VBS Generalsekretariat
Recht VBS
Maulbeerstrasse 9
3003 Bern
recht-vbs@gs-vbs.admin.ch

Bern, 3. Juli 2014

Stellungnahme zum Entwurf eines neuen Bundesgesetzes über die Informationssicherheit

Sozialdemokratische Partei
der Schweiz

Spitalgasse 34
Postfach · 3001 Bern

Telefon 031 329 69 69
Telefax 031 329 69 70

info@spschweiz.ch
www.spschweiz.ch

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Zustellung der Vernehmlassungsunterlagen **zum Entwurf eines neuen Bundesgesetzes über die Informationssicherheit (ISG).** Gerne nehmen wir dazu Stellung.

Zusammenfassung

Die SP Schweiz begrüsst die Absicht und Stossrichtung des Gesetzesentwurfs. Die Affären um den Datendiebstahl im Nachrichtendienst, die Enthüllungen von Edward Snowden sowie weitere Vorfälle machten deutlich, dass der Bund mehr für die Sicherheit seiner Informationen tun muss. Der vorliegende Entwurf eines Bundesgesetzes über die Informationssicherheit (ISG) trägt nach Ansicht der SP durch seine Ausrichtung auf eine integrale Informationssicherheit dem gesellschaftlichen und technischen Wandel im Umgang mit Information (Stichworte: Chancen und Risiken der Informationsgesellschaft, Digitalisierung, Cyber, BigData, OpenData) angemessen Rechnung. Insgesamt bildet das neue ISG eine gute Grundlage für eine moderne, professionelle und umfassende Organisation des Informationsschutzes. Ob das Ziel am Ende erreicht wird, dürfte massgeblich von den zur Verfügung stehenden finanziellen und personellen Ressourcen abhängen.

Für die SP Schweiz ist zentral, dass das ISG nicht in Konflikt mit dem Öffentlichkeitsprinzip, dem Datenschutz, den Anforderungen an einen guten Service Public und anderen gleichrangigen Grundsätzen gerät. Die SP erwartet, dass Klassifizierungen – wie in Artikel 12 gefordert – tatsächlich „auf das notwendige Mindestmass“ beschränkt bleiben und auch die Sicherheitseinstufung von IKT-Mitteln so gehandhabt wird, dass das betroffene (Staats-)Personal seine Aufgaben weiterhin einfach und benutzerfreundlich erfüllen kann. Die SP fordert zudem an verschiedenen Stellen des Gesetzes, den Datenschutz zu stärken und die Einhaltung der Archivierungspflicht sicherzustellen.

Allgemeine Bemerkungen

Verfügbarkeit, Integrität und Vertraulichkeit der Daten als zentrale Zielsetzung der Informatiksicherheit ist zu gewährleisten: Die SP Schweiz begrüsst die Absicht und Stossrichtung des Gesetzesentwurfs. Zwei Affären in jüngster Vergangenheit riefen einer breiten Öffentlichkeit in Erinnerung, dass der Bund mehr für die Sicherheit seiner Informationen tun muss. 2012 kam es ausgerechnet im Nachrichtendienst des Bundes zu einem grossen Datendiebstahl, der zu allem Überfluss erst durch einen Tipp von Dritten erkannt wurde. Eine Inspektion der Delegation der Geschäftsprüfungskommissionen GPDel zeigte auf, dass selbst unser „Geheimdienst" als Organisation nicht genügend darauf ausgerichtet war, die Verfügbarkeit, die Integrität und die Vertraulichkeit der Daten als zentrale Zielsetzung der Informatiksicherheit zu gewährleisten. Wenig später enthüllte Edward Snowden, wie systematisch die Nachrichtendienste der USA selbst bei Regierungsmitgliedern von Bündnispartnern hoch sensible Informationen beschaffen. Wie der erläuternde Bericht zum ISG klarstellt, verdienen die Risiken der Informationsgesellschaft tatsächlich die vermehrte Aufmerksamkeit der Behörden. Das Ziel des Gesetzesentwurfes, den sicheren Umgang mit Informationen sowie den sicheren Einsatz von Informations- und Kommunikationstechnologien zu gewährleisten, kann die SP Schweiz uneingeschränkt unterstützen.

