Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

**Generalsekretariat VBS**
Recht VBS

**16. Oktober 2014**

# Entwurf eines Bundesgesetzes über die Informationssicherheit (ISG)

## Bericht über das Ergebnis des Vernehmlassungsverfahrens

**Entwurf eines Bundesgesetzes über die Informationssicherheit (ISG): Bericht über das Ergebnis des Vernehmlassungsverfahrens**

# Inhaltsverzeichnis


1 Ausgangslage ... 3
2 Vernehmlassungsteilnehmer ... 3
2.1 Kantone ... 4
2.2 In der Bundesversammlung vertretene politische Parteien ... 4
2.3 Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete ... 4
2.4 Gesamtschweizerische Dachverbände der Wirtschaft ... 4
2.5 Weitere interessierte Organisationen ... 5
2.6 Nicht individuell eingeladene Teilnehmer ... 5
3 Generelle Beurteilung ... 5
3.1 Kantone ... 7
3.2 In der Bundesversammlung vertretene politische Parteien ... 10
3.3 Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete ... 11
3.4 Gesamtschweizerische Dachverbände der Wirtschaft ... 11
3.5 Weitere interessierte Organisationen ... 11
3.6 Nicht individuell eingeladene Teilnehmer ... 12
4 Stellungnahmen zum allgemeinen Teil des erläuternden Berichts ... 14
4.1 Risiken der Informationsgesellschaft ... 14
4.2 Heutige Organisation der Informationssicherheit in der Bundesverwaltung ... 14
5 Stellungnahmen zu den Gesetzesentwürfen und deren Erläuterungen ... 14
5.1 Bundesgesetz über die Informationssicherheit ... 15
Titel ... 15
1. Kapitel: Allgemeine Bestimmungen ... 15
2. Kapitel: Allgemeine Massnahmen der Informationssicherheit ... 20
3. Kapitel: Personensicherheitsprüfungen ... 31
4. Kapitel: Betriebssicherheitsverfahren ... 37
5. Kapitel: Informationssicherheit bei kritischen Infrastrukturen (KI) ... 41
6. Kapitel: Organisation und Vollzug ... 43
7. Kapitel: Schlussbestimmungen ... 49
5.2 Änderung anderer Erlasse ... 49
6 Stellungnahmen zu den im erläuternden Bericht dargestellten Auswirkungen ... 49
6.1 Auswirkungen auf den Bund ... 50
6.2 Auswirkungen auf die Kantone und Gemeinden ... 51
6.3 Auswirkungen auf die Volkswirtschaft ... 53
7 Stellungnahmen zu den rechtlichen Aspekten ... 53

## 1 Ausgangslage

Die Gefahren und Bedrohungen für Informationen sind mit der Entwicklung zu einer Informationsgesellschaft komplexer und dynamischer geworden. Mehrere Angriffe auf Informationssysteme des Bundes haben aufgezeigt, dass der Schutz von Informationen beim Bund Lücken aufweist. Diese Lücken, insbesondere im organisatorischen Bereich, sind auch auf unzeitgemässe oder inkohärente Rechtsgrundlagen zurückzuführen.

In Zusammenarbeit mit den Departementen, der Bundeskanzlei sowie anderen Bundesbehörden hat das VBS den Entwurf eines neuen Bundesgesetzes über die Informationssicherheit erarbeitet. Das Informationssicherheitsgesetz soll die Kernelemente der Informationssicherheit an einer Stelle zusammenfassen. Es regelt insbesondere das Risikomanagement, die Klassifizierung von Informationen und die Grundsätze der Sicherheit beim Einsatz der Informations- und Kommunikationstechnologie. Das Öffentlichkeitsprinzip in der Verwaltung soll weiterhin uneingeschränkt gelten, weshalb das ISG explizit den Vorbehalt des Öffentlichkeitsgesetzes vorsieht. Das Gesetz soll zudem die Personensicherheitsprüfungen neu regeln und ein einheitliches Betriebssicherheitsverfahren schaffen. Es soll ferner die Unterstützung der kritischen Infrastrukturen beim Risikomanagement im Bereich der Informationssicherheit regeln. Schliesslich soll es eine gesetzliche Grundlage für den Abschluss von völkerrechtlichen Vereinbarungen im Bereich der Informationssicherheit durch den Bundesrat liefern.

Wegen der Zunahme der Vernetzung der Systeme und des elektronischen Informationsaustauschs soll das Gesetz nicht nur für die Bundesverwaltung und die Armee, sondern auch für das Parlament, die eidgenössischen Gerichte, die Bundesanwaltschaft und ihre Aufsichtsbehörde sowie die Nationalbank gelten. Kantone, Private und die Wirtschaft sollen nur dann betroffen sein, wenn sie im Auftrag des Bundes sicherheitsempfindliche Tätigkeiten ausführen.

Der Bundesrat hat am 26. März 2014 das VBS beauftragt, bei den Kantonen, den politischen Parteien, den gesamtschweizerischen Dachverbänden der Gemeinden, Städte und Berggebiete, den gesamtschweizerischen Dachverbänden der Wirtschaft und den interessierten Kreisen ein Vernehmlassungsverfahren zum Entwurf des Informationssicherheitsgesetzes durchzuführen. Das Vernehmlassungsverfahren dauerte bis zum 4. Juli 2014.

## 2 Vernehmlassungsteilnehmer

Zur Vernehmlassung eingeladen wurden 62 Organisationen:

- alle 26 Kantone sowie die Konferenz der Kantonsregierungen;
- alle 13 in der Bundesversammlung vertretenen politischen Parteien;
- 3 gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete;
- 9 gesamtschweizerische Dachverbände der Wirtschaft;
- 10 weitere interessierte Organisationen.

Die Eröffnung der Vernehmlassung wurde zudem im Bundesblatt vom 8. April 2014 öffentlich bekannt gegeben.

Eine Vernehmlassung eingereicht haben:

- alle 26 Kantone;
- 4 in der Bundesversammlung vertretene politische Parteien;
- 1 gesamtschweizerischer Dachverband der Gemeinden, Städte und Berggebiete;
- 4 gesamtschweizerische Dachverbände der Wirtschaft;
- 9 weitere interessierte Organisationen;
- 11 nicht individuell eingeladene Teilnehmer;

Das ergibt ein Total von 55 Vernehmlassungen.

Im Folgenden werden die Vernehmlassungsteilnehmer, die eine schriftliche Eingabe gemacht haben, namentlich aufgeführt. Die Ausdrücke in den Klammern entsprechen den im weiteren Text verwendeten Abkürzungen.

### 2.1 Kantone

Eine Vernehmlassung eingereicht haben:

- Kanton Zürich (ZH)
- Kanton Bern (BE)
- Kanton Luzern (LU)
- Kanton Uri (UR)
- Kanton Schwyz (SZ)
- Kanton Obwalden (OW)
- Kanton Nidwalden (NW)
- Kanton Glarus (GL)
- Kanton Zug (ZG)
- Kanton Freiburg (FR)
- Kanton Solothurn (SO)
- Kanton Basel-Stadt (BS)
- Kanton Basel-Landschaft (BL)
- Kanton Schaffhausen (SH)
- Kanton Appenzell Innerrhoden (AI)
- Kanton Appenzell Ausserrhoden (AR)
- Kanton Sankt Gallen (SG)
- Kanton Graubünden (GR)
- Kanton Aargau (AG)
- Kanton Thurgau (TG)
- Kanton Tessin (TI)
- Kanton Waadt (VD)
- Kanton Wallis (VS)
- Kanton Neuenburg (NE)
- Kanton Genf (GE)
- Kanton Jura (JU)

### 2.2 In der Bundesversammlung vertretene politische Parteien

Eine Vernehmlassung eingereicht haben:

- Christlichdemokratische Volkspartei (CVP)
- FDP.Die Liberalen (FDP)
- Schweizerische Volkspartei (SVP)
- Sozialdemokratische Partei (SP)

### 2.3 Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete

Der Schweizerische Städteverband (SSV) hat trotz der unbestrittenen Bedeutung der Vorlage aus Kapazitätsgründen ausdrücklich auf eine Vernehmlassung verzichtet, verweist jedoch auf die Stellungnahme der Schweizerischen Informatikkonferenz.

### 2.4 Gesamtschweizerische Dachverbände der Wirtschaft

Eine Vernehmlassung eingereicht haben:

- economiesuisse
- Schweizerischer Gewerbeverband (SGV)

Der Schweizerische Arbeitgeberverband (SAGV) verzichtete ausdrücklich auf eine Stellungnahme, da die Vorlage die Wirtschaft als Arbeitgeber nicht direkt betreffe. Der Kaufmännische Verband Schweiz (KVS) verzichtete aufgrund beschränkter Ressourcen ausdrücklich auf eine Stellungnahme zu einer Vorlage, die keine spezifisch die kaufmännisch Angestellten betreffende Punkte enthalte.

### 2.5 Weitere interessierte Organisationen

Eine Vernehmlassung eingereicht haben:

- Aufsichtsbehörde über die Bundesanwaltschaft (AB-BA)
- Bundesanwaltschaft (BA)
- Privatim, die schweizerischen Datenschutzbeauftragten (privatim)
- Schweizerische Informatikkonferenz (SIK)
- Schweizerische Nationalbank (SNB)
- Schweizerisches Bundesgericht (BGer)
- Swico – Der Wirtschaftsverband für die digitale Schweiz (swico)

Auf eine Vernehmlassung ausdrücklich verzichtet haben:

- Schweizerisches Bundespatentgericht (BPatGer)
- Schweizerisches Bundesverwaltungsgericht (BVGer)

### 2.6 Nicht individuell eingeladene Teilnehmer

Eine Vernehmlassung eingereicht haben:

- Association suisse de la sécurité de l'information (Clusis)
- Centre Patronal, Equipes Patronales (CP)
- Centre Patronal, Chambre vaudoise des arts et métiers (CVAM)
- Fédération des Entreprises Romands (FER)
- Insecor GmbH (insecor)
- IT-Riskmanagement GmbH (it-rm)
- Lehmann Beat (LB)
- Nachrichtendienst des Bundes (NDB)
- Rat der Eidgenössischen Technischen Hochschulen (ETH-Rat)
- Rektorenkonferenz der Schweizer Universitäten (crus.ch)
- Verbindung der Schweizer Ärztinnen und Ärzte (FMH)

## 3 Generelle Beurteilung

Die nachstehenden Tabellen vermitteln eine Übersicht über die generelle Beurteilung der Vernehmlassungsvorlage durch die Teilnehmenden:

*Grobübersicht Resultat*

| **Wer** | **Ja** | **Ja, aber** | **Nein, aber** | **Nein** | **Kein Kom.** | **Total** |
|---|---|---|---|---|---|---|
| *Kantone* | 7 | 18 | 1 | | | *26* |
| *Parteien* | 1 | 2 | | 1 | | *4* |
| *DV Gemeinde, Städte, Berggebiete* | | | | | 1 | *1* |
| *DV Wirtschaft* | | 1 | 1 | | 2 | *4* |
| *Weitere* | 1 | 6 | | | 2 | *9* |
| *Nicht Eingel.* | 2 | 8 | 1 | | | *11* |
| **Total** | **11** | **35** | **3** | **1** | **5** | **55** |

| | | |
|---|---|---|
| Legende | **Ja:** | Vorbehaltlose Zustimmung |
| | **Ja, aber:** | Grundsätzliche Zustimmung mit Änderungsanträgen |
| | **Nein, aber:** | Grundsätzliche Ablehnung mit Änderungsanträgen |
| | **Nein:** | Vollumfängliche Ablehnung |
| | **Kein Kom.:** | Ausdrücklicher Verzicht auf eine Stellungnahme |

*Grobübersicht mit Herkunftsangabe*

| **Gesamtwürdigung** | **Anzahl** | **Teilnehmer** |
|---|---|---|
| **Ja:**<br>Vorbehaltlose Zustimmung | **11** | 7 Kantone (SZ, OW, BL, SH, AR, VS, JU)<br>1 in der Bundesversammlung vertretene politische Partei (FDP)<br>1 weitere interessierte Organisation (BGer)<br>2 nicht individuell eingeladene Teilnehmer (CP, CVAM) |
| **Ja, aber:**<br>Grundsätzliche Zustimmung mit Änderungsanträgen | **35** | 17 Kantone (ZH, LU, UR, NW, GL, ZG, FR, SO, BS, AI, SG, GR, AG, TG, TI, VD, NE, GE)<br>2 in der Bundesversammlung vertretene politische Parteien (CVP, SP)<br>1 gesamtschweizerischer Dachverband der Wirtschaft (economiesuisse))<br>6 weitere interessierte Organisation (AB-BA, BA, privatim, SIK, SNB, swico)<br>8 nicht individuell eingeladene Teilnehmer (Clusis, FER, insecor, it-rm, NDB, ETH-Rat, crus.ch, FMH) |
| **Nein, aber:**<br>Grundsätzliche Ablehnung mit Änderungsanträgen | **3** | 1 Kanton (BE)<br>1 gesamtschweizerischer Dachverband der Wirtschaft (SGV)<br>1 nicht individuell eingeladener Teilnehmer (LB) |
| **Nein:**<br>Vollumfängliche Ablehnung | **1** | 1 in der Bundesversammlung vertretene politische Partei (SVP) |
| **Kein Kommentar:**<br>Ausdrücklicher Verzicht auf eine Stellungnahme | **5** | 1 gesamtschweizerischer Dachverband der Gemeinden, Städte und Berggebiete (SSV)<br>2 gesamtschweizerische Dachverbände der Wirtschaft (SAGV, KVS)<br>2 weitere interessierte Organisation (BPatGer, BVGer) |
| **Total** | **55** | |

Kernaussagen der Vernehmlassungen

- Die überwiegende Mehrheit der Vernehmlasserinnen und Vernehmlasser begrüsst die Schaffung eines Informationssicherheitsgesetzes.
- Viele Kantone beantragen, dass die Modalitäten der Anwendung des Gesetzes auf die Kantone und die Zusammenarbeit Bund-Kantone präzisiert werden.
- Einigen Kantonen ist es ein Anliegen, dass sie keine eigenen parallelen Organisationen schaffen müssen, sondern auf jene des Bundes zugreifen können.
- Einige Kantone fordern, bei der Erarbeitung der Ausführungsvorschriften einbezogen zu werden.
- Verschiedentlich wird bemängelt, dass die im Gesetz verwendeten Begriffe zu offen oder unklar seien, was den Behörden ein erhebliches Ermessen geben würde. Es wird daher gefordert, zumindest in den Ausführungsvorschriften für Klärung und Eingengung zu sorgen.
- Vereinzelt wird auf die Schnittstellen zwischen Informationssicherheit, Datenschutz und Öffentlichkeitsprinzip der Verwaltung hingewiesen, die noch besser zu klären seien.

### 3.1 Kantone

ZH begrüsst den Erlass von einheitlichen Vorschriften für den sicheren Umgang mit Informationen durch Bundesbehörden und weitere Organisationen. Der Entwurf erscheine insgesamt als gelungen und konzeptionell gut durchdacht. Die Auswirkungen auf die Kantone seien aber noch unklar und müssten spätestens bei der Umsetzung des Gesetzes und dem Erlass der entsprechenden Ausführungsvorschriften geklärt werden.

BE kann der Vorlage nur unter der Voraussetzung zustimmen, dass die kantonalen und kommunalen Behörden, soweit sie das ISG anwenden (entweder direkt als verpflichtete Behörde oder im Rahmen der Übernahme von Vorschriften des ISG in das kantonale Recht), die vom ISG vorgesehenen zentralen Fachstellen des Bundes ebenfalls beauftragen können, damit sie diese Fachstellen nicht erneut bei sich aufbauen müssen, und dass angemessene Übergangsfristen vorgesehen werden.

LU begrüsst grundsätzlich die Absicht und Stossrichtung des Gesetzesentwurfs. Dieser trage dem gesellschaftlichen und technischen Wandel im Umgang mit Information durch seine Ausrichtung auf eine integrale Informationssicherheit angemessen Rechnung. Im Kapitel 3 (Personensicherheitsüberprüfung) wird jedoch eine gewisse Überreglementierung festgestellt, welche zu einem übermässigen Aufwand bei den Kantonen führe. Desweitern seien die Kosten für die Kantone unklar. Der Vollzug sei so auszugestalten, dass den Kantonen kein grosser Verwaltungsaufwand entstehe.

UR begrüsst grundsätzlich den Entwurf des ISG und die damit zu schaffende Rechtssicherheit im Bereich der Informationssicherheit. Bei den Kosten im Rahmen des Risikomanagement und den erforderlichen Sicherheits- und Schutzmassnahmen sei das nötige Augenmass gefordert. Zudem sei dem Umgang mit klassifizierten Daten und Systemen und die daraus resultierenden Konsequenzen für die Kantone mit ergänzenden, rechtsverbindlichen Ausführungen Rechnung zu tragen. UR erkennt die Wichtigkeit der Personensicherheitsprüfungen an.

