten gelten können. Dafür wird eine formell-gesetzliche Grundlage geschaffen.
- Änderung anderer Erlasse: Einige Bestimmungen anderer Erlasse regeln die Bearbeitung von Personendaten im Zusammenhang mit der PSP nach Artikeln 28–49. Dafür gelten die entsprechenden Erläuterungen sinngemäss.

Personendaten gelten im Sinne des ISG als Informationen, die bezüglich Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit geschützt werden müssen. Die Vorlage schafft die Grundlage für einheitliche, behördenübergreifende Prozesse, Massnahmen und Fähigkeiten zum Schutz der Informationen, für die der Bund zuständig ist. Im Rahmen des Vollzugs und insbesondere der Ausarbeitung von standardisierten Massnahmen wird der EDÖB einbezogen werden. Die ergänzende Anwendung des Gesetzes auf Personendaten wird deshalb auch die Umsetzung des Datenschutzes, insbesondere der Datensicherheit, verbessern.

Abkürzungsverzeichnis

AHVG	Bundesgesetz vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung; SR *831.10*
BAKOM	Bundesamt für Kommunikation
BGA	Archivierungsgesetz vom 26. Juni 1998; SR *152.1*
BGG	Bundesgerichtsgesetz vom 17. Juni 2005; SR *173.110*
BGÖ	Öffentlichkeitsgesetz vom 17. Dezember 2004; SR *152.3*
BGÖ-Botschaft	Botschaft vom 12. Februar 2003 zum BGÖ (BBl *2003* 1963)
BinfV	Bundesinformatikverordnung vom 9. Dezember 2011; SR *172.010.58*
BIT	Bundesamt für Informatik und Telekomunikation
BJ	Bundesamt für Justiz
BK	Bundeskanzlei
BöB	Bundesgesetz vom 16. Dezember 1994 über das öffentliche Beschaffungswesen; SR *172.056.1*
BPG	Bundespersonalgesetz vom 24. März 2000; SR *172.220.1*
BPI	Bundesgesetz vom 13. Juni 2008 über die polizeilichen Informationssysteme des Bundes; SR *361*
BSE	Betriebssicherheitserklärung
BSV	Betriebssicherheitsverfahren
BV	Bundesverfassung; SR *101*
BWIS	Bundesgesetz vom 21. März 1997 über Massnahmen zur Wahrung der inneren Sicherheit; SR *120*
CERT	Computer Emergency Response Team
DSG	Bundesgesetz vom 19. Juni 1992 über den Datenschutz; SR *235.1*
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDÖB	Eidgenössische/r Datenschutz- und Öffentlichkeitsbeauftragte
EDI	Eidgenössisches Departement des Innern
EFK	Eidgenössische Finanzkontrolle
EFD	Eidgenössisches Finanzdepartement
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EPA	Eidgenössisches Personalamt
Fedpol	Bundesamt für Polizei
FHG	Finanzhaushaltgesetz vom 7. Oktober 2005; SR *611.0*

FMG	Fernmeldegesetz vom 30. April 1997; SR *784.10*
FUB	Führungsunterstützungsbasis der Armee
GPDel	Geschäftsprüfungsdelegation
GPK-N	Geschäftsprüfungskommission des Nationalrats
GPK-S	Geschäftsprüfungskommission des Ständerats
GS	Generalsekretariat
IAM	Identity und Access Management
IDAG	Interdepartementale Arbeitsgruppe
IKT	Informations- und Kommunikationstechnologie bzw. -technik
IOS	Informations- und Objektsicherheit
ISA CH-EU	Abkommen vom 28. April 2008 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Union über die Sicherheitsverfahren für den Austausch von Verschlusssachen; SR *0.514.126.81*
ISB	Informatiksteuerungsorgan des Bundes
ISchV	Informationsschutzverordnung vom 4. Juli 2007; SR *510.411*
ISG	Entwurf eines Bundesgesetzes über die Informationssicherheit beim Bund bzw. eines Informationssicherheitsgesetzes
ISMS	Informationssicherheits-Managementsystem
KI	Kritische Infrastrukturen
KEG	Kernenergiegesetz vom 21. März 2003; SR *732.1*
MELANI	Melde- und Analysestelle Informationssicherung
MG	Militärgesetz vom 3. Februar 1995; *SR 510.10*
MStG	Militärstrafgesetz vom 13. Juni 1927; SR *321.0*
MIG	Bundesgesetz vom 3. Oktober 2008 über die militärischen Informationssysteme; SR *510.91*
MStP	Militärstrafprozess vom 23. März 1979; SR *322.1*
NBG	Nationalbankgesetz vom 3. Oktober 2003; *SR 951.11*
NCS	Nationale Strategie vom 27. Juni 2012 zum Schutz der Schweiz vor Cyber-Risiken (BBl *2013* 563)
NDB	Nachrichtendienst des Bundes
NDG	Nachrichtendienstgesetz vom 25. September 2015; BBl *2015* 7211
OGD	Open Government Data
ParlG	Parlamentsgesetz vom 13. Dezember 2002; SR *171.10*
PSP	Personensicherheitsprüfung bzw. Personensicherheitsprüfungen

PSPV	Verordnung vom 4. März 2011 über die Personensicherheitsprüfungen; SR *120.4*
RVOG	Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997; SR *172.010*
SIK	Schweizerische Informatikkonferenz
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937; SR *311.0*
StPO	Strafprozessordnung; SR *312.0*
StromVG	Stromversorgungsgesetz vom 23. März 2007; SR *734.7*
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VG	Verantwortlichkeitsgesetz vom 14. März 1958, SR *170.32*
VGG	Verwaltungsgerichtsgesetz vom 17. Juni 2005; SR *173.32*
VDSG	Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz; SR *235.11*
VwVG	Verwaltungsverfahrensgesetz vom 20. Dezember 1968; SR *172.021*