Negative Begleitfolgen in Bezug auf das Öffentlichkeitsprinzip und den Datenschutz vermeiden: Eine andere Frage ist, ob die vorgeschlagenen Massnahmen ohne negative Begleitfolgen ergriffen und durchgesetzt werden können. Die SP Schweiz erwartet namentlich, dass das neue Informationssicherheitsgesetz nicht in Konflikt mit dem Gedanken des Öffentlichkeitsprinzips gerät. Klassifizierungen müssen tatsächlich – wie in Artikel 12 E-ISG gefordert – „auf das notwendige Mindestmass" beschränkt bleiben. Auch die Sicherheitseinstufung von IKT-Mitteln muss so gehandhabt werden, dass das betroffene Staatspersonal seine Aufgaben weiterhin einfach, speditiv und benutzerfreundlich erfüllen kann. Zudem braucht es hinsichtlich Datenschutz verschiedene Nachbesserungen des ISG, damit mindestens das aktuelle Schutz-Niveau gehalten werden kann.

ISG ist kein Nachrichtendienstgesetz: Die im erläuternden Bericht angeführten Überlegungen sind nachvollziehbar, dass die aktuell im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR 120) enthaltenen Bestimmungen über die Personensicherheitsprüfung ins ISG (und die davon zu unterscheidende Prüfung der Vertraulichkeit in entsprechende Spezialgesetze) transferiert und gleichzeitig modernisiert werden. Anlässlich der missglückten Berufung von Roland Nef zum Chef der Armee wurden die Defizite des bisherigen Systems der Personensicherheitsprüfung augenfällig. Dies ist indes kein Grund, aus dem ISG ein zweites Nachrichtendienstgesetz zu machen. Die SP fordert, die im ISG – teilweise durch die Hintertüre – erfolgte, pauschale Ermächtigung zu nachrichtendienstlichen Tätigkeiten wieder zu entfernen und – falls tatsächlich unverzichtbar – im Nachrichtendienstgesetz unterzubringen, wo Verfahren wie Qualitätssicherung, gerichtliche Ermächtigung und parlamentarische Oberaufsicht geregelt werden können.

Informationssicherheit bei kritischen Infrastrukturen sorgfältiger regeln: Das ganze 5. Kapitel über die Informationssicherheit bei kritischen Infrastrukturen (E-ISG Art. 81 – Art. 83) muss grundsätzlich überarbeitet werden. Der Entwurf ISG enthält in diesem Kapitel unannehmbare pauschale Ermächtigungen zu nachrichtendienstlichen Tätigkeiten und klärt die Schnittstellen ungenügend zwischen der Gewährleistung der Informationssicherheit bei kritischen Infrastrukturen und dem Schutz kritischer Infrastrukturen an und für sich. Der Schutz kritischer Infrastrukturen ist aus sicherheitspolitischer Sicht eine viel zu wichtige Aufgabe, um ihn in derart unsorgfältiger, pauschaler Weise abzuhandeln, wie dies im Entwurf ISG gemacht wird.

Chancen und Risiken der Informationsgesellschaft richtig dargestellt; der korrekten Analyse muss nun aber auch die korrekte Mittelverteilung folgen: Die im allgemeinen Teil des erläuternden Berichtes vorgenommene Analyse der Chancen und Risiken der Informationsgesellschaft wird von der SP geteilt. Namentlich teilt die SP die Aussage, dass die Bekämpfung der Risiken nicht dazu führen darf, die Chancen der Informationsgesellschaft zu schmälern. Wenn zur angeb-