SZ befürwortet die Schaffung einer einheitlichen formell-gesetzlichen Grundlage für das Management der Informationssicherheit im Zuständigkeitsbereich des Bundes. Das ISG wird von SZ unterstützt. SZ geht davon aus, dass die Kantone, soweit sie betroffen sein sollten, auch zur Vernehmlassung der Ausführungsbestimmungen zur Stellungnahme eingeladen werden.

OW begrüsst die Ausrichtung des vorliegenden Entwurfs, Informationssicherheit umfassend zu regeln, mit einer für die einzelnen Bereiche angepassten Tiefe. Gemessen am eher klei-

nen Anteil Bundesaufgaben bezogen auf die gesamte Aufgabenerfüllung dürfte sich der Mehraufwand für die Kantone eher im engen Rahmen halten.

Für NW stellt das vorliegende Informationssicherheitsgesetz in erster Linie eine gute und umfassende Umsetzung eines Informationsmanagement Systems (ISMS) nach ISO Standard 2700x dar. Die Kantone seien nur betroffen, soweit sie im unmittelbaren Auftrag und unter Aufsicht des Bundes sicherheitsempfindliche Tätigkeiten ausüben. Es dürfte wohl schwierig werden, einheitliche Kriterien zu schaffen, die den in den verschiedenen Kantonen vorherrschenden Verhältnissen gerecht würden. Falls dieses Gesetz gemäss der Vernehmlassungsfassung in Kraft trete, könnten die für das ISG ausführenden Verordnungen für NW einen massiven operativen Aufwand verursachen. NW geht davon aus, dass die Kantone auch bei der Vernehmlassung zu den entsprechenden Ausführungsbestimmungen wieder begrüsst würden.

Für GL schafft das Informationssicherheitsgesetz Klarheit für die Bundesbehörden. Für die Kantone wäre eine Zusammenfassung ihrer wesentlichsten Aufgaben, Kompetenzen und Verantwortlichkeiten ebenfalls nützlich. Hinsichtlich einzelner Begriffe bestehe zudem noch Konkretisierungsbedarf. Insbesondere fehle es an Klarheit darüber, in welcher Form die einzelnen Kantone genau von Auflagen und von nötigen Ausbildungen betroffen sind.

ZG unterstützt das Bestreben des Bundes, die Informationssicherheit zu verbessern und damit den Anforderungen einer vernetzten Informationsgesellschaft gerecht zu werden. Es sei auch zu begrüssen, dass der Bund eine Vorreiterrolle in der Gesetzgebung in Sachen Informationssicherheit einnehme. Ziel müsse sein, ein möglichst einheitliches Sicherheitsniveau und eine möglichst einheitliche Fachdoktrin zu erreichen. Der vorliegende Gesetzesentwurf scheint dazu grundsätzlich geeignet. ZG stellt aber in Frage, ob die vorgeschlagene «Opting Out»-Regelung zielführend sei, wonach jede Behörden den Erlass in ihrem Bereich selbständig vollzieht und entsprechendes Verordnungsrecht erlasse. Das Gesetz müsse mehr als nur Mindeststandards festlegen, wenn die Informationssicherheit in allen angegliederten Behörden gewährleistet werden soll. Übergreifende Standards und Normen wären diesbezüglich notwendig und wichtig. Auch die Einbindung der Kantone sei daher grundsätzlich sinnvoll. Die Auswirkungen auf die Kantone scheinen im Gesetzesentwurf und im Bericht allerdings zu wenig durchdacht.

FR begrüsst die Absicht des Bundesrates, die in der Informationssicherheit anzuwendenden Standards auf Bundesebene zu vereinheitlichen. FR weist aber darauf hin, dass der Bundesrat noch die anwendbaren Regeln für die Verifizierung der Umsetzung der auf dem ISG basierenden Massnahmen und den Vollzug der Personensicherheitsprüfungen für kantonale Organe festlegen muss. FR wünscht, die Gelegenheit zu erhalten, sich zu den noch zu erstellenden Ausführungsvorschriften äussern zu können.

SO begrüsst es, dass der Bund die Grundsätze der Informationssicherheit in einem Gesetz regle. Die Verantwortung für den sicheren Umgang mit Informationen lasse sich nur dann wahrnehmen, wenn zeitgemässe Instrumente zu deren Schutz bestehen und Lücken des geltenden Rechts geschlossen würden. SO erachtet es auch als wichtig, dass auf Gesetzesstufe klare Regeln für die Personensicherheitsprüfung geschaffen würden, denn die entsprechenden Massnahmen greifen stark in die Persönlichkeitsrechte der Betroffenen ein. In einzelnen Punkten hat SO Änderungsvorschläge.

BS begrüsst grundsätzlich die geplante Regelung. Zu einzelnen Vorhaben hat BS jedoch Änderungsvorschläge oder ergänzende Bemerkungen anzubringen.

BL stimmt dem Gesetzesentwurf zu. Dass Handlungsbedarf im Bereich der Informationssicherheit bestehe, sei allgemein anerkannt. Die vorgesehenen gesetzgeberischen Massnahmen trügen zur Erhöhung der Informationssicherheit bei, weshalb BL sie befürworte. Aus der Unterstellung unter das neue Gesetz dürfen den Kantonen aber keine Kosten entstehen, da solche im erläuternden Bericht nicht ausgewiesen würden.

SH erklärt sich mit der Vorlage einverstanden.

AI ist mit dem neuen Gesetz unter Vorbehalt dreier Punkte (volle Entschädigung der Aufwendungen der Kantone durch den Bund, unentgeltlicher Zugriff der Kantone auf die Fach-

stellen des Bundes, Vorlage der Bundesratsverordnungen zur Stellungnahme) einverstanden.

AR begrüsst die Vorlage, auch wenn die Kantone bzw. einzelne kantonale Ämter nur am Rande von der bundesgesetzlichen Regelung tangiert würden. Auf eine detaillierte Stellungnahme könne unter diesen Gegebenheiten verzichtet werden.

SG beschränkt seine Stellungnahme auf das Kapitel Personensicherheitsprüfungen, da nur diese Bestimmungen den Kanton unmittelbar betreffen. SG hat keine grundsätzlichen Einwände gegen die neuen Bestimmungen.

GR begrüsst im Grundsatz die Schaffung eines Bundesgesetzes über die Informationssicherheit. Die Schnittstellen zwischen Bund und Kantonen seien aber noch nicht genügend klar. Zudem müsse den Kantonen die Möglichkeit eingeräumt werden, die gemäss ISG zu schaffenden zentralen Fachstellen des Bundes zu beauftragen. Für die Umsetzung des Gesetzes seien, angepasst an den Lebenszyklus von ICT-Systemen angemessene Übergangsfristen von mindestens fünf bis zehn Jahren vorzusehen.

AG befürwortet grundsätzlich den Erlass des ISG, fordert aber, dass im Rahmen des Gesetzesverfahrens noch die offenen Fragen betreffend Personensicherheitsprüfung kantonaler Angestellter, Aufsichtsverfahren durch den Bund sowie Schnittstellen des Informationssicherheitsrechts mit der Datenschutzaufsicht der Kantone geklärt und in der Botschaft erläutert werden.

Für TG kann ein gutes Informationssicherheitsgesetz datenschutzrechtlich von grosser Wichtigkeit sein. Ein solches Gesetz könne jedoch bei zu strikter Ausformulierung auch diverse Gefahren für die Persönlichkeitsrechte der Betroffenen in sich bergen.

TI begrüsst die Absicht und die Stossrichtung der Gesetzesrevision. Der Hauptzweck des Gesetzesentwurfs sei die Konsolidierung und Koordination von bereits Bestehendem. Dadurch werde es möglich, zukünftige Bedrohungen im Zusammenhang mit der laufenden Verbreitung von IKT-Systemen, mit der Auslagerung von Daten und ihrer zunehmenden Vernetzung entsprechend im Voraus richtig einzuschätzen. Daher hätten klare gesetzliche Grundlagen mit einer hohen Regelungsdichte auf Gesetzesstufe in jenem Bereich ihre besondere Berechtigung, wo teilweise schwerwiegende Eingriffe in die Grundrechte stattfinden, welche die persönliche Freiheit, die Persönlichkeit und Privatsphäre der Bürger schützen.

VD hat, angesichts der sich diversifizierenden und zunehmenden Risiken, keine grundsätzlichen Vorbehalte gegen das Projekt, das beabsichtigt, die gesetzlichen Grundlagen der Informationssicherheit im Bund unter Beachtung der bestehenden Regeln zum Datenschutz zu vereinheitlichen. VD nimmt Kenntnis von der Analyse, wonach die Auswirkungen auf die Kantone minimal sein werden, in dem die Kantone nur betroffen sein werden, soweit sie sensible Aufgaben im Auftrag und unter Aufsicht des Bundes vollziehen. Trotzdem kann VD nicht ausschliessen, dass die Auswirkungen auf die personellen Ressourcen und auf die Finanzen gewichtiger ausfallen könnten als vorgesehen. Dieser Punkt müsse bei der Ausarbeitung der Vollzugsvorschriften noch vertieft abgeklärt werden. VD wünscht insbesondere, dass diesbezüglich die kantonalen Polizei- und Nachrichtendienste, die aktuell verpflichtet sind, die Personensicherheitsprüfungen durchzuführen, berechtigt sind und bleiben, die für die Aufgabenerfüllung notwendigen Daten zu bearbeiten.

VS begrüsst das Gesetzesprojekt, dessen Ziel die Schaffung einheitlicher gesetzlicher Grundlagen für die Informationssicherheit auf Stufe Bund ist. VS versteht auch, dass der Bundesrat die Kontrolle der Umsetzung der Massnahmen und die Personensicherheitsprüfung kantonaler Angestellter in den Ausführungsvorschriften regeln muss. VS wünscht, dass die kompetenten Stellen des Kantons Wallis in diese Arbeiten von Anfang an aktiv integriert werden.

NE unterstützt die Absicht des Bundesrates, seiner Informationssicherheitspolitik einen umfassenden Rahmen zu geben. Das vorgeschlagene Gesetz gehe in die richtige Richtung und reagiere gewiss auf die Vorarbeiten im Bund, ohne sich zu stark auf die Kantone auszudehnen. Trotzdem muss die Informationssicherheit, wie alle Sicherheitsprobleme, gemeinsam mit den kantonalen und kommunalen Partnern betrachtet werden. NE wünscht daher, dass

im neuen Gesetz ein Koordinationsorgan zwischen Bund und Kantonen vorgesehen wird, um einen gemeinsame Politik in Sachen Sicherung der Kommunikationsinfrastrukturen und Abwehr der Cyberkriminalität verfolgen zu können.

GE begrüsst grundsätzlich die Initiative, die Informationssicherheit auf Bundesebene zu stärken. Das Gesetz ist komplett und berücksichtigt alle notwendigen Parameter. GE ist daher für dieses Gesetzesprojekt, dass nur geringe Auswirkungen auf die kantonale Verwaltung haben dürfte.

JU begrüsst das Gesetzesprojekt im Bewusstsein der Notwendigkeit die Rechtsgrundlagen an die Entwicklung im Informatikbereich und die damit verbundenen Risiken anzupassen. Der Entwurf enthalte die grundlegenden Elemente einer Sicherheitspolitik, die der Schweiz erlaube, die Risiken des Informatikbereiches umfassend zu begrenzen. Es ist daher weder formell noch im Grundsatz auf etwas hinzuweisen. Die vorliegenden rechtlichen Grundlagen betonen das Risikomanagement als Mittel zur Sicherheitsverbesserung und führen klarerweise zu einem Fortschritt in Sachen Sicherheitsniveau auf nationaler Ebene. JU unterstützt das Projekt vollumfänglich.

### 3.2 In der Bundesversammlung vertretene politische Parteien

Die CVP befürwortet grundsätzlich die Schaffung eines Bundesgesetzes über die Informationssicherheit. In unserer vernetzten Gesellschaft werde der Schutz von Informationen immer wichtiger. Die Entwicklung zu einer Informationsgesellschaft biete denn auch nicht nur Chancen sondern auch Risiken. Die CVP spricht sich aus diesen Gründen für eine einheitliche gesetzliche Grundlage für das Management und die Organisation der Informationssicherheit für die verpflichteten Behörden aus. Die CVP verlangt aber vom Bundesrat, dass er in seiner Botschaft aufzeigt, wo es Schnittstellen zu bereits bestehenden Systemen und zwischen Institutionen und Privaten ausserhalb der Bundesverwaltung gibt.

Die FDP unterstützt grundsätzlich das Gesetz, das die Sicherheit unseres Landes verbessern will. Die FDP ist für das im Gesetz ausgedrückte generelle Prinzip, ein angemessenes Sicherheitsniveau bei der Verwendung von Informatikmitteln zu definieren, die für die Arbeit der Bundesbehörden immer unerlässlicher werden. Bei der Verwendung von Informatikmitteln ist ein Risikomanagement in allen Bereichen der Bundesverwaltung unerlässlich für die Weiterentwicklung der Informationsgesellschaft. Das vorliegende Gesetz ist daher notwendig, um einerseits die technischen Lücken in unserem System des Informationsschutzes als auch die organisatorischen Lücken zu füllen. Deshalb spricht sich die FDP für die Zusammenfassung aller Massnahmen der Informationssicherheit in einer einzigen, homogenen Regelung aus, die für alle Bundesbehörden und deren Unterstellten gilt. Für die FDP ist es wichtig, ein Gleichgewicht zwischen dem Sicherheitsniveau und den Kosten dafür zu finden, um eine Kostenexplosion zu vermeiden.

Aus Sicht der SVP ist die Vorlage abzulehnen. Massgebende Mehrwerte würden mit einem Bundesgesetz über die Informationssicherheit nicht geschaffen. Es führe vielmehr zu mehr Bürokratie und könne zu einer einheitlichen Anwendung der Bestimmungen nur beschränkt beitragen. Der Entwurf lasse den jeweiligen Bundesbehörden im Rahmen ihrer Unabhängigkeit und Organisationsautonomie beim Vollzug viel Raum. In diesem Sinne sei es vorteilhafter, das derzeitige System beizubehalten und allenfalls gezielte Verbesserungen im Rahmen der bestehenden Strukturen anzubringen.

Die SP begrüsst die Absicht und Stossrichtung des Gesetzesentwurfs. 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 angemessen Rechnung. Insgesamt bilde das neue ISG eine gute Grundlage für eine moderne, professionelle und umfassende Organisation des Informationsschutzes. Ob das Ziel am Ende erreicht werde, 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 blieben und auch die Sicherheitseinstufung von IKT-Mitteln so gehandhabt werde, dass das betroffene (Staats-)Personal seine Aufgaben weiterhin einfach und benutzerfreundlich erfüllen könne. Die SP fordert zudem an verschiedenen Stellen des Gesetzes, den Datenschutz zu stärken und die Einhaltung der Archivierungspflicht sicherzustellen.

### 3.3 Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete

Der Schweizerische Städteverband (SSV) verzichtet ausdrücklich auf eine Vernehmlassung, verweist jedoch auf die Stellungnahme der Schweizerischen Informatikkonferenz.

### 3.4 Gesamtschweizerische Dachverbände der Wirtschaft

Economiesuisse begrüsst das mit der Gesetzesvorlage verfolgte Vorhaben, das Informationsmanagement der Bundesbehörden an die Anforderungen der vernetzten modernen Informationsgesellschaft anzupassen. Das vorgeschlagene Gesetz zur Schaffung einer einheitlichen formell-gesetzlichen Grundlage zum Schutz von Informationen und zur Sicherheit beim Einsatz von IKT-Mitteln werde daher insgesamt begrüsst. Für Unternehmen sei es wichtig, dass bei der Bearbeitung von sensiblen Informationen durch die Bundesbehörden die Vertraulichkeit gewährleistet sei. Allerdings enthalte der vorliegende Entwurf zahlreiche unbestimmte und zu weit gefasste Begriffe. Economiesuisse fordert daher, dass der Ermessenspielraum in der noch zu erlassenden Verordnung durch genauere Begriffsbestimmungen und klare Beurteilungskriterien begrenzt werde.

Der SGV lehnt den vorliegenden Entwurf ab, da das Gesetz einen irreführenden Titel habe und die Qualität der erläuternden Materialien mangelhaft sei. Mit einer markanten Verbesserung des erläuternden Berichts sowie der Präzisierung der Benennung des Gesetzes wäre der SGV mit dem materiellen Gesetzesentwurf einverstanden. Gleichzeitig verweist der SGV in seiner Stellungnahme auf eine beigelegte Stellungnahme des Chambre vaudoise des arts et métiers (FPV), welche den Gesetzesentwurf ausdrücklich unterstützt.

Der SAGV und der KVS verzichteten aufgrund fehlender Betroffenheit ausdrücklich auf eine Stellungnahme.

### 3.5 Weitere interessierte Organisationen

AB-BA nimmt zur Kenntnis, dass die Aufsichtsbehörde, welche gemäss Artikel 2 Buchstabe d als verpflichtete Behörde aufgeführt sei, nach Artikel 87 Absatz 1 ihre eigenen Ausführungsbestimmungen erlassen könne. Damit entfielen einige der Vorbehalte, welche die Behörde in der Ämterkonsultation vom 2. April 2013 angebracht habe. Noch unklar sei, mit Bezug auf die Aufsichtsbehörde bzw. die Bundesanwaltschaft, bei welcher Behörde eine Verfügung der Prüfstelle angefochten werden könne und ob bei Personen, die derzeit nicht personensicherheitsüberprüft sind, dies aber nach den neuen Bestimmungen wohl sein müssten, nachträglich eine Personensicherheitsprüfung stattzufinden habe.

Die BA sieht sich, was den Umgang und den Schutz von Informationen aus Strafverfahren betrifft, primär den Vorgaben der StPO verpflichtet. Diese regele insbesondere den Zugang zu Informationen aus Strafverfahren umfassend. Die Vorgaben des ISG werden von der BA bereits im Rahmen der Umsetzung des Projekts Integrale Sicherheit berücksichtigt. Im Übrigen verweist die BA auf ihre Stellungnahme vom 12. April 2013 (Klassifizierung von Akten/Informationen aus Strafverfahren, Sicherheitseinstufung von IKT-Mitteln).

Privatim kann die Schaffung eines Bundesgesetzes über die Informationssicherheit aus zweierlei Überlegungen grundsätzlich begrüssen: Der Informationssicherheit werde endlich jene Rolle verliehen, welche sie im Verwaltungsalltag und in der Gesellschaft längst hätte einnehmen sollen und die Durchführung der Personensicherheitsprüfungen (PSP) werde in einer dafür notwendigen formell-gesetzlichen Grundlage geregelt. Der Entwurf zum ISG sowie der erläuternde Bericht würden jedoch aus datenschutz- und informationsrechtlicher

Sicht diverse Fragen aufwerfen, welche es zwingend zu diskutieren bzw. zu klären und zu verbessern gelte.

Die SIK begrüsst jegliche Verbesserungen und Zusammenarbeit im Bereich Informationssicherheit zwischen den föderalen Ebenen Bund, Kantone und Gemeinden. Aufgrund der knappen Ressourcen der Fachstelle der SIK beschränkt sich die SIK bei ihrer Stellungnahme auf die kantonsrelevanten Themen. Die SIK kann der Vorlage nur unter der Voraussetzung zustimmen, dass die kantonalen und kommunalen Behörden, soweit sie das ISG anwenden, die vom ISG vorgesehenen zentralen Fachstellen des Bundes, namentlich die Fachstellen Personensicherheitsprüfung (PSP) oder das Betriebssicherheitsverfahren (BS), ebenfalls beauftragen können, damit sie diese Fachstellen nicht erneut bei sich aufbauen müssen, und dass angemessene Übergangsfristen vorgesehen werden. Ansonsten wären die Kantone vom Geltungsbereich des ISG auszunehmen. Die SIK erwartet, dass die Kantone bzw. ihre Fachbehörden bei der Erarbeitung der Ausführungsbestimmungen des Bundes eng mit einbezogen werden, insbesondere soweit die Ausführungsbestimmungen auch die Kantone betreffen.

Die SNB begrüsst grundsätzlich die Stossrichtung des Gesetzesentwurfs zum Schutz der Landesinteressen und insbesondere der wirtschafts-, geld- und währungspolitischen Interessen der Schweiz. Der Gesetzesentwurf nehme sich der Herausforderung an, eine gemeinsame Basis für die Informationssicherheit einerseits für Behörden und andererseits für Organisationen zu schaffen. Dabei erweise sich die Verpflichtung der Behörden gemäss Artikel 2 Absatz 1 des Gesetzesentwurfs als anspruchsvoll, da diese in ihrer Tätigkeit grundsätzlich keiner unmittelbaren Weisungsbefugnis einer anderen Behörde unterstehen. Der Grundsatz, wonach die verfassungsmässige Autonomie der erfassten Behörden nicht angetastet werde, sei im Gesetzesentwurf nicht mit letzter Konsequenz eingehalten. Die SNB legt Wert darauf, dass die Anordnungen des Gesetzesentwurfes mit der verfassungsmässig gewährleisteten Unabhängigkeit der Nationalbank (Artikel 99 Absatz 2 der Bundesverfassung) vereinbar ist.

Das BGer macht darauf aufmerksam, dass einige Artikel für das BGer wesentlich seien und deshalb nicht zu seinem Nachteil verändert werden dürften. Ansonsten verzichtet das BGer auf eine Stellungnahme.

Das BPatGer verzichtet nach Durchsicht der Unterlagen auf eine Stellungnahme.

Das BVGer verzichtet ausdrücklich auf eine Stellungnahme und betont, dass dies als Enthaltung und nicht als Zustimmung zur Vorlage zu werten sei.

Swico befürwortet die im vorliegenden Gesetzesentwurf vorgesehene Anpassung der Rechtsgrundlagen an die moderne vernetzte Informationsgesellschaft. Der vorliegende Gesetzesentwurf sei jedoch in seiner Begrifflichkeit mehrheitlich zu unbestimmt und weit gefasst, was auch einen zu weiten Ermessensspielraum zur Folge habe. Daher fordert swico, dass die Umsetzung in den entsprechenden Verordnungsbestimmungen konkret und mit klaren Begriffsbestimmungen erfolge.

### 3.6 Nicht individuell eingeladene Teilnehmer

Clusis äussert sich zu einigen spezifischen Artikeln, ohne eine explizite Gesamtwürdigung der Vorlage abzugeben.

CP und CVAM können das Projekt für ein Informationssicherheitsgesetz unterstützen. Im besten Fall ermöglicht dieses Organisationsgesetz dem Bund klare und homogene gesetzliche Grundlagen in der Sache festzulegen, auch wenn er damit das Sicherheitsniveau konkret nur gering steigern kann. Zudem ist das Betriebssicherheitsverfahren dazu geeignet, die Wettbewerbsfähigkeit der Unternehmen zu steigern.

Die FER macht lediglich zu vier Artikeln und einem Abschnitt Bemerkungen, ohne eine explizite Gesamtwürdigung der Vorlage abzugeben.

Insecor begrüsst die einheitliche Regelung der Informationssicherheit sowie deren Regelung auf Gesetzesstufe sehr. Mit dem neuen ISG werde eine dringend benötigte Lücke in der Gesetzeslandschaft der Informationssicherheit bzw. der Sicherheit von Informations- und Kom-

munikationstechnologien geschlossen, welche nicht nur für die Bundesverwaltung oder die kantonalen Behörden von grosser Bedeutung sein werde, sondern auch für die Privatwirtschaft wichtige Anhaltspunkte geben könne. Insecor heisst die Gesetzesvorlage grundsätzlich gut, bringt dazu aber einige Überlegungen und Anregungen ein.

Die it-rm begrüsst es sehr, dass ein Gesetzesentwurf dem Parlament vorgelegt werden soll, welcher den Schutz von Informationen in der Bundesverwaltung und der ihr nahe gelegenen Behörden regle. Der Gesetzesentwurf messe aber der Vertraulichkeit der Informationen (wie z.B. bei der Klassifizierung Artikel 14) einen zu hohen Stellenwert bei, womit der Schutz anderer, d.h. nicht vertraulicher Informationen eine untergeordnete Rolle spiele. Für das Funktionieren einer modernen, mit IKT-Mitteln ausgestatteten Gesellschaft und Verwaltung und für die Wahrung der wirtschafts- und finanzpolitischen Interessen eines Staates bedürfe es nicht nur des besonderen Schutzes vertraulicher Informationen, sondern auch derjenigen Informationen, worauf sich alle Bürger und Beamte verlassen können müssten, wie Informationen aus einem Register oder aus einem Archiv.

LB hat den Eindruck, dass der im ISG vorgesehene umfassende Ansatz zur Gewährleistung der Informationssicherheit für alle Anwendungen bei den verpflichteten Behörden des Bundes und der Kantone sowie bei den mit Aufgaben der Verwaltung betrauten privaten Organisationen dem Zweck des ISG nicht gerecht wird. Es sollte angestrebt und ein Weg gefunden werden, dass sich die Anwendung des ISG auf jene Anwendungen beschränkte, welche für die Wahrnehmungen der Interessen unseres Landes, seiner Gesellschaft und Wirtschaft entscheidend seien. Unter diesem Aspekt erscheine das ISG mit seinen 94 über 30 Seiten ausgebreiteten Artikeln als gesetzgeberisches Monstrum ohne bekannte vergleichbare ausländischen Regelungen, mit vielen unbestimmten Rechtsbegriffen und zahlreichen offenen Fragen, dessen Umsetzung in Bereichen, welche für das Gesamtinteresse des Landes nicht entscheidend sein dürften, einen sehr hohen Aufwand erfordern wird. Es sollte somit angestrebt werden, den Anwendungsbereich des ISG auf existentielle Bedrohungen der in Artikel 1 Absatz 2 ISG umschriebenen Schlüsselbereiche für den Umgangs mit lebenswichtigen Informationen und die in diesem Bereich eingesetzten IKT -Mitteln auszurichten und dadurch ein optimiertes Verhältnis von Aufwand und Nutzen der Informationssicherheit zu erreichen. Man sollte sich auch überlegen, das ISG von zahlreichen Detailvorschriften, von denen viele Selbstverständlichkeiten im Bereich der Informationssicherheit wiedergeben, zu entschlacken, weil diese eigentlich auf die Stufe von Verordnung, Empfehlungen, Weisungen oder Checklisten gehörten.

Der NDB weist auf einige Artikel hin, die inhaltlich angepasst werden müssten. Ansonsten äussert sich der NDB nicht zur Vorlage.

Der ETH-Rat unterstützt den vorliegenden Entwurf grundsätzlich und begrüsst vor allem die Vereinheitlichung der Vorgaben für den ganzen Bundesbereich. Allerdings wird betont, dass die Forschung, auch innerhalb des Bundesbereiches, eine spezielle Position einnehme, da sie angewiesen sei auf einen möglichst offenen Austausch und reibungslose nationale und internationale Zusammenarbeit. Der ETH-Rat würde es daher begrüssen, wenn in der Verordnung zum ISG auf diese Aspekte weitmöglichst eingegangen würde, allenfalls mit entsprechenden Ausnahmeregelungen für den Bereich der Forschung. Ansonsten könnte der Forschungsplatz Schweiz in seiner heutigen Form gefährdet sein. Zusammenfassend sei festzustellen, dass der Gesetzesentwurf noch zu wenig konsistent bzw. zu wenig durchdacht erscheine und zahlreiche Rechtsunsicherheiten bestünden bzw. zu viel Interpretationsspielraum offen gelassen werde.

CRUS ist der Wichtigkeit der Informationssicherheit bewusst. Der Entwurf des Informationssicherheitsgesetzes soll jedoch nur auf die in Artikel 2 des Gesetzes genannten Instanzen anwendbar sein. Die Universitäten sollten nur soweit betroffen sein, als sie mit Aufträgen einer dieser Instanzen betraut sind. Die Sicherheitsmassnahmen, die mit solchen Aufträgen einhergehen müssen, hängen von den Vorgaben des Auftragsgebers ab. Für CRUS ist es wichtig, dass der Auftraggeber die Kosten, die durch die auferlegten Sicherheitsmassnahmen entstehen, übernimmt. Die Sicherheitsmassnahmen dürfen zudem nicht dazu führen, dass die wissenschaftlichen Resultate nicht publiziert werden können.

Die FMH begrüsst die Stossrichtung des Gesetzesentwurfs, für alle Bundesbehörden einheitliche gesetzliche Grundlagen zur "Informationssicherheit" im Sinne von "sämtliche Anforderungen und Massnahmen, die zum Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen dienen, und zwar unabhängig davon, ob die Informationen elektronisch, mündlich oder in Papierform bearbeitet werden" zu schaffen. Aus ihrer Sicht ist es jedoch wichtig, insbesondere Personendaten im in den Erläuterungen beschriebenen umfassenden Sinne der Informationssicherheit zu schützen.

## 4 Stellungnahmen zum allgemeinen Teil des erläuternden Berichts

Im Folgenden werden die Stellungnahmen zu den einzelnen Themen des allgemeinen Teils des erläuternden Berichts dargelegt. Es werden nur die Themen des allgemeinen Teils des erläuternden Berichts angeführt, zu denen explizit oder implizit Stellung genommen wurde.

### 4.1 Risiken der Informationsgesellschaft

Die SP teilt die im allgemeinen Teil des erläuternden Berichtes vorgenommene Analyse der Chancen und Risiken der Informationsgesellschaft; namentlich die Aussage, dass die Bekämpfung der Risiken nicht dazu führen darf, die Chancen der Informationsgesellschaft zu schmälern. Unannehmbar wäre für die SP, wenn die Schweiz in das von einigen Grossmächten inszenierte digitale Wettrüsten einsteigen würde. Gefragt seien vielmehr vertrauensbildende Massnahmen durch grösstmögliche Transparenz und internationale Zusammenarbeit. 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 bestünden aber grosse Lücken.

### 4.2 Heutige Organisation der Informationssicherheit in der Bundesverwaltung

SO bemerkt, dass in den Erläuterungen auf Seite 28 in Ziffer 1.3.1.2 die Organisation des Datenschutzes erläutert werde, ohne dass die Zuständigkeiten der kantonalen Datenschutzbeauftragten erklärt würden. Diese seien für die Datenschutzaufsicht von kantonalen Behörden zuständig, und zwar auch dann, wenn die kantonalen Behörden Bundesaufgaben vollziehen. Es sollte deshalb verdeutlicht werden, dass sich für die Zuständigkeit der Datenschutzaufsicht keine Änderungen ergäben und die kantonalen Behörden, die im Auftrag des Bundes sicherheitsempfindliche Tätigkeiten ausübten, unter der Aufsicht der kantonalen Datenschutzbeauftragten verbleiben würden.

Privatim verlangt in der Botschaft in Ziffer 1.3.1.2 zu verdeutlichen dass die Datenschutzaufsicht über die kantonalen Behörden, die im Auftrag des Bundes sicherheitsempfindliche Tätigkeiten ausüben, bei den kantonalen Datenschutzbeauftragten bleibe. Kantonale öffentliche Organe würden beim Vollzug von Bundesaufgaben nicht zu Bundesorganen und blieben deshalb dem kantonalen (Informations- und) Datenschutzgesetz und der kantonalen Datenschutzaufsicht unterstellt.

## 5 Stellungnahmen zu den Gesetzesentwürfen und deren Erläuterungen

Im Folgenden werden die Stellungnahmen dargelegt, die sich spezifisch zu einzelnen Artikeln der Gesetzesentwürfe oder dessen Erläuterungen äussern. Es werden nur die Artikel angeführt, zu denen explizit oder implizit Stellung genommen wurde.

## 5.1 Bundesgesetz über die Informationssicherheit

### Allgemein

NW weist darauf hin, dass im Bundesgesetz grundlegend der Begriff Informationssicherheit verwendet werde. Dies sei in der Gesetzgebung von NW noch nicht der Fall. Es werde wohl schwierig sein, einheitliche Kriterien zu schaffen, die den in den verschiedenen Kantonen vorherrschenden Verhältnissen gerecht würden. Als Beispiel dazu sei einerseits die Definition von „sicherheitsempfindlichen Tätigkeiten" nach Artikel 2 Absatz 3 ISG, und andererseits die Klassifizierung von Daten bzw. Informationen (z.B. als „geheim", „vertraulich" oder „intern") zu nennen.

SO bemerkt, dass weder der Entwurf des ISG noch die Erläuterungen auf den Lifecycle der Dokumente bzw. Informationen eingingen. Es wäre jedoch wichtig zu regeln, in welchem Verhältnis die einzelnen Bestimmungen des ISG bei der Entstehung, Nutzung, Speicherung, Archivierung und Entsorgung stünden.

Der SGV weist auf die mangelnde Qualität der erläuternden Materialien hin. Sätze wie „Information ist die Währung der Informationsgesellschaft (S. 1)“ oder „Die Welt erlebt seit einigen Jahrzehnten einen fundamentalen gesellschaftlichen Wandel (S. 9)“ seien lediglich Worthülsen, die keinerlei Erklärungsgehalt hätten. Selbst wenn sie substantielle Aussagen wären, wären sie sachlich falsch und werden zusammenhangslos oder unreflektiert in den Materialien angeführt. Die mangelnde Qualität zeige sich auch in den verwendeten Denkmodellen. Ein besonders deutliches Beispiel einer simplizistischen Vorstellung finde sich auf S. 77 „Einerseits wird ihr Vertrauen [das Vertrauen der Gesellschaft] in die sichere Bearbeitung von Informationen durch Bundesbehörden erhöht.“ Es sei erstaunlich, welch billiger Kausalismus in dieser Aussage enthalten sei. Selbst die empirische Überprüfung dieser Aussage scheine so offensichtlich unplausibel, dass es nicht erklärbar sei, wie sie getroffen, geschweige denn publiziert, werden konnte.

Der vorliegende Gesetzesentwurf enthält nach Ansicht der swico etliche unbestimmte und weit auslegbare Begriffe und Bestimmungen (z.B. sicherheitsempfindliche Tätigkeiten, sicherheitsempfindliche Bereiche etc.). Die swico fordert, dass in der noch zu erlassenden Verordnung der Ermessensspielraum klar begrenzt und klare Kriterien und Begriffsbestimmungen festgelegt würden, um der Gefahr einer Ungleichbehandlung und Wettbewerbsverzerrung zu begegnen.