lichen Vermeidung eines „Cyber War“ eine massenhafte Überwachung des Internetverkehrs eingeführt wird, so läuft etwas schief. Unannehmbare wäre für die SP auch, wenn die Schweiz in das von einigen Grossmächten inszenierte digitale Wettrüsten einsteigen würde. Unter dem Deckmantel angeblicher Schutzvorkehrungen gegen den „Cyber war“ sind Mächte wie die USA, China oder Russland im Begriff, offensive militärische und nachrichtendienstliche Fähigkeiten aufzubauen. Die SP lehnt es ab, dass nun auch die Schweiz in dieses Wettrüsten einsteigen würde. Gefragt sind vielmehr vertrauensbildende Massnahmen durch grösstmögliche Transparenz und internationale Zusammenarbeit. Auch muss bei der Mittelverteilung die Priorität klar im zivilen und im alltäglichen Bereich gelegt werden. Entsprechend unterstützt die SP die Aussage des erläuternden Berichts zum ISG, Risiken seien nicht allein im Bereich „Cyber“ zu orten, sondern müssten breiter analysiert werden. Allerdings stellt die SP gleichzeitig fest, dass der Bundesrat bisher zwar gute Arbeit im Bereich der Analyse und der Formulierung einer „Nationalen Strategie für eine Informationsgesellschaft Schweiz 2011–2015“, einer „Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken“ (NCS) und einer „Nationalen Strategie zum Schutz kritischer Infrastrukturen“ (SKI-Strategie) geleistet hat. Bei der Umsetzung dieser Strategien bestehen aber grosse Lücken. Es fehlt in den zuständigen zivilen Departementen an personellen und finanziellen Ressourcen, um den Ankündigungen auch Taten folgen zu lassen. Für die SP ist klar: Die Hauptzuständigkeit muss weiterhin dezentral bei den zivilen Departementen liegen. Und es braucht eine Umverteilung der Mittel aus obsolet gewordenen Bereichen der militärischen Sicherheitspolitik in diese neuen Bereiche einer dringend geforderten zivilen Sicherheitspolitik. Wer tatsächlich einen Zugewinn an Sicherheit will, muss die durch das Gripen-Nein im VBS freigewordenen Mittel in der Höhe von rund 250 bis 300 Millionen Franken pro Jahr im Bereich der Risiken der Informationsgesellschaft, der Cyber-Risiken und dem Schutz kritischer Infrastrukturen einsetzen. Wie prekär die Ressourcenfrage ist, zeigt sich auch am erläuternden Bericht zum ISG, der sich um die Bezifferung der Folgekosten und zusätzlichen Stellen drückt. Ohne klare Antwort auf diese Frage würde aber auch das beste neue Gesetz nicht zu einem tatsächlichen Zugewinn an Sicherheit führen.

Stellungnahme zu einzelnen Artikeln

Ad Artikel 1: Zweck

Die SP Schweiz unterstützt den in Artikel 1, Absatz 1 umschriebenen Zweck des ISG, den sicheren Umgang mit Informationen sowie den sicheren Einsatz von Informations- und Kommunikationstechnologien zu gewährleisten. Auch der Verzicht auf eine Legaldefinition, was unter „Information“ zu verstehen ist, kann unterstützt werden. Es ergibt sich von selbst, dass dieser Begriff implizit auch (elektronische) Daten aller Art einschliesst.

Auch der Versuch in Absatz 2, die zu schützenden „öffentlichen Interessen“ zu benennen, ist nachvollziehbar. Die gewählten Begriffe sind freilich von einem derart hohen Abstraktionsgrad, dass sie einen äusserst breiten Interpretationsraum offen lassen. Dies birgt das Risiko für exzessive Interpretationen. Dieses Risiko ist umso höher einzustufen, als Artikel 1 Absatz 2 Buchstaben a-d weiter hinten im Gesetz als Grundlage herangezogen wird, um die Klassifizierungsstufen (Art. 14 E-ISG) und die Sicherheitseinstufung von IKT-Mitteln (Art. 21 E-ISG) zu bestimmen.

Es ist zu begrüssen, dass der erläuternde Bericht einschränkende Definitionen der zu schützenden „öffentlichen Interessen“ enthält. So wird beispielsweise klargestellt, dass unter „wirtschafts-, finanz- und währungspolitische Interessen der Schweiz“ (Art. 1 Abs. 2 Bst. d E-ISG) allein Informationen der Bundesbehörden über gesamtwirtschaftliche Phänomene zu verstehen sind. Diese Einschränkung geht allerdings nicht aus dem Wortlaut von Art. 1 Abs. 2 Bst. d E-ISG hervor. Dort könnte auch der falsche Eindruck entstehen, unter „wirtschafts-, finanz- und währungspolitischen Interessen der Schweiz“ seien auch privatwirtschaftliche Einzelinteressen subsumiert.

Die SP regt deshalb an, im Zweckartikel präzisere, d.h. eindeutigere Begriffe und Formulierungen zu verwenden.

Ad Artikel 2. Verpflichtete Behörden und Organisationen

Der Geltungsbereich des ISG wird in Artikel 2 ausgesprochen breit gefasst. Dafür gibt es gute Gründe, bewegt sich das ISG doch in einem derart stark vernetzten Bereich, dass ein stärker sektorielles oder föderalistisches legislatives Vorgehen schnell an seine Grenzen stossen würde.

Aus Sicht der SP Schweiz geht es aber nicht, einen derart weit ausgestreckten Arm des Bundesgesetzgebers vorzusehen, dann aber keine Rechenschaft über die organisatorischen, personellen und finanziellen Folgen für Bund, Kantone, Gemeinden und beauftragte weitere Behörden abzulegen. Im erläuternden Bericht wird dazu lapidar vermerkt, die Kosten der notwendigen Verbesserung der Informationssicherheit beim Bund und den weiteren betroffenen Behörden könnten „jedoch erst nach der Durchführung der Vernehmlassung sachgemäss abgeschätzt werden".

Die SP erwartet, dass die organisatorischen, personellen und finanziellen Folgen des ISG in der Botschaft sauber dargelegt werden und der Bund sicherstellt, dass bei allen verpflichteten Behörden ausreichend Ressourcen für einen sachgemässen Vollzug zur Verfügung stehen. Die grössten Lücken bei der Informationssicherung und dem Schutz der IKT-Strukturen bestehen heute weniger auf der konzeptionellen und legislativen Ebene, als in organisatorischen Mängeln und namentlich in der ungenügenden finanziellen und personellen Ausstattung der zuständigen Stellen.

Ad Artikel 3. Vorbehalt des Öffentlichkeitsgesetzes

Obschon Art. 3, Abs. 1 E-ISG das Öffentlichkeitsgesetz (BGÖ, SR 152.3) ausdrücklich vorbehält, sind die Wechselwirkungen zwischen dem ISG und dem im BGÖ verankerten Öffentlichkeitsprinzip nicht wirklich geklärt. Für die SP Schweiz ist zentral, dass das neue ISG nicht zu mehr Klassifizierungen führt, als dies bisher der Fall war. Andernfalls ist das Risiko gross, dass das Öffentlichkeitsprinzip eingeschränkt wird, zeigt doch die BGÖ-Praxis, dass einmal klassifizierte Dokumente deutlich seltener gestützt auf das Öffentlichkeitsprinzip zugänglich gemacht werden.

Diese Ambivalenz bildet sich auch im erläuternden Bericht zum ISG ab. Einerseits betont dieser: "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." Andererseits betont der Bericht auch: "Die Klassifizierung von Informationen kann bei der Beurteilung von Dokumenten nach BGÖ jedoch als Indiz für die Nichtöffentlichkeit des entsprechenden Dokuments gewertet werden."

Die SP Schweiz erwartet, dass die Bestimmungen über die Klassifizierung inhaltlich so gestaltet werden, dass sie unter keinen Umständen über den Ausnahmekatalog nach Art. 7 BGÖ hinausgehen und diesem zumindest inhaltlich nicht widersprechen. Es muss sichergestellt sein, dass das ISG in Zukunft nicht zu noch mehr Streitfällen zwischen Nutzern des BGÖ und der Verwaltung führt. Und käme es dennoch zu zusätzlichen Streitfällen, so muss parallel zur Stärkung der Informationssicherung auch der Vollzug des Öffentlichkeitsprinzips gestärkt werden.

Eine Schlüsselrolle bei der Etablierung einer guten Rechtspraxis nimmt der Öffentlichkeitsbeauftragte EDÖB ein. Der EDÖB vermittelt nicht nur zwischen BGÖ-Nutzerinnen und -Nutzern, sondern entlastet mit seinem Mediationsprozess auch die Bundesgerichte. Denn seine Empfehlungen werden, zumindest von den Medienschaffenden, meistens akzeptiert.