Insecor bemerkt, dass einige wesentliche Inhalte lediglich im Erläuternden Bericht enthalten, im Gesetzesentwurf hingegen nicht zu finden seien. Dies betreffe beispielsweise eine Reihe von Begriffen. Es sei durchgehend zu prüfen, welche Inhalte des Erläuternden Berichts zum besseren Verständnis des Vorhabens in den Gesetzestext aufgenommen werden sollten und welche nicht.

### Titel

Der SGV weist auf den verwirrenden Titel des Gesetzes hin. Aus seinem Zweckartikel sowie aus dem erläuternden Bericht werde deutlich, dass das ISG an Behörden und ähnliche Stellen adressiert sei, und dass damit insbesondere nicht ein gesamtgesellschaftliches Regelwerk zu Information und Informationssicherheit aufgestellt werde. Dies sollte aber auch schon aus dem Titel zu entnehmen sein, beispielsweise durch seine Ergänzung: „Bundesgesetz über die Informationssicherheit in Bundesbehörden und ähnlichen Organisationen“.

### 1. Kapitel: Allgemeine Bestimmungen

### Allgemein

BS schlägt vor, zur Förderung eines einheitlichen Verständnisses die Begriffe Informationssicherheit und deren drei Bereiche Informationsschutz, Datenschutz und Informatiksicherheit einleitend zu definieren.

Für privatim gehen weder der ISG noch die Erläuterungen auf den LifeCycle der Dokumente bzw. Informationen, welche es zu schützen gelte, ein. Wie verhalten sich die Klassifizierungen mit den Stadien der Entstehung, Nutzung, Speicherung, bis hin zur Entsorgung der Dokumente bzw. Informationen? Dieses Thema müsse zwingend aufgegriffen und, wenn nicht im Gesetz selbst geregelt, so zumindest in der Botschaft erörtert werden.

Insecor regt an, die einleitenden Artikel des ISG wie folgt zu benennen (als Begründung vergleiche auch nachstehend die Anmerkungen zu den Artikeln 2 und 3 ISG) und die wichtigsten Begriffe der Informationssicherheit und Klassifizierung bereits im vorliegenden Gesetz zu definieren: Artikel 1 Zweck (oder „Gegenstand"), Artikel 2 Geltungsbereich, Artikel 3 Begriffe. In der Praxis führten gerade die fehlenden Legaldefinitionen im Bereich der Informationssicherheit immer wieder zu grossen Unklarheiten und entsprechenden Diskussionen. Bei Rechtsgrundlagen für eher komplexe Themen sei es von grosser Bedeutung, entsprechende Klarheit bereits auf Bundesgesetzesstufe zu schaffen.

Der ETH-Rat bedauert den kompletten Wegfall des früheren Artikels 5 ISG Version 2013, der Begriffsdefinitionen enthielt. Durch den Wegfall einer Definition der relevanten Begriffe im ISG lasse sich nicht mehr selbsterklärend verstehen, was z.B. alles als IKT-Mittel zu verstehen sei. Der ETH-Rat schlägt vor, den Definitionskatalog besagter Begriffe an passender Stelle wieder aufzunehmen, sei es im ISG selber oder zwecks einfacherer Ergänzung bzw. Korrektur der Begriffe bevorzugt in der entsprechenden Verordnung zum ISG.

**Artikel 1** Zweck

Aufgrund der vorgesehenen «Opting-out»-Regelung (Artikel 87 Absatz 3 ISG), wonach jede der verpflichteten Behörden eigenes Verordnungsrecht erlassen kann und die vom Bundesrat festgelegten Standardanforderungen und -Massnahmen nur Empfehlungscharakter haben, sieht ZH die Gefahr, dass die teilweise sehr offenen Begriffe unterschiedlich ausgelegt und in den Ausführungsbestimmungen der verschiedenen Behörden unterschiedlich geregelt werden. ZH ist deshalb der Ansicht, dass das an sich sehr detaillierte Gesetz zumindest in Bezug auf die in Artikel 1 Absatz 2 ISG definierten, zu schützenden öffentlichen Interessen und die vorgesehenen Klassifizierungsstufen näher spezifiziert werden sollte.

TI hält fest fest, dass die Liste der Zweckbestimmungen der gesetzlichen Regelung zu einschränkend sei, und zwar insofern, als sie sich ausdrücklich nur auf den Schutz der öffentlichen Interessen beziehen würde (insbesondere des Bundes) und private Interessen nur indirekt einbeziehe. Der Anspruch, die Rechte der Persönlichkeit und der Privatsphäre (und somit der Personendaten) sowie das Berufs-, Geschäfts- und Fabrikationsgeheimnis zu schützen, sollte nicht nur implizit auf die Bestimmung (Bst. e) begrenzt werden. Denn so würde schlussendlich das Vertrauen in jene Stellen gestärkt, welche diese Art von Informationen aufgrund des Spezialrechts bearbeiten. Für TI, sollte auf diese Elemente ausdrücklich hingewiesen werden, wenn auch nur beispielhaft, indem man den entsprechenden Buchstaben der Regelung anpasse. Ebenso und in diesem Masse sollte im Einführungssatz von Abs. 2 auch der Schutz der privaten Interessen (und nicht nur der öffentlichen) hinzugefügt werden.

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 sei, könne unterstützt werden. Es ergebe sich von selbst, dass dieser Begriff implizit auch (elektronische) Daten aller Art einschliesse. Auch der Versuch in Absatz 2, die zu schützenden „öffentlichen Interessen" zu benennen, sei nachvollziehbar. Die gewählten Begriffe seien freilich von einem derart hohen Abstraktionsgrad, dass sie einen äusserst breiten Interpretationsraum offen liessen. Dies berge das Risiko für exzessive Interpretationen. Dieses Risiko sei umso höher einzustufen, als Artikel 1 Absatz 2 Buchstaben a-d weiter hinten im Gesetz als Grundlage herangezogen wird, um die Klassifizierungsstufen (Artikel 14 ISG) und die Sicherheitseinstufung von IKT-Mitteln (Artikel 21 ISG) zu bestimmen. Es sei zu begrüssen, dass der erläuternde Bericht einschränkende Definitionen der zu schützenden „öffentlichen Interessen" enthalte. Diese Einschränkung gehe allerdings nicht aus dem Wortlaut von Artikel 1 Absatz 2 Buchstabe d ISG hervor. Die SP regt

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

Privatim bedauert, dass sich der vorgeschlagene Artikel 1 ISG nur auf die Wahrung der Eigeninteressen des Bundes beziehe und die Wahrung der Interessen der Bevölkerung nur indirekt einbezogen werde. Die Wahrung der verfassungsmässig garantierten Persönlichkeitsrechte (Artikel 10 Absatz 2 und Artikel 13 Absatz 2 BV) oder von Berufs-, Geschäfts- und Fabrikationsgeheimnisse würden nur insofern vom Gesetzeszweck miterfasst, als allfällige Mängel bei der Informationssicherheit zu einem Vertrauensverlust beim Bund führten (vgl. Erläuternder Bericht zu Art. 1 Abs. 2 Bst. d ISG). Nach Ansicht von privatim müssen durch die Informationssicherheit auch die Interessen der direkten Betroffenen selbst geschützt werden, über welche die Behörden Daten bearbeiten. Privatim schlägt daher vor, Artikel 1 Absatz 2 E- ISG wie folgt anzupassen:

[2] Es soll damit die folgenden öffentlichen und privaten Interessen schützen:

a) die Entscheidungs- und Handlungsfähigkeit der Bundesbehörde
b) die innere und äussere Sicherheit der Schweiz
c) die aussenpolitischen Interessen der Schweiz
d) die wirtschafts-, finanz- und währungspolitischen Interessen der Schweiz
e) die verfassungsmässigen Grundrechte der betroffenen Personen
f) die Berufs-, Geschäfts- und Fabrikationsgeheimnisse
g) die Erfüllung weiterer gesetzlicher und vertraglicher Verpflichtungen der Bundesbehörden zum Schutz von Informationen.

Angesichts des hohen Stellenwertes des Datenschutzes und des Schutzes der Privatsphäre in der Schweiz, scheint es FER angezeigt, einen weiteren Punkt in den Absatz 2 dieses Artikels aufzunehmen: «Die Klassifizierung von Personendaten oder Persönlichkeitsprofilen, die im Rahmen des Schutzes der unten beschriebenen Interessen erhoben wurden.» Damit soll betont werden, dass die vom Bund gesammelten Daten behandelt werden, als wenn sie in der Kategorie «sehr hoher Schutz» klassifiziert wären, sei es für die gesammelten Daten (im Rahmen der Personensicherheitsprüfung) oder für alle anderen Prozesse, die spezifisch Individuen oder deren Persönlichkeit betreffen.

Für LB würde es der Klärung dienen, wenn Buchstabe e wie folgt ergänzt würde: „… zum Schutz von Informationen und zum Datenschutz." Es sollte zudem geprüft werden, ob die für das Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlichen kritischen Infrastrukturen nicht als besonders wichtiges schützenswertes Interesse in den Katalog von Artikel 1 Absatz 2 ISG aufgenommen werden sollten.

Der ETH-Rat beantragt Artikel 1 Absatz 2 Buchstabe d zu ergänzen mit: „… der Schweiz, ihrer Behörden und Organisationen sowie betroffener Dritter." Über das ganze ISG gesehen, gehe es nicht nur um Landesinteressen, sondern insbesondere auch um spezifische Interessen der betroffenen Behörden und Organisationen, deren Tätigkeiten auch ihre eigenen Berufs-, Geschäfts- und Fabrikationsgeheimnisse sowie die schutzwürdigen Interessen Dritter umfasst. Insbesondere werde damit auch möglich, dass die Klassifizierung nach INTERN, VERTRAULICH und GEHEIM auch die wirtschaftlichen Interessen des ETH-Bereichs abdeckten, ohne die Kompatibilität mit dem Öffentlichkeitsprinzip zu verletzen.

In Artikel 1 Absatz 2 Buchstabe e werde der Begriff der Bundesbehörden gebraucht: Die Benutzung dieses Begriffs ist für den ETH-Rat verwirrend, da er im Text nicht weiter vorkomme und anschliessend nur von verpflichteten Behörden und verpflichteten Organisationen gesprochen werde. Es sei somit nicht klar, ob mit Bundesbehörden nur die in Artikel 2 definierten verpflichteten Behörden oder auch die verpflichteten Organisationen gemeint sind. Die Empa erachtet es zudem als stossend, wenn nur die Behörden, nicht aber auch die Organisationen von einem solchen Informationsschutz profitieren könnten.

Die FMH beantragt, Personendaten des Bürgers in Artikel 1 Absatz 2 Buchstabe e explizit zu erwähnen. Der Schutz des Bürgers müsse im Gesetzestext klar benannt werden. Bei einem Datenmissbrauch könnten die Persönlichkeitsrechte der Personen, deren Daten bearbeitet

werden, schwerwiegend verletzt werden. Gewisse Personendaten seien ebenso gefragt wie Technologieinformationen der Industrie. Ihr finanzieller Wert sollte nicht unterschätzt werden.

**Artikel 2** Verpflichtete Behörden und Organisationen

Trotz gewisser Bedenken, erscheint es ZH von der Sache her grundsätzlich sinnvoll, dass kantonale Behörden und Stellen, die im Auftrag des Bundes und unter seiner Aufsicht sicherheitsempfindliche Tätigkeiten ausüben, gemäss Artikel 2 Absatz 2 Buchstabe f ISG in den Geltungsbereich des ISG fallen. Nur so könne die durchgängige Sicherheit von Informationen im ganzen Verantwortungsbereich des Bundes gewährleistet werden. Die Regelung greife zwar in die Organisationsautonomie der Kantone ein, es wäre aber nicht praktikabel, in einer Verwaltung zwei oder mehrere unterschiedliche Sicherheitsregimes anzuwenden.

ZG beantragt, Artikel 2 Absatz 2 Buchstabe f sei wie folgt zu ändern: „[«]2 Es gilt für die nachstehenden Organisationen (verpflichtete Organisationen): f. kantonale Behörden und Stellen, die ~~im Auftrag des Bundes und unter seiner Aufsicht~~ in Zusammenarbeit mit dem Bund sicherheitsempfindliche Tätigkeiten ausüben.“ Die Informationssicherheit betreffe die Kantone nicht nur als Vollzugsbehörden von Bundesaufgaben, wie die Vorlage vorgebe. Die Kantone operierten im Sicherheitsbereich nicht als klassische Vollzugsorgane «im Auftrag des Bundes und unter seiner Aufsicht». Im Bereich der Inneren Sicherheit nehmen sie hoheitliche Befugnisse wahr. Die Bundesorgane seien Teilnehmer im Sicherheitsverbund und gelegentlich sogar Auftragnehmer der Kantone. Die Kantone würden aber nicht vom Gesetzesentwurf erfasst, wenn sie nicht «im Auftrag des Bundes» handelten. Das mache keinen Sinn, da gerade auch im Bereich der Inneren Sicherheit sensitive und klassifizierte Informationen und Daten anfallen und ausgetauscht würden, die besonderen Schutz verdienten.

Für BS ergibt sich weder aus dem vorgeschlagenen Gesetzeswortlaut (Art. 2 Abs. 2 Bst. f ISG) noch aus den Erläuterungen klar, welche Tätigkeiten kantonaler Behörden in den Geltungsbereich fielen. BS regt an, Artikel 87 ISG um eine Bestimmung zu ergänzen, wonach der Bundesrat die Tätigkeiten gemäss Artikel 2 Absatz 2 Buchstabe f durch Verordnung festzulegen habe. Damit die Auswirkungen auf den Kanton abgeschätzt werden können, sollte bereits die Botschaft eine Fassung dieser Liste aus heutiger Sicht enthalten. Ausserdem sollte die Botschaft auch klarstellen, was unter «unter Aufsicht» zu verstehen ist.

Für GE ist es notwendig zu die in Artikel 2 Buchstabe f vorgesehenen kantonalen Behörden und Stellen exakt zu bezeichnen, insbesondere was gemeint ist mit «sensible Aufgaben im Auftrag und unter Aufsicht des Bundes». Diese Informationen würden erlauben, die möglichen technischen und finanziellen Konsequenzen für die Infrastrukturen genauer zu bemessen.

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

Für privatim ist es grundsätzlich sinnvoll, dass nach Artikel 2 Absatz 2 Buchstabe f ISG kantonale Behörden und Stellen, die im Auftrag des Bundes und unter seiner Aufsicht sicherheitsempfindliche Tätigkeiten ausüben, in den Geltungsbereich des ISG fallen. Nur so könne die durchgängige Sicherheit von Informationen im ganzen Verantwortungsbereich des Bundes gewährleistet werden. Daraus ergäbe sich aber für die Kantone die praktische Notwendigkeit, ihre eigenen Informationssicherheitsregeln an das ISG anzupassen; es wäre nicht praktikabel, in einer Verwaltung zwei oder mehrere unterschiedliche Sicherheitsregimes anzuwenden. Damit werde auf Kantons- (und allenfalls Gemeinde-)ebene Handlungsbedarf ausgelöst, weil das ISG Massnahmen vorsieht (namentlich Personensicherheitsprüfung und Betriebssicherheitsverfahren), die auf der Stufe Kanton (und allenfalls Gemeinde) vermutlich weitgehend noch nicht oder nur ansatzweise geregelt seien. Daher müssten die Kantone die Dienste der Bundesfachstellen in Anspruch nehmen können. Soweit das ISG die kantonalen Stellen direkt verpflichte, müssten die Leistungen (z.B. Durchführung des PSP) vom Bund finanziert werden. Privatim beantragt deshalb den Artikel 89 ISG um eine Regelung zu ergänzen, die vorsehe, dass kantonale Behörden und Stellen die Leistungen der im ISG vorgesehenen Fachstellen des Bundes in Anspruch nehmen könnten. Falls andere als die in

Artikel 2 Absatz 2 Buchstabe f ISG vorgesehenen Stellen diese Leistungen in Anspruch nehmen (wenn also der Kanton für weitere Kantonsmitarbeitende eine PSP einführt), dann soll der Bund dafür kostendeckende Gebühren erheben. Falls dieser Antrag nicht umgesetzt werde, sei die Lösung des Bundesdatenschutzgesetzes gegenüber der vorgeschlagenen Regelung in Artikel 2 Absatz 2 Buchstabe f ISG vorzuziehen (Selbstverantwortung der Kantone, solange Minimalstandards eingehalten werden, Art. 37 Abs. 1 DSG).

Die SIK beantragt Buchstabe f zu streichen, falls ihr Antrag zu Artikel 89 nicht umgesetzt werde (siehe unten Bemerkungen der SIK zu Art. 89).

Insecor regt an, den Artikel mit „Geltungsbereich“ zu benennen. Die verpflichteten Bundesstellen neben den „sicherheitsempfindlichenTätigkeiten“ in einem Artikel zu umschreiben schaffe mehr Verwirrung als Klarheit. Insecor empfiehlt diese beiden unterschiedlichen Themen entsprechend aufzugliedern (vgl. die Anmerkungen zu „Begriffe“). Insecor regt dringend an, den sachlichen Geltungsbereich im Erläuternden Bericht (Kap. 1.2.2.1) sowie im Gesetzestext dahingehend zu präzisieren, dass die gesamtheitliche Betrachtung der Gefahren (integrale Sicherheit) wichtig sei. Die Thematik „IT-Sicherheit“ lasse sich schwer strikte von der „Cyber-Sicherheit“ trennen, soweit sinnvoll sei eine solche Trennung aber vorzunehmen.

Für it-rm reicht es aus Sicherheitsüberlegungen nicht aus, dass nur kantonale Behörden, die im Auftrag des Bundes und unter seiner Aufsicht sicherheitsempfindliche Tätigkeiten ausüben, dem Gesetz unterstehen. Unterstehen sollten ihm vielmehr alle kantonalen Behörden, welche in ihrer Funktion Einsicht in sicherheitsempfindliche Informationen des Bundes haben, ihm solche zustellen oder solche bearbeiten müssen. Ansonsten habe man bei den kantonalen Stellen gegebenenfalls weniger oder effizientere Sicherheitsmassnahmen und somit weniger oder mehr Schutz der Informationen. Der Begriff Auftragsverhältnis suggeriere ein Subordinationsverhältnis. Es könnte aber auch sein, dass sensitive Informationen zwischen Bund und Kantone transferiert werden, welche für die Erfüllung von Arbeiten benötigt werden, welche unter die Hoheit der Kantone fallen. Weiter sollte ergänzt werden, dass auf Organisationen und Institutionen, welche kritische Infrastrukturen betreiben (Art. 81 ff.), dieses Gesetz Anwendung finde. Die Liste in Absatz 3 ist nach Ansicht von it-rm nicht abschliessend und sollte daher mit „namentlich“ oder „unter anderem“ ergänzt werden.

Für sicherheitsempfindliche Tätigkeiten sollen auch “Organisationen des privaten Rechts“ dem ISG unterstellt werden. Auf welche privatrechtlichen Organisationen das ISG ganz oder teilweise anwendbar sein soll, wird gemäss Artikel 87 Absatz 4 ISG durch den Bundesrat in einer Verordnung festgelegt. LB empfiehlt, dass beim Erlass dieser Verordnung die interessierten Kreise der Wirtschaft beigezogen werden, einschliesslich die im Bereich der Informatik tätigen Fachverbände, wie ICT Switzerland und deren Mitglieder sowie die auf Informationssicherheit spezialisierten Fachorganisationen ISSS, Clusis, swissecurity.org und deren Mitgliedorganisationen.

**Artikel 3** Verhältnis zur Spezialgesetzgebung

Obwohl Artikel 3 Absatz 1 ISG die Anwendung des BGÖ vorbehält, erscheint es ZH fraglich, ob eine zum Voraus erfolgte Klassifizierung nach Artikel 14 ISG die Entscheidungs- und Ermessensfreiheit einer nach Artikel 10 Absatz 1 BGÖ zuständigen Behörde weiter im vollen Umfang belasse. ZH bezweifelt es. Eine gesetzgeberische Koordination sei deshalb hier wünschenswert.

TI begrüsst das Prinzip, wonach die Bestimmungen des Öffentlichkeitsgesetzes (BGÖ) über den Zugang zu amtlichen Dokumenten auf der Grundlage des ISG (intern, vertraulich, geheim) sowohl auf nicht klassifizierte als auch auf klassifizierte Informationen Anwendung finden sollen. Das Ergebnis der üblichen Interessensabwägung auf der Grundlage des BGÖ (Art. 7) werde dann die eventuellen Einschränkungen des Rechts auf Zugang zu den Informationen rechtfertigen. Betreffend das Verhältnis des ISG zu anderen Bundesgesetzen weise Absatz 2 richtigerweise darauf hin, dass das ISG als ergänzendes Recht anzusehen sei, mit besonderem Bezug auf den Schutz von Personendaten. Das bedeutet, dass Personendaten im Aufgabenbereich der Bundesbehörden weiterhin zu Recht nach dem DSG behandelt werden und, was die Schutzmassnahmen betrifft (organisatorische, technische, physische und personelle), in die diesbezüglichen und punktuellen Bestimmungen des ISG inte-

griert werden. Das bedeute gleichzeitig, dass Personendaten, die zur Wahrung der öffentlichen Sicherheit wesentlich seien, nach den Vorschriften des ISG klassifiziert werden könnten, ohne dass der allgemeine bzw. der Querschnittscharakter des DSG dadurch angetastet oder zumindest relativiert würde.

Für die SP Schweiz ist zentral, dass das neue ISG nicht zu mehr Klassifizierungen führten, als dies bisher der Fall gewesen sei. Andernfalls sei das Risiko gross, dass das Öffentlichkeitsprinzip eingeschränkt werde, zeige doch die BGÖ-Praxis, dass einmal klassifizierte Dokumente deutlich seltener gestützt auf das Öffentlichkeitsprinzip zugänglich gemacht würden. Obschon Artikel 3 Absatz 1 ISG das Öffentlichkeitsgesetz (BGÖ, SR 152.3) ausdrücklich vorbehalte, seien die Wechselwirkungen zwischen dem ISG und dem im BGÖ verankerten Öffentlichkeitsprinzip nicht wirklich geklärt. Die SP Schweiz erwartet, dass die Bestimmungen über die Klassifizierung inhaltlich so gestaltet werden, dass sie unter keinen Umständen über den Ausnahmekatalog nach Artikel 7 BGÖ hinausgingen und diesem zumindest inhaltlich nicht widersprechen würden. Es müsse sichergestellt sein, dass das ISG in Zukunft nicht zu noch mehr Streitfällen zwischen Nutzern des BGÖ und der Verwaltung führe.

Für die SP ist das Öffentlichkeitsprinzip eng verbunden mit dem Konzept der Open Government Data (OGD). In der Strategie e-government des Bundes sei OGD ein Bestandteil. Die Ratifizierung der Aarhus-Konvention führe dazu, dass die Schweiz bei Umweltdaten dem Transparenzprinzip nachlebe. Auch das Pilotprojekt "Single Point of Orientation" des Schweizerischen Bundesarchivs zeige, wie eine bürgerfreundliche Übersicht über die Unterlagen der Bundesverwaltung realisiert werden könne. Die SP erwartet, dass das neue ISG den Projekten und generell der vom Bundesrat in seinem Bericht vom 13. September 2013 bekräftigten OGD-Strategie keine Hindernisse in den Weg lege. Es sei deshalb zu prüfen, ob im ISG ein entsprechender ausdrücklicher Vorbehalt zu verankern sei.

Clusis bedauert, dass ein Hinweis auf das Datenschutzgesetz fehlt. Absatz 2, der vorgibt, dass «wenn die Informationen gestützt auf andere Bundesgesetze geschützt werden müssen, die Bestimmungen des vorliegenden Gesetzes ergänzend Anwendung finden» müsse ergänzt werden mit «Die Bestimmungen des DSG sind zusätzlich anwendbar.»

Für insecor ist es nicht nachvollziehbar, warum in Absatz 2 lediglich Bezug zu „Informationen“ genommen werde. Es müsste heissen „Soweit Informationen und Informations- und Kommunikationstechnologien aufgrund anderer Bundesgesetze geschützt werden müssen …“.

Der wichtige Begriff “kritische Infrastrukturen“ und der generelle Verweis auf die anwendbare “Spezialgesetzgebung“ bedarf nach LB einer konkreteren und präziseren Umschreibung, weil das Gesetz ja auch auf privatrechtliche Betreiber kritischer Infrastrukturen anwendbar sein soll.

Der Entwurf zum Nachrichtendienstgesetz sieht in Artikel 66 Ausnahmen vom Öffentlichkeitsprinzip bei Unterlagen über die nachrichtendienstliche Informationsbeschaffung vor. Der NDB geht davon aus, dass dieser Grundsatz durch Artikel 3 ISG nicht tangiert wird. Es erschliesst sich dem NDB nicht vollständig, weshalb beispielsweise GEHEIM klassifizierte Dokumente, deren Kenntnisnahme durch Unberechtigte öffentliche Interessen nach Artikel 1, Absatz 1 ISG schwerwiegend gefährden können, dem Öffentlichkeitsprinzip unterstellt bleiben sollen.

## 2. Kapitel: Allgemeine Massnahmen der Informationssicherheit

### Allgemein

LB empfiehlt das ISG durchgehend darauf zu prüfen, ob sich eine bestimmte Anforderung, Vorschrift oder Regel nur auf „verpflichtete Behörden“ oder auch auch auf „Organisationen“ (des privaten Rechts) bezieht, wenn diese gemäss Artikel 2 Absatz 2 Buchstabe e ISG dem Anwendungsbereich des ISG unterstellt sind.

Die FMH stellt die Unterscheidung zwischen der Klassifizierung von Informationen und von Sicherheitsstufen von IKT-Mitteln und deren unterschiedlichen Anwendungsbereich in Frage: Der Schutz der Systeme müsse ja dem Schutz der Informationen in den Systemen dienen.

**Artikel 4** Informationssicherheit

TG fehlt der Grundsatz der Verhältnismässigkeit. So sollte die Bestimmung dahingehend ergänzt werden, dass eine Massnahme nur so lange zulässig ist, bis ihr Zweck erreicht ist oder sich zeigt, dass er nicht erreicht werden kann. Zudem dürfe diese zu keinem Nachteil führen, der zum angestrebten Erfolg in einem offenbaren Missverhältnis steht. Zwar werde später (bei Artikel 12 des Entwurfes ISG) hinsichtlich der Klassifizierung von Informationen die Beschränkung auf das Mindestmass erwähnt. Dies sollte aber bei allen Bestimmungen zur Informationssicherheit gelten, weshalb dieser Grundsatz hier bei den allgemeinen Bestimmungen klar aufzunehmen sei. Für TG sollte bei der Informationssicherheit auch sichergestellt werden, dass die Dokumente von der richtigen Stelle kommen, d.h. als von der genannte Quelle stammend, erkannt werden können. In Artikel 4 Absatz 4 des Entwurfes ISG werde aber nur die "Nachvollziehbarkeit" erwähnt, welche deshalb noch um den Begriff der "Authentizität" zu erweitern sei. Damit könne sichergestellt werden, dass die Informationen auch authentisch seien, was bei der Informationssicherheit einen wichtigen Aspekt darstellen könne.

Aus Sicht der SP Schweiz fehlt in Artikel 4 Absatz 3 die Nennung des Grundsatzes der Verhältnismässigkeit. Die SP regt deshalb folgende Ergänzung an: „$^{3bis}$ 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."

Für FER scheint es angezeigt, auf die Klassifizierung der Informationen zu fokussieren und nicht auf «…einer funktionsbezogene Verantwortung im Sinne von Artikel 1 Absatz 2. Ziel muss es sein, eine präventive Strategie zu definieren und nicht bloss auf Vorkommnisse zu reagieren oder zu überreagieren, die nachträglich eine Änderung der existierenden Prozesse verlangten.

Insecor stellt fest, dass unter Absatz 3 plötzlich die Abkürzung „IKT-Mittel" für den Begriff „Informations- und Kommunikationstechnologien" auftauche. Da dieser Begriff bereits in vorangehenden Artikeln mehrmals erwähnt werde, sollte die entsprechende Abkürzung bereits zu Beginn der Gesetzesvorlage, also in Artikel 1 Absatz 1 stehen.

Für It-rm sollte Absatz 2 mit einem Buchstaben e „verlässlich sein müssen" ergänzt werden. Die Verlässlichkeit setze auch die Korrektheit des Inhalts, sprich die richtige und vollständige Erfassung und Verarbeitung von Informationen voraus. Die Verlässlichkeit der Informationen sei zentral. Der Bürger dürfe sich auf die Richtigkeit der in den Registern enthaltenen Angaben verlassen (Gutglaubensschutz). Wären die Informationen in den Registern fehlerhaft, so käme es massenweise zu Beanstandungen und gegebenenfalls zu strittigen Verfahren. Für It-rm sollte Absatz 2 zudem mit einem Buchstaben f „authentisch oder anonym sein müssen" ergänzt werden. Authentisch seien Daten und Informationen dann, wenn sie einer Person oder Maschine zugeordnet werden können. Ansonsten habe man ein Sicherheitsproblem, weil man nicht wisse, wer Zugang zu diesen Informationen gehabt und diese versandt hat. Um die Berechtigung einer online Anfrage auf vertrauliche Daten und Informationen festzustellen, bedürfe es zuerst eines Nachweises, wem die Verantwortung für die Anfrage zugeordnet werden kann. Dies benötige die Prüfung der Echtheit der Anfrage (Authentizität). Anonymität bezwecke das Gegenteil von Authentizität, nämlich dass die Information nicht zugeordnet werden kann. Der Schutz der Anonymität werde beim Stimmgeheimnis verlangt. Was beim Stimmgeheimnis geschützt werden müsse, sei, dass die eingegangene Stimme nicht einer natürlichen Person zugeordnet werden kann.

**Artikel 5** Oberste Führungsverantwortung

Für insecor ist es ist nicht ersichtlich, wieso in Absatz 1 die Oberste Führungsverantwortung nur bei den „verpflichteten Behörden" liegen soll und nicht auch bei den „verpflichteten Orga-

nisationen“ (sprich z.B. der „Bundesverwaltung“). Es könne bereits gestützt auf die in der RVOG (SR 172.010) erwähnten Verantwortlichkeiten nicht sein, dass die Bundesverwaltung die Sicherheit nicht auch als „Chefsache“ zu betrachten habe (vgl. Erläuternder Bericht, Kommentar zu Artikel 5, S. 39). Zu Absatz 4: Das Personal sollte nicht nur regelmässig und stufengerecht „informiert“ werden, sondern auch „geschult und verpflichtet“ werden. Eine blosse Information betreffend Informationssicherheit sei noch nie zielführend gewesen.

It-rm hält die in Absatz 1 Buchstabe a geforderte Prüfung der Informationstechnologie nach Stand der Lehre und Technik im Bereich der Informationstechnologie für nicht erfüllbar, weil sie uferlos wäre. Wichtig scheine, dass die Koordinationsstelle für die Erarbeitung und Aktualisierung eines Mindeststandards bei der Prüfung verantwortlich zeichne. Die Behörden hätten dann aufgrund dieser Vorgaben entsprechend zu prüfen. Ansonsten bestünde die Gefahr, dass der Prüfungsumfang von den Behörden individuell definiert werde, was zu einer Inhomogenität bei den Sicherheitsmassnahmen und deren Umsetzung führen könnte. It-rm schlägt vor, einen Verweis auf Artikel 88 ISG aufzunehmen und dann dort den Aspekt der Prüfung zu ergänzen und die Koordinationsstelle zu ermächtigen, Vorschriften zu erlassen, welche Prüfschritte bei entsprechendem Schutzbedarf durchzuführen sind.

LB schlägt vor, dass sich Artikel 5, wie der nachfolgende Artikel 6, auf “verpflichtete Behörden und Organisationen“ beziehen soll. Denn gerade im Bereich der privaten Wirtschaft wäre erwünscht auf einen Grundsatz des Inhalts verweisen zu können, wonach die Wahrung der Informationssicherheit zur Verantwortung des obersten Führungsorgans gehört.

Gestützt auf die Erläuterungen zu Artikel 6 ist für den ETH-Rat nicht klar, ob Artikel 5 tatsächlich auch für die dezentralen Einheiten des Bundes gelten soll. Zumal für den ETH Bereich betreffend Risikomanagement eigene Bestimmungen gelten würden.

**Artikel 6** Risikomanagement

TG und SP beantragen, das Wort „identifiziert“ im letzten Satz des zweiten Absatzes zu streichen. Für TG werden nach der Lehre des Risikomanagements die Risiken - wie im Entwurf erwähnt - identifiziert, bewertet, beurteilt und überprüft. Absatz zwei des genannten Artikels verfange sich dann aber zu stark in dieser Begriffssystematik. Es sollten richtigerweise nicht nur die „identifizierten“ Risiken vermieden werden, sondern alle Risiken. Für die SP sollen die verantwortlichen Behörden und Organisationen generell dafür sorgen, dass Risiken vermieden oder auf ein tragbares Mass reduziert würden – sowohl die identifizierten als auch die noch nicht erkannten.

Dem Ausdruck „Tragbares Mass“ mangelt es aus Sicht von it-rm an Konkretisierung und er enthalte ein grosses Mass an individueller Einschätzung bei der Umsetzung. Zudem leiste diese Unbestimmtheit in einem technischen Umfeld Vorschub zur Rechtsunsicherheit. Weiter kann es ebenfalls zu einer Inhomogenität im Sicherheitsdispositiv führen. It-rm schlägt v, folgende Ergänzung sinngemäss aufzunehmen: „Die Koordinationsstelle bestimmt Mindeststandards für die jeweiligen Klassifikationsstufen, welches Schadensausmass bei Verletzung oder Umgehung der Informationssicherheit als tragbar erachtet wird.“

**Artikel 7** Sicherheitsanforderungen und -massnahmen

Für TG könnte Absatz 2 allenfalls gestrichen werden, da bezüglich der Festlegung der Standardanforderungen und der Standardmassnahmen bereits in Artikel 88 des Entwurfes ISG (beim Vollzug) ein Hinweis auf den Stand der Lehre und Technik erfolge. Es ergebe sich somit bereits aus der genannten Vollzugsbestimmung im hinteren Teil des Entwurfes, dass auch die hier genannten Sicherheitsmassnahmen dem (anerkannten) Stand der Lehre und Technik zu entsprechen hätten.