Allerdings ist der EDÖB bereits heute nur ungenügend mit Ressourcen ausgestattet. Entsprechend bekräftigt die SP Schweiz gerade im Zusammenhang mit diesem konfliktträchtigen neuen Gesetz die Forderung, dem EDÖB endlich die nötigen Ressourcen zu geben.

Es ist ein Ärgernis, dass das Büro von Hanspeter Thür die im BGÖ gesetzlich vorgesehene Bearbeitungszeit noch immer um ein Vielfaches überschreitet. Weil nur gut begründete Empfehlungen aber zur gewünschten Klärung und einer guten Einsichtspraxis führen, ist eine Aufstockung des Stellenetats unumgänglich. Denn es wäre niemandem gedient, aufgrund der Ressourcenknappheit nun oberflächlichere Empfehlungen zu Streitfällen abzugeben.

Vorbehalt des Prinzips Open Government Data

Eng mit dem Öffentlichkeitsprinzip verbunden ist das Konzept der Open Government Data (OGD). Die SP setzt sich seit langem für eine offensive ODG-Strategie ein. Als Open Government Data (OGD) wird die offene Zugänglichkeit und freie Wiederverwendung von Behördendaten bezeichnet, sofern dadurch nicht Datenschutz-, Urheberrechts- oder Informationsschutzbestimmungen verletzt werden. OGD basiert auf dem Öffentlichkeitsprinzip und verspricht mehr Transparenz, gesellschaftlichen Nutzen und wirtschaftliches Wachstum. Umfragen zeigen, dass sich die Mehrheit der Bevölkerung mehr Transparenz wünscht und davon überzeugt ist, dass die Verwaltung dadurch effektiver arbeiten kann. Auch die demokratische Mitwirkung kann dadurch gestärkt werden. OGD ist bereits Realität: Swisstopo verfolgt eine Open access Strategie. In der Strategie e-government des Bundes ist OGD ein Bestandteil. Die Ratifizierung der Aarhus-Konvention führt dazu, dass die Schweiz bei Umweltdaten dem Transparenzprinzip nachlebt. Auch das Pilotprojekt "Single Point of Orientation" des Schweizerischen Bundesarchivs zeigt, wie eine bürgerfreundliche Übersicht über die Unterlagen der Bundesverwaltung realisiert werden kann.

Die SP erwartet, dass das neue ISG diesen Projekten und generell der vom Bundesrat in seinem Bericht vom 13. September 2013 bekräftigten ODG-Strategie keine Hindernisse in den Weg legt. Es ist deshalb zu prüfen, ob im ISG ein entsprechender ausdrücklicher Vorbehalt zu verankern ist.

Ad Artikel 4: Informationssicherheit

Aus Sicht der SP Schweiz fehlt in dieser Bestimmung die Nennung des Grundsatzes der Verhältnismässigkeit. Die SP regt deshalb folgende Ergänzung an:

Art. 4 Abs. 3^{bis} (neu)

[3] Sie sorgen für die Verhältnismässigkeit der ergriffenen Schutzmassnahmen. Diese sind nur so lange zulässig, bis ihr Zweck erreicht ist oder sich zeigt, dass er nicht erreicht werden kann. Zudem darf eine solche Massnahme zu keinem Nachteil führen, der zum angestrebten Erfolg in einem offenbaren Missverhältnis steht.

Ad Artikel 6: Risikomanagement

Die verantwortlichen Behörden und Organisationen sollen generell dafür sorgen, dass Risiken vermieden oder auf ein tragbares Mass reduziert werden – sowohl die identifizierten als auch die noch nicht erkannten. In Absatz 2 ist die Einschränkung „identifiziert“ deshalb zu streichen:

Art. 6 Abs. 2

... werden, um ~~die identifizierten~~ Risiken zu vermeiden oder ...

Ad Artikel 11: Kontrollen

Dieser Artikel verpflichtet die Behörden, die Einhaltung der ISG-Vorschriften und die Wirksamkeit der getroffenen Massnahmen regelmässig zu überprüfen. Das sind Informationen, die auch die parlamentarische Oberaufsicht interessieren. Die SP schlägt deshalb folgende Ergänzung vor:

Art. 11 Abs. 3 (neu)

[3] Die Ergebnisse der Kontrollen nach Absatz 1 und 2 werden periodisch den Geschäftsprüfungskommissionen der eidgenössischen Räte zur Kenntnis gebracht.