Für insecor ist es unüblich, zuerst auf einen Gesetzesartikel zu verweisen, welcher erst am Ende des betreffenden Gesetzes zu finden sei. Inseco empfiehlt bereits zu Beginn des ISG einen Hinweis auf die „Standardanforderungen und –massnahmen“ aufzunehmen und dort auf den Artikel 88 zu verweisen.

Da gemäss den Erläuterungen für Behörden und Organisationen, die nicht dem Bundesrat unterstellt sind, keine Pflicht bestehe den Standardanforderungen gemäss Artikel 88 zu folgen, regt der ETH-Rat an, Artikel 7 Absatz 1 in diesem Sinne allenfalls zu präzisieren.

**Artikel 8** Zusammenarbeit mit Dritten

Privatim vermisst hier den Grundsatz, dass die Verantwortung für die Wahrung der Informationssicherheit bei der jeweiligen Behörde oder Organisation, die zu ihrer Aufgabenerfüllung eine Drittperson beizieht, verbleibe. Art 8 ISG müsse, um diesem Grundsatz Nachdruck zu verleihen, um einen Passus zur Verantwortung des auftraggebenden Organs bzw. der auftraggebenden Organisation ergänzt werden.

Ein Vertrag rechtfertigt für it-rm grundsätzlich nicht, dass ein Amtsgeheimnis einem aussenstehenden Dritten zugänglich gemacht werden dürfe. Mit der hier aufgenommenen Klausel würde jedoch über das Gesetz die Möglichkeit eröffnet, strafrechtlich sensitive Daten Dritten zugänglich zu machen. Auf diesen Punkt sollte in der Erläuterung deutlich hingewiesen werden, damit sich das Parlament dessen bewusst sei. Wenn die Behörde nicht Geheimnisherr, sondern nur Geheimnisträger sei, wäre es bedenklich wenn Dritte von der Behörde hinzugezogen würden. Um gegebenenfalls einen Interessenskonflikt frühzeitig zu erkennen, wäre es wünschenswert, den Geheimnisherrn zu informieren. Für It-rm sollte im Sinne der Rechtssicherheit und Transparenz gegenüber dem hinzugezogenen Dritten. auch die Haftung geregelt sein, wenn ein Schaden an einer Privatperson durch den hinzugezogenen Dritten verursacht wird. Weiter sollte noch ergänzt werden, dass die Koordinationsstelle Ausführungsvorschriften erlasse, wie Dritte auszuwählen seien und welche Kriterien diese im Einzelnen zu erfüllen hätten.

Für den ETH-Rat sollte dieser Artikel klarstellen, welche Arten von Zusammenarbeiten hierunter fallen. Eine Unterstellung des ETH-Bereichs unter Artikel 8 Absatz 2 sei unverhältnismässig und wäre mit entsprechenden Kosten verbunden. Das Beschaffungsverfahren dürfte durch diese Bestimmung erheblich erschwert werden, v.a. was die operative Abwicklung der Offertevaluation betreffe (zeitliche Verzögerungen). Eine derart weitreichende Bestimmung, wonach in den entsprechenden Vereinbarungen und Verträgen mit Dritten die Anforderungen und Massnahmen nach Massgabe des ISG berücksichtigt werden müssten, sei in der Praxis nicht umsetzbar: die weitreichenden Anforderungen und Massnahmen des ISG seien in deren Breiten- und Tiefenwirkung nicht überschaubar, es werde daher weder eine Behörde noch einer Organisation gelingen, dementsprechende Klauseln in ihre Verträgen einfliessen zu lassen, welche den Forderungen von Artikel 8 wie verlangt gerecht würden. Des Weiteren erachtet die Empa einen derart weitreichenden Eingriff weder als mit der Autonomie einer öffentlich-rechtlichen Anstalt verträglich noch liessen sich solche Vorgaben mit den Prinzipien der Vertrags- bzw. der Forschungs- und Lehrfreiheit vereinbaren. Der ETH-Rat schlägt als neuen Text vor: „Verpflichtete Behörden und Organisationen haben bei der vertraglichen Zusammenarbeit mit Dritten auf die Geltung und Einhaltung der Bestimmungen des Informationssicherheitsgesetzes ISG summarisch hinzuweisen.“

**Artikel 9** Vorgehen bei Verletzungen der Informationssicherheit

Für TG fehlt hier eine Bestimmung, wonach bei erkannten Verletzungen entsprechende Gegenmassnahmen zu treffen seien. Es werde hier bloss erwähnt, dass bei Verletzungen der Informationssicherheit die Auswirkungen zu minimieren seien. Dies sollte entsprechend ergänzt werden, um ein sinnvolles Ganzes zu erhalten.

FER fragt sich, ob es nicht eine klare Bestimmung benötige, welche möglichen richterlichen oder administrativen Strafen eine Verletzung der Informationssicherheit haben kann.

**Artikel 10** Vorsorgeplanungen

LB schlägt vor, dass sich Artikel 10 auf “verpflichtete Behörden und Organisationen“ bezieht. Denn gerade im Bereich der privaten Wirtschaft wäre erwünscht auf einen Grundsatz des Inhalts verweisen zu können, wonach zur Wahrung der Informationssicherheit eine Vorsorgeplanung erstellt und entsprechende Übungen durchgeführt werden müssen.

**Artikel 11** Kontrollen

Für TG muss die Vertraulichkeit der unabhängigen Stelle gesetzlich verlangt werden, zumal diese bei ihrer Prüfung zwangsläufig Einsicht in sehr vertrauliche Dokumente erhalten wird.

Für VD sind die Erläuterungen bezüglich der Modalitäten und der Kosten der Kontrollen im Anwendungsbereich der kantonalen Behörden wenig präzis. Ein Organ wie eine kantonale Finanzkontrolle ist allein rechtlich und professionell in der Lage die Aufgaben gemäss Absatz 2 zu erfüllen.

Die SP schlägt folgende Ergänzung vor: „[3] Die Ergebnisse der Kontrollen nach Absatz 1 und 2 werden periodisch den Geschäftsprüfungskommissionen der eidgenössischen Räte zur Kenntnis gebracht.“ Artikel 11 verpflichte die Behörden, die Einhaltung der ISG-Vorschriften und die Wirksamkeit der getroffenen Massnahmen regelmässig zu überprüfen. Das seien Informationen, die auch die parlamentarische Oberaufsicht interessierten.

**Artikel 12-18** Klassifizierungen von Informationen

Aufgrund fehlender Legaldefinitionen stellt sich in diesem Abschnitt für insecor die Frage, ob die erwähnten Bestimmungen auch für „klassifiziertes Material“ gelten sollen. Dies sei sehr unbefriedigend und sollte unbedingt entsprechend präzisiert werden.

**Artikel 12-14** Klassifizierungen

Die CVP stimmt der Schaffung einer einheitlichen Regelung für die Klassifizierungsstufen und der Klassifizierungsgründe für alle verpflichteten Behörden zu.

Die BA spricht sich gegen eine Klassifizierungspflicht für Akten aus Strafverfahren aus. Schon in der IschV sei seinerzeit für Akten aus Strafverfahren keine Klassifizierungspflicht verankert worden. Die Bearbeitung und der Zugang zu diesen Akten richte sich ausschliesslich nach den Regeln der StPO. Eine Klassifizierungspflicht nach ISG sei nicht nur unnötig (es gilt das strafprozessuale Untersuchungsgeheimnis), sie sei gerade in aufwändigen und komplexen Strafverfahren, wie sie die BA führe, nicht praktikabel. Eine Klassifizierung nach ISG würde dazu führen, dass Akten ein und desselben Strafverfahrens verschiedenen Klassifizierungsstufen zugewiesen und dementsprechend unterschiedlich behandelt werden müssten. Eine damit verbundene Ausgliederung einzelner Aktenstücke würde nicht nur die nach Gesetz und Rechtsprechung vorgegebene Aktenführung verunmöglichen, sondern würde auch den Grundsätzen der Einheit und Vollständigkeit der Verfahrensakten zuwiderlaufen. Um dies zu vermeiden, müssten die gesamten Akten – wie das bis anhin im Rahmen der geltenden Strafprozessordnung unter Wahrung des Untersuchungsgeheimnisses gehandhabt wurde – einer einzigen „Klassifizierungsstufe“ zugewiesen werden, nämlich derjenigen Stufe der in den Akten vorhandenen, sensitivsten Informationen. Dies dürfte jedoch nicht im Sinne des vorliegenden Entwurfs sein, zumal gemäss den Erläuterungen die Menge der klassifizierten Informationen im Interesse eines tragbaren Vollzugsaufwandes auf das notwendige Minimum beschränkt und somit nicht der gesamte Aktenbestand einheitlich einer Klassifizierungsstufe zugewiesen werden soll. Zusätzlich würden sich für die BA unlösbare Probleme im Verkehr mit kantonalen Strafverfolgungsbehörden ergeben. Kantonale Behörden seien dem ISG grundsätzlich nicht unterworfen.

**Artikel 12** Grundsätze der Klassifizierung

Nach Erachten von it-rm sollte ergänzt werden, dass die Koordinationsstelle eine Anleitung erstelle, wie sensitive Informationen zu klassifizieren seien.

Für den NDB sind auf Ebene der Ausführungsbestimmungen zu Absatz 4 vereinfachte Vorschriften für den NDB festzulegen (analog geltende Regeln der vereinfachten Bearbeitung von klassifizierten Informationen im Bereich der Nachrichtendienste und der Polizei vom 18.1.2008)

**Artikel 13** Zuständigkeiten

Für TG müsste bei einer Delegation der Klassifizierungskompetenz an eine andere Stelle bzw. Person allenfalls auch die verpflichtete Behörde selbst (hier nur: klassifizierende Stelle und Vorgesetzte) die Möglichkeit haben, die Klassifizierung zu ändern.

Nach Auffassung der SP müsste, je nach Situation, auch die verpflichtete Behörde selbst die Möglichkeit haben, die Klassifizierung zu ändern oder aufzuheben, nicht nur die klassifizierende Stelle oder die ihr vorgesetzten Stelle.

Für den NDB sind auf Ebene der Ausführungsbestimmungen zu Absatz 2 vereinfachte Vorschriften für den NDB festzulegen (analog geltende Regeln der vereinfachten Bearbeitung von klassifizierten Informationen im Bereich der Nachrichtendienste und der Polizei vom 18.1.2008).

**Artikel 14** Klassifizierungsstufen

UR begrüsst, dass lediglich drei Klassifizierungsstufen festgelegt wurden. Der Umgang mit klassifizierten Daten und Systemen und die daraus resultierenden Konsequenzen für die Kantone würden im Entwurf jedoch nicht näher umschrieben. Diesem Umstand sei mit ergänzenden, rechtsverbindlichen Ausführungen Rechnung zu tragen.

Für TG ist es nicht nachvollziehbar, weshalb bei allen Klassifizierungsstufen bloss ein Hinweis auf die Buchstaben a-d von Artikel 1 des Entwurfes ISG erfolge, jedoch Buchstabe e nicht erwähnt wird. Offenbar habe bei Artikel 1 des Entwurfes eine nachträgliche Ergänzung stattgefunden, welche hier fälschlicherweise nicht nachgetragen worden sei.

Für privatim müsste der Vollständigkeit halber mindestens die Botschaft darauf hinweisen, was eine Nichtklassifizierung bedeute: Unterstehen solche Informationen trotzdem dem Amtsgeheimnis? Wie steht es mit der Zugänglichkeit nach dem Öffentlichkeitsprinzip?

Clussis versteht die drei Klassifizierungsstufen INTERN, VERTRAULICH und GEHEIM gut. Aber wie kommt es, dass es keine Stufe ÖFFENTLICH gibt? Es sei unmöglich, dass es keine Dokumente gebe, die von Anfang an öffentlich seien, umso mehr als das Öffentlichkeitsgesetz vorbehalten sei.

Das vorgeschlagene Klassifikationsschema ist für it-rm zu wenig differenziert, damit der ordnungsgemässe Ablauf der Bundesbehörden wie mit diesem Gesetz beabsichtigt geschützt werden könne. Es gebe weitere Beeinträchtigungen im Bereich Informationsbearbeitung als die Bekanntgabe von vertraulichen Informationen, um den Staat und die Verwaltung massiv zu schädigen. It-rm schlägt vor, die Klassifikationsstufen abzuändern in: „Für internen Gebrauch“, „Schützenswert oder hoher Schutz“ und „Ausserordentlich schützenswert oder sehr hoher Schutz“. Für das Funktionieren einer modernen, mit IKT-Mitteln ausgestatteten Gesellschaft und Verwaltung und für die Wahrung der wirtschafts- und finanzpolitischen Interessen eines Staates bedürfe es nicht nur des besonderen Schutzes vertraulicher Informationen, sondern auch derjenigen Informationen, worauf sich alle Bürger und Beamte verlassen können müssten, wie Informationen aus einem Register oder aus einem Archiv.

LB weist der guten Ordnung halber darauf hin, dass die Kriterien für die Zuweisung von Informationen zu einer Klassifizierungsstufe sehr allgemein gehalten sind und einen erheblichen Spielraum des Ermessens bei der klassifizierenden Stelle offen lassen. Allenfalls könnte das Gesetz in diesem Zusammenhang noch um den Grundsatz ergänzt werden, dass Informationen, welche sich auf klassifizierte Informationen beziehen oder solche enthalten, mindestens die gleiche Klassifizierungsstufe aufweisen müssen. Das wäre ein nützlicher Hinweis für das Verhalten privater Organisationen, wenn sie mit den verpflichteten Behörden klassifizierte Informationen erhalten, bearbeiten, austauschen usw.

Der ETH-Rat weist darauf hin, die Institutionen des ETH-Bereichs wie alle Organisationen selbstverständlich intern-vertrauliche Daten hätten, die durch organisatorische Massnahmen oder – bei Systemen – durch ein geeignetes Berechtigungsmanagement geschützt würden. In den Kerngeschäften Forschung, Lehre und Beratung seien die meisten Informationen grundsätzlich offen. Es gebe nur einige wenige, nicht offen zugängliche Projekte, die mit den Geldgebern vertraglich vereinbart seien.

Die FMH hinterfragt, warum die Personendaten der Bürger bei der Klassifikation von Informationen nach Vertraulichkeitsstufen explizit ausgenommen würden (Artikel 14). Dies stehe im Widerspruch zu den Erläuterungen, die zu Recht feststellten: „Der Bund bearbeitet überdies in grossem Umfang Personendaten. Diese dürfen nach den Vorschriften der Daten-

schutzgesetzgebung 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. Ihr finanzieller Wert sollte nicht unterschätzt werden. Es gibt einen blühenden Markt für die Beschaffung und die Bekanntgabe personenbezogener Daten." Durch den zunehmenden elektronischen Informationsaustausch werden nach Ansicht der FMH auch Personendaten zunehmend gefährdet. Insbesondere habe die Zusammenführung von Informationen zu einer Person zur Folge, dass diese immer einfacher reidentifizierbar werde.

Die FMH beantragt Artikel 14 Absatz 1-3 zu ergänzen mit: „Interessen nach Artikel 1 Absatz 2 Buchstaben a-e." Den Bürger betreffende Informationen – beispielsweise Gesundheitsdaten – müssten ebenfalls den Schutz von Klassifizierungen gemäss Artikel 14 erhalten können. Klassifizierungen dürfen nicht auf die „Entscheidungs- und Handlungsfähigkeit der Bundesbehörden, die innere und äussere Sicherheit, die aussenpolitischen und die wirtschafts-, finanz- und währungspolitischen Interessen der Schweiz" beschränkt werden.

**Artikel 15** Zugang zu klassifizierten Informationen

Beim Vollzug von Artikel 15 ist nach Auffassung der FMH darauf zu achten, dass der Nachweis auch wirklich erbracht werde, dass die Erfüllung der gesetzlichen Aufgabe ohne die jeweilige Information nicht möglich sei.

**Artikel 17** Bekanntgabe klassifizierter Informationen in besonderen Verfahren

Im Sinne von fairen Gerichtsverfahren hält TG dafür auf Absatz 2 von Artikel 17 des Entwurfes ISG zu verzichten, da hier der Anschein erweckt werden könnte, dass sich Gerichte auf geheime Beweismittel stützen dürften, was nie zulässig werden dürfe. In Artikel 17 des Entwurfes ISG werde zwar erwähnt, dass sich die Bekanntgabe von Informationen bei Gerichten und Staatsanwaltschaften (...) nach dem jeweils anwendbaren Verfahrensrecht richte. Damit sollte sichergestellt werden, dass die Wahrheitsfindung in Gerichtsverfahren nicht durch das Mittel der Klassifizierung erschwert werde. In Absatz 2 der genannten Bestimmung werde dann aber ergänzt, dass das zuständige Gericht die klassifizierende Stelle anhören könne. Dies deute darauf hin, dass Gerichtsverfahren allenfalls durch die Klassifizierung eingeschränkt werden dürften. Damit die Gerichte aber weiterhin den eigenen Aufgaben nachkommen können, dürfe es in Gerichtsverfahren keine Klassifizierung geben. Bei Klassifizierungen gehe es um Geheimdaten. Jede Art von *Geheimgerichten* sei unbedingt zu vermeiden, da sonst der staatlichen Willkür Tür und Tor geöffnet werden könnten.

Das BGer macht darauf aufmerksam, dass dieser Artikel für das BGer wesentlich sei und deshalb nicht zu seinem Nachteil verändert werden dürfe.

**Artikel 18** Vorläufige Schutzmassnahmen

Der ETH-Rat beantragt, in Artikel 18 die verpflichtete Organisation zu streichen oder die dezentralen Einheiten der Bundesverwaltung bzw. der ETH-Bereich explizit von dieser Regelung auszunehmen, denn gemäss Artikel 13 müssten nur die verpflichteten Behörden eine klassifizierende Stelle festlegen.

**Artikel 19 – 27** Sicherheit beim Einsatz von IKT-Mitteln

Mit dem in Artikel 19 ISG erwähnten "Sicherheitsverfahren" seien offenbar die in Artikel 20 – 23 ISG umschriebenen Massnahmen gemeint. Dabei ist aus Sicht von LB darauf hinzuweisen, dass den verpflichteten Behörden der Kantone und Gemeinden, welche dem ISG gemäss dessen Artikel 2 Absatz 2 Buchstabe f unterstellt sind, und welche natürlich in ihrer Tätigkeit umfassend IKT Mitteln einsetzen, aus der Erfüllung der Anforderungen von Artikel 19 ff. ISG - zu Lasten der Steuerzahler! - erhebliche Aufwendungen entstehen können. Mindestens im Bereich des "Grundschutzes" sollte daher ein System von Massnahmen vorgesehen werden, die einfach, rasch und kostengünstig umgesetzt werden können. Dies entspreche im Übrigen den heutigen Vorstellungen der Informatiksicherheit, 1. die für die Weiterführung der Geschäfte notwendigen Schlüsselinformationen stark, 2. die in der täglichen

Arbeit eingesetzten Daten und Prozesse nur so weit zu sichern, dass sie nicht ohne weiteres verändert, gelöscht, missbraucht oder unterdrückt werden können.

**Artikel 19** Sicherheitsverfahren

TG vermisst hier den Grundsatz der Verhältnismässigkeit, weshalb dieser in Artikel 4 des Entwurfes ISG - wie vorerwähnt - unbedingt aufzunehmen sei.

Für VD muss die Beschreibung des Sicherheitsverfahrens viel präziser werden.

Für insecor ist aus diesem Artikel nicht ersichtlich, was genau unter „Sicherheitsverfahren“ zu verstehen sei und wieso dies nur die „Behörden“ (jedoch nicht die „Organisationen“) betreffen sollte. Dies sei dahingehend zu präzisieren, dass das Sicherheitsverfahren die nachstehenden Artikel 20-26 umfassen solle.

Welcher Schutz für die entsprechende Sicherheitsstufe oder Klassifikation angemessen sei, sehe gemäss it-rm ein jeder anders. Deswegen sei es notwendig, dass eine zentrale Fachstelle, die Koordinationsstelle, dazu ermächtigt werde, festzulegen, welche Sicherheitsmassnahmen bei entsprechendem Schutzbedarf oder Klassifikation der Informationen mindestens umzusetzen seien. Gestützt darauf sollte gemäss Absatz 1 die Behörde ein Verfahren festlegen.

Gemäss den Erläuterungen zu Artikel 19 Absatz 1 hätten explizit nur verpflichtete Behörden, nicht aber verpflichtete Organisationen ein Sicherheitsverfahren für IKT-Mittel festzulegen. Dennoch bezögen sich Vorschriften von Artikel 19-27 wiederholt auch auf verpflichtete Organisationen. Somit ist für den ETH-Rat unklar, wozu Letztere konkret verpflichtet seien.

**Artikel 20** Schutzbedarfsanalyse und Risikobeurteilung

Für privatim sollte Artikel 20 ISG dahingehend ergänzt werden, dass nicht nur beim Einsatz neuartiger Technologien, sondern auch beim Einsatz neuer IT-Systeme eine Schutzbedarfsanalyse und eine Risikobeurteilung erstellt werden müssen. Mit neuen IT-Systemen ergeben sich neue Risiken und Verwundbarkeiten, Versäumnisse bestehender Lösungen können behoben werden, und allenfalls können auch neue Massnahmen und Kontrollmechanismen institutionalisiert werden.

Gemäss Artikel 20 Absatz 2 sollen nicht nur Organisationen, sondern auch Behörden verpflichtet werden, beim Einsatz neuer Technologien ihre Risikobeurteilung der Fachstelle des Bundes für Informationssicherheit mitzuteilen. Die SNB unterstützt ausdrücklich einen Austausch von Erkenntnissen aus Risikobeurteilungen auf freiwilliger Basis. Sie lehnt hingegen die in Artikel 20 Absatz 2 statuierte Mitteilungspflicht ab, da beispielsweise aufgrund der eingesetzten Technologie (z.B. Software) auf spezifische Aktivitäten zur Umsetzung geldpolitischer Massnahmen geschlossen werden könne. In diesen Bereichen könne auch der mit der Mitteilungspflicht angestrebte Nutzen des Austausches von Erkenntnissen nicht erreicht werden, weil keine der anderen verpflichteten Behörden oder Organisationen im gleichen Geschäftsfeld tätig sei wie die SNB. Mit einer Formulierung von Artikel 20 Absatz 2 als Kann-Vorschrift könne dem Anliegen der SNB hier Rechnung getragen werden.

Für LB ist der Einsatz “neuartiger Technologien“ (der Begriff erscheine auslegungsbedürftig: Ist eine neue Generation von IKT Mitteln, die auf dem Markt angeboten wird, bisher jedoch beim verpflichteten Betrieb nicht eingesetzt wurde, “neuartig“?) im Bereich der Anwendung der durch eine sehr rasche technologische Entwicklung gekennzeichneten IKT Mittel fast alltäglich. Für private Organisationen sei die Pflicht zur Meldung der Risikobeurteilung an die Fachstelle des Bundes für Informationssicherheit heikel, denn damit könne die Offenlegung von Geschäftsgeheimnissen verbunden sein. Grundsätzlich sollte für alle nicht allgemein zugänglichen Informationen privater Organisationen, welche verpflichteten Behörden oder der Fachstelle des Bundes für Informationssicherheit bekanntgegeben würden, das Geschäftsgeheimnis explizit gewährleistet werden. LB schlägt vor, das ISG in diesem Sinne zu ergänzen.

**Artikel 21** Sicherheitseinstufung von IKT-Mitteln

Nach Erachten von it-rm sollte Absatz 2 Buchstabe a mit den Sicherheitsdiensten Verlässlichkeit, Authentizität und Anonymität ergänzt werden (vgl. Bemerkung zu Art. 4 Abs. 2).

Für den ETH-Rat ist die Einstufung von IKT-Mitteln, mit denen besonders schützenswerte Personendaten bearbeitet würden, weiterhin unklar. Die entsprechenden Ausführungen auf Seite 44 und 48 des Erläuternden Berichts (EB) seien schwer verständlich und würden keine klaren Hinweise geben. Merkwürdig erscheine insbesondere die Aussage auf Seite 44 des EB, wonach das entsprechende Informationssicherheitskonzept zu klassifizieren sei, wenn in einem Informationssystem besonders schützenswerte Personendaten bearbeitet würden. Konkret: das Konzept wäre zu schützen, jedoch nicht die Daten selbst; das mache keinen Sinn!

Diese Bestimmung ist nach der Beurteilung des ETH-Rats sehr offen formuliert (was bedeutet „Grundschutz genau“) und führe zu Unsicherheiten, die nicht den Ausführungsbestimmungen überlassen werden sollten. Einige Institutionen des ETH-Bereichs gingen davon aus, dass sie praktisch keine als intern, vertraulich oder geheim zu klassifizierende Informationen im Sinne dieses Gesetzes haben bzw. haben werden (Artikel 14 „Klassifizierungsstufen“). Der erläuternde Bericht stütze diese Einschätzung. Infolge dessen betrieben sie auch keine «IKT-Mittel der Sicherheitsstufe „hoher Schutz“ oder „sehr hoher Schutz“».

**Artikel 22** Sicherheitsanforderungen der Sicherheitsstufe «Grundschutz»

Für insecor ist unklar, wer die Mindestanforderungen festlege. Absatz 1 stehe im Widerspruch zum gesetzlichen Auftrag des ISB, welches die Mindestanforderungen für IKT-Mittel für die Bundesverwaltung vorgeben soll (vgl. z.B. Art. 17 Abs. 1 Bst. d BinfV). Andererseits sollen nach Absatz 2 „diese Mindestanforderungen“ für sämtliche IKT-Mittel erfüllt sein. Wer überprüft deren Einhaltung? Und gestützt auf welche Grundlagen bzw. Anforderungen? Dies müsste noch entsprechend präzisiert werden.

Absatz 1 sollte nach it-rm mit folgendem Satz ergänzt werden. „Dabei sind die Mindeststandards einzuhalten, welche von der Koordinationsstelle festgelegt worden sind.“ Es seien auch Mindeststandards für die entsprechenden Schutzbedürfnisse durch die Koordinationsstelle festzulegen.

LB schlägt, ungeachtet von Bedenken betreffend von Eingriffen in die Souveränität der Kantone (Art. 3 BV) sowie des Grundsatzes der Subsidiarität (Art. 5a und 43a BV), für den Bereich der IKT Infrastruktur vor, dass der Fachstelle des Bundes die Kompetenz eingeräumt wird, die Anforderungen an alle drei Sicherheitsstufen von IKT-Mitteln für das gesamte Gebiet der Schweiz einheitlich festzulegen, mindestens durch Herausgabe von Standards, Wegleitungen, Empfehlungen, Checklisten oder Mindestanforderungen. Artikel 88 ISG würde dafür eine Grundlage schaffen.

**Artikel 23** Informationssicherheitskonzept

Die Mindestinhalte der Informationssicherheitskonzepte sollten nach Erachten von SO im Gesetz oder zumindest in der Verordnung konkretisiert werden.

Für privatim lässt der Gesetzestext völlig offen, was ein Informationssicherheitskonzept konkret sei, welche (Mindest-)Inhalte es vorweisen sollte und welche Wirkungen mit einem Informationssicherheitskonzept verknüpft sein sollen. Es sei daher zu prüfen, ob im Gesetz, in der Verordnung zum ISG oder in der Botschaft konkretisiert werden müsse, was in einem Informationssicherheitskonzept enthalten sein soll — andernfalls könne keine bundesweite Einheit bezüglich der Informationssicherheit garantiert werden und Artikel 23 ISG bleibe ein Lippenbekenntnis.

Clusis fragt sich, warum die Risikoanalyse und das Sicherheitskonzept nur für die Sicherheitskategorien «erhöhter Schutz und sehr hoher Schutz» vorgesehen sind. Die Risikoanalyse muss die zu ergreifenden Sicherheitsmassnahmen abgestuft nach den Kategorien .bestimmen

Weil vorgängig keine Begriffe definiert wurden, ist für insecor somit auch unklar, wie vorliegend das Informationssicherheitskonzept zu verstehen sei. Soll darin nur die „Informationssicherheit“ betrachtet werden? Was bedeutet dies genau? Fällt der Datenschutz nicht mehr unter diese Verpflichtung wie dies in der HERMES Projektmanagementmethode für Informationssysteme bzw. „ISDS-Konzepte“ vorgesehen sei? Wie soll auf Kantons-und Gemeindeebene mit diesen Vorgaben umgegangen bzw. entsprechende Massnahmen umgesetzt werden (vgl. Artikel 89)? Diese Fragen müssten noch eingehender geklärt werden.

Der ETH-Rat weist darauf hin, dass einige Institutionen bereits heute über ein Informationssicherheitskonzept verfügten.

**Artikel 24** Konformitäts- und Wirksamkeitsprüfungen

Privatim stellt den Antrag die Konformitäts- und Wirksamkeitsprüfungen des Artikel 24 ISG mit Konsequenzen zu ergänzen. Es sei zu regeln oder zumindest in der Botschaft zu erläutern, ob neben der Effizienz auch die Effektivität der beschlossenen und eingeführten Massnahmen geprüft werden müssten (vgl. dazu Artikel 4 Absatz 4 ISG). Ebenso wäre zu regeln, was geschehen solle, wenn die Resultate dieser Prüfungen ignoriert würden.

Nach Erachten von LB, sollten die Anforderungen an die Sicherheit von IKT-Mitteln auch dadurch erfüllt werden können, dass zertifizierte Produkte eingesetzt werden. Für solche nach international anerkannten Sicherheitsstandards wie die “Common Criteria“ in einem definierten Verfahren zertifizierte Produkte sollte nicht eine zusätzliche Konformitäts- und Wirksamkeitsprüfung erforderlich sein. Die Pflicht zur Inventarisierung der IKT Mittel dürfte hingegen angesichts des ständigen Wechsels der eingesetzten Mittel und des steigenden Anteils von geschäftlich genutzten privaten Endgeräten einen erheblichen organisatorischen und administrativen Aufwand zur Folge haben.

**Artikel 25** Sicherheitsfreigabe

Für TG ist es nicht verständlich, weshalb die Behörde mit der Sicherheitsfreigabe das Restrisiko akzeptieren darf. Damit nicht bedenkenlos mit ausgestellten Sicherheitsfreigaben umgegangen werde, sollte auf den zweiten Absatz verzichtet werden. Wenn doch schon in Artikel 23 des Entwurfes ISG erwähnt werde, dass das Sicherheitskonzept laufend aktualisiert werden müsse, dürfe nicht zwei Artikel später sinngemäss festgehalten werden, dass man bei Sicherheitsfreigaben nicht mehr an die immer bestehenden Restrisiken denken müsse und diese einfach akzeptieren solle. Die Bestimmung, wonach das Restrisiko akzeptiert werde, sollte ersatzlos gestrichen werden, da sonst die Informations- und Kommunikationstechnologie zu leichtfertig und zu bedenkenlos verwendet werde, wenn man sich im Sinne des Entwurfes einfach auf eine Sicherheitsfreigabe abstützen dürfte und deshalb nicht weiter an Risiken denken müsste.

**Artikel 27** Sicherheit beim Betrieb

Pour VD Il serait utile de préciser que la sécurité traite des quatre critères de confidentialité, d'intégrité, de disponibilité et de traçabilité.

Nach Ansicht von FER sind die Begriffe Lagerung und Schutz angesichts des einem Technikers notwendigen Zugangs stillschweigend eingeschlossen. Aufgrund der festgestellten Diebstähle können diese zwei Punkte weggelassen werden.

**Artikel 28 / Artikel 29** Personelle Massnahmen

Dieser Artikel geht dem ETH-Rat hinsichtlich Auftragnehmer, die mit Informationen oder IKT-Mitteln der ETH bzw. des Bundes umgehen sollen, zu weit. In der Praxis würde das bedeuten, dass die ETH bei der Auftragsvergabe an Dritte (Unternehmen) für die stufengerechte Aus- und Weiterbildung der Auftragnehmer im Bereich Informationssicherheit sorgen müsste. Eine Umsetzung dieser Regelung in der Praxis würde finanzielle Implikationen haben.

**Artikel 29** Restriktive Erteilung von Berechtigungen

TG begrüsst es, dass hier nicht verschiedene Kategorien von generellen Sicherheitsüberprüfungen stattfinden, sondern dass nur diejenigen Berechtigungen erteilt werden, welche zur Aufgabenerfüllung erforderlich sind. Allenfalls wäre es sinnvoll, den Zeitraum der Sicher-

heitsüberprüfung auch hier analog zu Artikel 50 des Entwurfes ISG betreffend der Personensicherheitsüberprüfung klar festzusetzen. In Absatz 2 werde erwähnt, dass die Berechtigungen nur schon bei „Anhaltspunkten“ für eine Gefährdung der Informationssicherheit entzogen werden können. Dies könnte für die betroffenen Personen eine sehr harte Massnahme darstellen, da allenfalls im konkreten Fall bei genauerer Hinsicht später ausgeschlossen werden könne, dass - trotz Vorliegen von Anhaltspunkten - eine effektive Gefahr bestehe. Heirate beispielsweise eine überprüfte Person einen Ehegatten aus einem Krisengebiet, kann dies zunächst einen Anhaltspunkt für eine Gefährdung darstellen. Anschliessend sollte aber die Möglichkeit bestehen, dass trotz Vorliegen von Anhaltspunkten der klare Beweis erbracht werden könne, dass eine konkrete Gefährdung ausgeschlossen sei. Aufgrund des rechtlichen Grundsatzes von "audiatur et altera pars", bzw. dem Anspruch auf das rechtliche Gehör, müsse bei personellen Massnahmen die Möglichkeit bestehen, dass die betroffene Person nach dem vorläufigen Entzug der Berechtigung in einem umfassenden Verfahren darlegen könne, dass bei ihr trotz vermuteter Anhaltspunkte weiterhin eben gerade keine Sicherheitsgefährdung vorliege.