Ad Artikel 13: Zuständigkeiten

Gemäss dieser Bestimmung dürfen Klassifizierungen nur von der klassifizierenden Stelle oder von der ihr vorgesetzten Stelle geändert oder aufgehoben werden. Je nach Situation müsste nach Auffassung der SP auch die verpflichtete Behörde selbst die Möglichkeit haben, die Klassifizierung zu ändern.

Ad Artikel 31: Sicherheitszonen

Die Verwendung von biometrischen Verifikationsmethoden im Sinne von Abs. 3 Bst. a dieser Bestimmung sollte genauer geregelt werden. So ist insbesondere festzulegen, wie lange entsprechende Profile aufbewahrt werden dürfen.

Bei der Erlaubnis zu Taschen- und Personenkontrollen nach Abs. 3 Bst. d können faktisch Amts- und Berufsgeheimnisse verletzt werden. Zudem stellt diese Bestimmung eine grosse Gefahr dar, da allenfalls die Effekten hoher Geheimnisträgerinnen oder -träger durch sicherheitsmässig nicht genügend hoch qualifiziertes Personal überprüft werden könnten, wodurch dieses Kontrollpersonal unweigerlich von Geheimnissen Kenntnis erhielte, ohne dass es der eigenen Sicherheitsüberprüfung entspricht. Die Erlaubnis zu Personen- und Taschenkontrollen muss deshalb näher umschrieben werden, damit der Zweck des Gesetzes nicht obsolet wird.

Unangemeldete Raumkontrollen des Personals im Sinne von Abs. 3 Bst. e müssen ebenso näher umschrieben werden, zumal dadurch allenfalls auch private Wohnräume betroffen sein könnten, was bei der generellen Kontrollzulässigkeit zu einem Konflikt mit der Achtung des Privat- und Familienlebens im Sinne von Art. 8 der Europäischen Menschenrechtskonvention führen könnte.

3. Kapitel: Personensicherheitsprüfung (Art. 32–55)

Beim Transfer der aktuellen Bestimmungen über die Personensicherheitsprüfung aus dem Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR 120) in das ISG wurde darauf verzichtet, auch BWIS Art. 20 über den Prüfungsinhalt zu übernehmen. Da es um Daten geht, die aus Sicht des Daten- und Persönlichkeitsschutzes äusserst sensitiv sind, ist für die SP eine ausreichend hohe regulatorische Dichte in diesem Bereich zwingend. Auch ist wie bisher explizit auszuschliessen, dass Fichen über die politische Betätigung angelegt werden. Die SP regt deshalb an, BWIS Art. 20 Abs. 1 in modifizierter Form ins ISG zu übernehmen:

Art. 32bis Prüfungsinhalt Bei der Sicherheitsprüfung werden sicherheitsrelevante Daten über die Lebensführung der betroffenen Person erhoben, insbesondere über ihre engen persönlichen Beziehungen und familiären Verhältnisse, ihre finanzielle Lage, ihre Beziehungen zum Ausland und Aktivitäten, welche die innere oder die äussere Sicherheit in rechtswidriger Weise gefährden können. Über die Ausübung der verfassungsmässigen Meinungs- und Informationsfreiheit werden keine Daten erhoben.

Ad Artikel 39: Datenerhebung

BWIS Art. 20 Abs. 2 enthält eine abschliessende Liste jener Stellen, bei denen zur Beurteilung des Sicherheitsrisikos Daten erhoben werden dürfen. Erwähnt werden ausschliesslich Behörden. Einzige Ausnahme bildet im BWIS die in Bst. e. vorgesehene Befragung von Drittpersonen. Dies ist laut BWIS nur möglich sein, „wenn die betroffene Person zugestimmt hat“. Die SP regt an, diese Einschränkung beizubehalten. Die im E-ISG Art. 39 Abs. 3 Bst. c vorgeschlagene vollständige Aushebelung des Bankgeheimnisses lehnt die SP deshalb ab. Das Bankgeheimnis soll in geeigneter Form gegenüber den Steuerbehörden aufgehoben werden. Dann können die Organe der Personensicherheitsprüfung alle relevanten Angaben über die finanziellen Verhältnisse der betroffenen Personen bei den Steuerbehörden abrufen und müssen sich nicht an Private (Banken etc.) wenden.

Art. 39 Abs. 3 Bst. c c. Bei Finanzinstituten und Banken, mit welchen die zu prüfende Person Geschäftsbeziehungen unterhält, wenn die betroffene Person zugestimmt hat.

Ad Artikel 54: Datenaufbewahrung und -vernichtung

Der in Absatz 6 vorgeschlagene Archivierungs-Vorbehalt nach den Vorschriften des Archivierungsgesetzes ist zu schwach ausgestaltet. Indem dieser Vorbehalt nicht bereits unmittelbar nach

Absatz 2 sowie im Titel erwähnt wird, könnte der Eindruck entstehen, dass zur Vernichtung bestimmte Akten nicht archivierungspflichtig sind. Diese Interpretation würde aber klar gegen die Archivierungspflicht gemäss aktuellem Archivierungsgesetz (SR 152.1) verstossen. Wie wichtig dem Gesetzgeber die Archivierungspflicht ist, zeigte sich auch anlässlich der jüngsten Revision des Bundesgesetzes über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes ZNDG (SR 121). Auf Anregung der GPDel fügten die eidg. Räte in der Vorlage 13.064 im ZNDG den neuen Art. 7a über die Archivierung ein. Diese Bestimmungen sind auch in das ISG zu übernehmen.

Der Vorbehalt des Archivierungsgesetzes muss deshalb unmittelbar nach Absatz 2 placiert und auch im Titel explizit erwähnt werden. Zudem braucht eine explizite Norm, dass die Archivierungspflicht nach aktuellem Archivierungsgesetz (SR 152.1) nicht durch die willkürliche Vernichtung von Akten umgangen werden darf. Auch ist dem Bundesarchiv das explizite Recht einzuräumen, die Einhaltung der Archivierungspflicht zu überprüfen.

Die SP schlägt deshalb folgenden neuen Titel von Art. 54, die neuen Absätze Abs. 2^{bis} und Abs. 2^{ter} sowie die Verschiebung von Abs. 6 (neu: Abs. 2^{quater}) vor:

Art. 54 Titel neu: „Archivierungspflicht und Datenaufbewahrung und –vernichtung“
Abs. 2^{bis} (neu) Die Fachstellen PSP bieten alle nicht mehr benötigten oder zur Vernichtung bestimmten Unterlagen dem Bundesarchiv zur Archivierung an. Die vom Bundesarchiv als nicht-archivwürdig eingestuften Unterlagen werden vernichtet.
Abs. 2^{ter} (neu) Die Fachstellen PSP gewähren dem Bundesarchiv mit Blick auf die langfristige Sicherung der Unterlagen Einblick in den Index des Informationssystems nach Art. 52.
Abs. 2^{quater} Die Vorschriften des Archivierungsgesetzes (SR 152.1) und des Bundesgesetzes über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (SR 121, Art. 7a) zur Archivierung der Daten bleiben vorbehalten.

Ad Artikel 79: Datenaufbewahrung und -vernichtung

Dieselben Überlegungen sind auch bei Art. 79 E-ISG zu berücksichtigen, wo es um die Aufbewahrung und Vernichtung von Daten geht, welche die für die Durchführung des Betriebssicherheitsverfahrens zuständige Fachstelle für Betriebssicherheit (Fachstelle BS) erhebt:

Art. 79 Titel neu: „Archivierungspflicht und Datenaufbewahrung und –vernichtung“
Abs. 2^{bis} (neu) Die Fachstelle BS bietet alle nicht mehr benötigten oder zur Vernichtung bestimmten Unterlagen dem Bundesarchiv zur Archivierung an. Die vom Bundesarchiv als nicht-archivwürdig eingestuften Unterlagen werden vernichtet.
Abs. 2^{ter} (neu) Die Fachstelle BS gewährt dem Bundesarchiv mit Blick auf die langfristige Sicherung der Unterlagen Einblick in sein internes Registratursystem.
Abs. 2^{quater} Die Vorschriften des Archivierungsgesetzes (Ar. 152.1) und des Bundesgesetzes über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (SR 121, Art. 7a) zur Archivierung der Daten bleiben vorbehalten.

Ad Artikel 81: Aufgaben des Bundes

Absatz 3 ermächtigt in pauschalen Formulierungen zum Austausch nicht näher bestimmter Informationen zwischen nicht näher bestimmten Betreibern und Betreiberinnen von kritischen Infrastrukturen und nicht näher bestimmten Stellen des Bundes. Die SP fordert, hier Klarheit zu schaffen und die Regelungsdichte deutlich zu erhöhen. Mindestens ist folgender neuer Absatz 4 einzufügen:

Art. 81
Abs. 4 (neu) Die Bestimmungen des Datenschutzgesetzes bleiben vorbehalten.

Ad Artikel 82: Bearbeitung von Personendaten

Gemäss dieser Regelung dürfen die zuständigen Stellen bei kritischen Infrastrukturen zur Abwehr von Gefahren Personendaten, insbesondere Adressierungselemente im Fernmeldebereich, bearbeiten und weitergeben und dies sogar, ohne dass es für die betroffenen Personen ersichtlich wird. Damit wird unter dem Vorwand der Informationssicherheit ein Instrument geschaffen, um besonders schützenswerte Personendaten von einer Vielzahl von Personen bearbeiten zu dürfen. Es fehlt an jeglicher Kontrolle oder rechtlicher Möglichkeit, einem allfälligen Missbrauch Einhalt gebieten zu können. Beim vorliegenden Gesetz geht es indessen darum, den sicheren Umgang mit Informationen zu gewährleisten. Es darf nicht als Hintertüre verwendet werden, um nachrichtendienstlich tätig zu werden. Aus diesem Grunde fordert die SP, Art. 82 zu streichen.

Art. 82
streichen

Ad Artikel 83: Ergänzende Bestimmungen des Bundesrats

Die SP lehnt die in Art. 83 E-ISG vorgenommene Kompetenzdelegation an den Bundesrat ab. Ein Informationssicherungsgesetz hat nicht die Aufgabe, durch die Hintertüre irgendwelche anonyme private Stellen und Behörden zu nachrichtendienstlichen Tätigkeiten zu ermächtigen.

Die Aufgabenteilung und Zusammenarbeit zwischen Stellen, welche Aufgaben nach Art. 81 wahrnehmen, und dem Nachrichtendienst des Bundes, muss auf Gesetzesstufe geregelt werden. Die Stellen sind aus datenschutzrechtlichen Gründen einzeln zu benennen, welche die Kompetenz erhalten, nachrichtendienstliche Informationen auszutauschen. Auch ist zu spezifizieren, welche Informationen diese Stellen mit dem Nachrichtendienst austauschen können. Weil es dabei oft um besonders schützenswerte Personendaten geht, ist im ISG die übliche hohe Normendichte einzuhalten. Kann dieses Ziel nicht erreicht werden, ist in Art. 83 E-ISG explizit jegliche nachrichtendienstliche Tätigkeit auszuschliessen.

Ad Artikel 85: Konferenz der Informationssicherheitsbeauftragten

Die Konferenz der Informationssicherheitsbeauftragten soll nicht allein die Koordination mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) suchen, sondern auch für die Koordination mit den jeweils betroffenen kantonalen Datenschutzbeauftragten sorgen.

Überträgt das ISG dem EDÖB neue Aufgaben, so muss der Bund für zusätzliche finanzielle und personelle Mittel besorgt sein. Die SP erwartet, dass die Botschaft zum ISG darlegen wird, mit wie vielen zusätzlichen Stellen der EDÖB ausgestattet wird, um diese wichtige, aber zusätzliche Aufgabe zu erfüllen.

Wir danken Ihnen, geschätzte Damen und Herren, für die Berücksichtigung unserer Anliegen und verbleiben mit freundlichen Grüssen

Sozialdemokratische Partei der Schweiz

Christian Levrat
Präsident

Peter Hug
Politischer Fachsekretär