Die CVP befürwortet, dass Berechtigungen für den Umgang mit Informationen und IKT-Mitteln restriktiv erteilt werden und dass diese Berechtigungen regelmässig auf ihre Gültigkeit überprüft werden.

Crusis begrüsst den Inhalt dieses Artikels, aber warum wird der Entzug der Berechtigungen nicht ausdrücklich als automatisch erwähnt. Wenn dies der Fall sein soll, sollte dies ausdrücklich gesagt werden.

**Artikel 31** Sicherheitszonen

Für SO sollte aus Datenschutzüberlegungen bei den biometrischen Verifikationsmethoden klar gestellt werden (entweder im Gesetzestext oder zumindest in den Erläuterungen), dass nicht die Rohdaten selbst gespeichert werden dürfen.

Aus Sicht TG sollte die Verwendung von biometrischen Verifikationsmethoden genauer geregelt werden. So sei insbesondere festzulegen, wie lange entsprechende Profile aufbewahrt werden dürften. Bei der Erlaubnis zu Taschen- und Personenkontrollen könnten faktisch Amts- und Berufsgeheimnisse verletzt werden. Zudem stelle diese Bestimmung eine grosse Gefahr für die Sicherheit dar, da allenfalls bei einer Überprüfung der Effekten höchster Geheimnisträger das sicherheitsmässig nicht entsprechend hoch qualifizierte Kontrollpersonal unweigerlich von Geheimnissen Kenntnis erhalten könnte, welche nicht der eigenen Sicherheitsstufe des Kontrollpersonals genügten. Die Erlaubnis zu Personen- und Taschenkontrollen, wozu zukünftig auch die Kontrolle (und die Gefahr der faktischen Manipulation) von Laptops gehören könnte, müsse deshalb unbedingt genauer umschrieben werden, damit der Zweck des Gesetzes nicht obsolet werde. Unangemeldete Raumkontrollen des Personals müssten ebenso näher umschrieben werden, zumal dadurch allenfalls private Wohnräume betroffen sein könnten, was bei einer generellen Kontrollzulässigkeit zu einem Konflikt mit der Achtung des Privat- und Familienlebens von Artikel 8 EMRK führen könnte.

TI sieht die Vorgaben unter Absatz 3 Buchstabe a als einschränkend an, da sie nur die derzeit verwendete Technik berücksichtigen. Für TI wäre daher eine Änderung der Formulierung angebracht, so dass möglichen künftigen technologischen Entwicklungen Rechnung getragen werden könne. Das hätte den Vorteil, dass eine Gesetzesänderung nicht mehr notwendig wäre.

Für VD sind die Voraussetzungen für Massnahmen nach Absatz 4 im Sinne der Verhältnismässigkeit zu präzisieren.

Für die SP sollte die Verwendung von biometrischen Verifikationsmethoden im Sinne von Absatz 3 Buchstabe a dieser Bestimmung genauer geregelt werden. So sei insbesondere festzulegen, wie lange entsprechende Profile aufbewahrt werden dürfen. Bei der Erlaubnis zu Taschen- und Personenkontrollen nach Absatz 3 Buchstabe d könnten faktisch Amts- und Berufsgeheimnisse verletzt werden. Die Erlaubnis zu Personen- und Taschenkontrollen müsse deshalb näher umschrieben werden, damit der Zweck des Gesetzes nicht obsolet werde. Unangemeldete Raumkontrollen des Personals im Sinne von Absatz 3 Buchstabe e

müssten 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 Artikel 8 der Europäischen Menschenrechtskonvention führen könnte.

Privatim beantragt zumindest in der Botschaft zu Artikel 31 Absatz 3 Buchstabe a ISG zu ergänzen, dass für die biometrischen Verifikationsmethoden ausschliesslich Hash-Werte der jeweiligen Daten und nicht die Rohdaten selber abgelegt werden dürfen.

Clusis begrüsst diesen Artikel, der eine genügende Rechtsgrundlage für die Bearbeitung von Personendaten, insbesondere besonders schützenswerte, schafft.

### 3. Kapitel: Personensicherheitsprüfungen

#### Allgemein

LU stellt im Kapitel Personensicherheitsprüfungen eine gewisse Überreglementierung fest, welche die Kantone dazu anhalte, verschiedene neue und vor allem kostspielige Prozesse einzuführen. LU beantragt daher eine generelle Überarbeitung des Kapitels mit dem Ziel, den Verwaltungsaufwand für die Kantone zu reduzieren.

UR anerkennt die Wichtigkeit von Personensicherheitsprüfungen, da eine der heikelsten und intensivsten Sicherheitsbedrohungen dann entstehen könne, wenn Personen, die über Zugang zu höher klassifizierten Informationen verfügen, Verrat oder Sabotage üben. Sensitive Funktionen sollten deshalb ausschliesslich Personen anvertraut werden, die möglichst weitgehend Gewähr dafür bieten, dass sie das ihnen entgegengebrachte Vertrauen nicht missbrauchen.

Die Reduzierung der Prüfstufen hat für SG keine Auswirkungen auf die Mitwirkung der Kantonspolizei im Personensicherheitsprüfungsverfahren. Die Mitwirkung der Kantonspolizei sei unter Artikel 39 ISG geregelt und unterscheide sich nicht wesentlich von den heute geltenden Bestimmungen im Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (SR 120). Nachdem die heute geltenden Bestimmungen überzeugten, hat SG keine grundsätzlichen Einwände gegen die neuen Bestimmungen zur Personensicherheitsprüfung.

Die SP regt an, Artikel 20 Absatz 1 BWIS in modifizierter Form ins ISG zu übernehmen: „Artikel 32$^{bis}$ 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.“ Da es um Daten gehe, die aus Sicht des Daten- und Persönlichkeitsschutzes äusserst sensitiv seien, ist für die SP eine ausreichend hohe regulatorische Dichte in diesem Bereich zwingend. Auch sei wie bisher explizit auszuschliessen, dass Fichen über die politische Betätigung angelegt würden.

Für CP und CVAM ist das 3. Kapitel des ISG (Art. 32-55), das die Voraussetzungen und das Verfahren der Personensicherheitsprüfung regelt, ein echter Gewinn für die Garantie des Persönlichkeitsrechts und die Rechtssicherheit für Personen im sensiblen Bereich der Informationssicherheit, wo das öffentlichen Interesse ein gewisses Gewicht bis Übergewicht hat.

Privatim begrüsst die klare Regelung der Personensicherheitsprüfungen (PSP) und die klare Regelung der Informationssysteme. Allerdings sieht privatim in zwei Punkten dringenden Klärungsbedarf (vgl. Bemerkungen zu Artikel 47 und 53).

Insecor begrüsst eine einheitliche und klare Regelung der Personensicherheitsprüfung.

LB bemerkt, dass im Bereich der Personensicherheitsüberprüfung die Anforderungen aus dem Persönlichkeits- und Datenschutzes beachtet werden müssten, da die Personensicherheitsüberprüfung in die grundrechtlich geschützte Privatsphäre (Artikel 13 BV) der betroffenen Personen eingreife.

Für den ETH-Rat ist unklar, ob die Bestimmungen im 3. Kapitel nur für die verpflichteten Behörden Anwendung finden würden (bei wörtlicher Auslegung könne dies so verstanden werden) und somit die verpflichteten Organisationen gar nicht unter dieses Kapitel fallen würden. Gemäss Artikel 34 Absatz 1 Buchstabe b könne sich die Situation ergeben, dass bei einem sicherheitsempfindlichen Auftrag Angestellte des zu beauftragenden Unternehmens der PSP unterliegten, die Auftrag gebenden Mitarbeitenden einer Institution des ETH-Bereichs aber nicht. Da gemäss Artikel 38 Absatz 3 und Artikel 46 Absatz 2 vor der Auftragsvergabe das Ergebnis der PSP abgewartet werden müsse, kann dies für die betroffene Institution des ETH-Bereichs zu erheblichen Verzögerungen bei der Auftragsvergabe führen. Für die PSP sei eine (kurze) Maximaldauer festzuschreiben, um Auftragsvergaben nicht unverhältnismässig zu verzögern.

**Artikel 33** Liste der Funktionen mit sicherheitsempfindlicher Tätigkeit

Das BGer macht darauf aufmerksam, dass dieser Artikel für das BGer wesentlich sei und deshalb nicht zu seinem Nachteil verändert werden dürfe.

**Artikel 34** Zu prüfende Personen

Wenn schon bundrechtlich der Bundesrat und der „Bundeskanzler“ von einer Personensicherheitsüberprüfung ausschlossen würden, macht es für TG keinen Sinn, in den Kantonen bloss die Regierungsmitglieder von der Prüfung auszunehmen. Die Bestimmung vergesse, dass in den Kantonen die Staatsschreiber auch als Magistratspersonen gelten und deshalb ebenfalls von der Überprüfung auszunehmen seien. Andernfalls könnten die Regierungsratsgeschäfte gar nicht durchgeführt werden.

Das BGer macht darauf aufmerksam, dass dieser Artikel für das BGer wesentlich sei und deshalb nicht zu seinem Nachteil verändert werden dürfe.

**Artikel 33 i.V.m. Artikel 34**

Der ETH-Rat weist darauf hin, dass während Artikel 34 Absatz 1 Buchstabe b auch Personen in eine Personensicherheitsprüfung miteinbeziehe, welche für die verpflichteten Behörden oder Organisationen tätig seien, Artikel 33 wiederum nur die verpflichteten Behörden in der Pflicht sehe, für ihren Zuständigkeitsbereich eine Liste der Funktionen zu verfassen, für deren Aufgabenerfüllung die Ausübung einer sicherheitsempfindlichen Tätigkeit erforderlich ist. Dies könne zur eigentümlichen Situation führen, dass bei einem sicherheitsempfindlichen Auftrag Angestellte des zu beauftragenden Unternehmens der PSP unterliegen, die Auftrag gebenden ETH-Mitarbeitenden hingegen nicht. Artikel 33 sei noch einmal zu überdenken. Die Verordnung zur Personensicherheitsprüfung (SR 120.4) führe möglicherweise just diese Liste der Funktionen mit sicherheitsempfindlicher Tätigkeit weiter aus bzw. die gemäss Artikel 33 verlangte Liste sollte mit der in der PSPV genannten Liste möglicherweise identisch sein. Der ETH-Rat schlägt vor, falls die Liste der Funktionen mit sicherheitsempfindlicher Tätigkeit mit derjenigen in der PSPV identisch sei, sei dies im ISG entsprechend klarzumachen bzw. habe die PSPV ebenfalls auf Artikel 33 ISG zu verweisen.

**Artikel 35** Prüfstufen

Bei Personen mit Zugang zu GEHEIM klassifizierten Informationen gehört aus Sicht des NDB die standardmässig durchgeführte persönliche Befragung durch entsprechend geschultes Personal ausnahmslos zu jeder PSP. Der Bericht zum ISG halte korrekterweise fest, dass eine der heikelsten und intensivsten Sicherheitsbedrohungen dann entstehe, wenn Personen Verrat oder Sabotage übten (Bericht S. 20). Solche Bedrohungen liessen sich im Vorfeld in aller Regel nicht alleine aus der Abfrage von Registern erkennen, sondern bedingten die vertiefte Auseinandersetzung mit der zu prüfenden Person. Der Verzicht auf diese Massnahme stehe in Widerspruch zur eben zitierten Analyse und bedeute eine markante Einbusse bei der Möglichkeit, Sicherheitsrisiken frühzeitig zu erkennen. Der NDB verlangt daher die Durchführung von persönlichen Befragungen als Standardmassnahme bei Prüfungen nach Artikel 35 Buchstabe b.

**Artikel 37** Einwilligung

BE beantragt, Artikel 37 mit einem neuen Absatz 3 wie folgt zu ergänzen: „[3] Die Kantone können durch Gesetz vorsehen, dass Personensicherheitsprüfungen auch für andere Funktionen ohne Einwilligung der zu prüfenden Personen durchgeführt werden können." Die Kantone sollten die Möglichkeit haben, auch in anderen sensiblen Bereichen der Kantons- oder Gemeindeverwaltungen, z.B. der Polizei, eine Personensicherheitsüberprüfung ohne die Einwilligung der zu prüfenden Person vorzusehen (z.B. für den Zugang zu wichtigen Infrastrukturen oder klassifizierten Daten).

TI möchte das Prinzip der Regelung, welches er befürwortet, nicht in Frage stellen. TI fragt sich nur, welche Folgen es haben könnte, wenn die Person, welche der Prüfung unterstellt werden soll, ihre Einwilligung verweigert.

Für Clusis ist es klar, dass eine Sicherheitskontrolle ohne die Zustimmung der betroffenen Person nicht durchgeführt werden kann. Es müsse aber präzisiert werden, dass die Beschäftigung einer solchen Person mit sicherheitssensiblen Aufgaben voraussetzt, dass die Sicherheitsprüfung durchgeführt wurde. Eine Formulierung wie: «eine Sicherheitskontrolle kann vor jeder Auftragsvergabe durchgeführt werden, sofern die Kandidaten vorher ausreichend informiert werden.

LB bemerkt, dass nach den Grundsätzen des Persönlichkeits- und Datenschutzes (Artikel 4 Absatz 5 DSG) die Einwilligung die ausreichende vorgängige Information der betroffenen Person über die Personensicherheitsprüfung und die dabei gemäss Artikel 39 ISG erhobenen Daten voraussetze. Da die erhobenen Daten auch besonders schützenswerte Daten im Sinne Artikel 3 Buchstabe e DSG umfassten, müsse die Einwilligung ausdrücklich abgegeben werden.

**Artikel 38** Zeitpunkt der Personensicherheitsprüfung

Dem ETH-Rat fehlt im jetzigen Vernehmlassungsentwurf eine Regelung, welche klarstellt, wie vorzugehen ist bzw. was gilt, falls eine Personensicherheitsprüfung (PSP) nicht vorgängig erfolgt ist bzw. diese vor Zuteilung einer Funktion an eine Person nicht erfolgt ist. Gerade im Forschungsbereich könnten Personen in Forschungsprojekten erst zu einem späteren Zeitpunkt bzw. erst kurzfristig und daher ohne vorgängige Kontrollmöglichkeit mit Aufgaben betraut werden, deren sicherheitsrelevanter Aspekt nicht auf den ersten Blick ersichtlich sei und auch von den beteiligten Projektpartnern nicht schon vorgängig als solcher erkannt worden sei. Das Fehlen einer klaren Regelung für die Durchführung einer nachträglichen PSP und insbesondere der Konsequenzen daraus werde in der Praxis unweigerlich zu einem Konflikt zwischen den personalrechtlichen Ansprüchen der betroffenen Person und den sicherheitspolitischen Absichten des ISG mit einer zeitlich unbefriedigenden Dauer führen. Der ETH-Rat schlägt vor, dass die PSP in diesen Fällen nachträglich mit Einwilligung der entsprechenden Person zu erfolgen habe. Verweigere die Person die Einwilligung für eine PSP, so solle die zuständige verpflichtete Behörde ohne finanzielle, personalrechtliche oder anderweitige Konsequenzen berechtigt sein, die entsprechende Person von einer Funktion zu entheben bzw. die Ausführung einer Tätigkeit zu untersagen, für welche eine PSP vorgesehen wäre.

**Artikel 39** Datenerhebung

Für VD müssen die kantonalen Polizei- und Nachrichtendienste wie heute mit der Durchführung der Personensicherheitsprüfung beauftragt werden; sie müssen berechtigt sein, auf die Gesamtheit der in Artikel 39 genannten Daten zugreifen zu können.

NE stellt fest, dass eine Steuerbehörde berechtigt sein kann, Steuergeheimnisse im Rahmen einer Personensicherheitsprüfung (PSP) weitergeben, soweit dies eine rechtliche Grundlage dies ausdrücklich vorsieht.

Die SP regt an, die bisher im BWIS enthaltene Einschränkung beizubehalten, Drittpersonen nur befragen zu dürfen, wenn die betroffene Person zugestimmt hat. Die im ISG Artikel 39 Absatz 2 Buchstabe c vorgeschlagene vollständige Aushebelung des Bankgeheimnisses lehnt die SP 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.

Clusis begrüsst diesen Artikel, der eine genügende gesetzliche Grundlage für die Bearbeitung von Personendaten, insbesondere auch von besonders schützenswerten darstellt.

Der NDB verlangt, dass auf Ebene der Ausführungsbestimmungen festzuhalten sei, dass der Informationsaustausch dann über den NDB stattzufinden habe, wenn die ausländische Dienststelle Teil einer nachrichtendienstlichen Organisation sei.

**Artikel 40** Kostentragung

AI beantragt, Artikel 40 mit dem Vorbehalt zu versehen, dass der Bund die Kosten für Sicherheitsüberprüfungen, die in seinem Auftrag ausgeführt würden, vollständig trage. Die Aufwendungen der Kantone, die ihnen mit Tätigkeiten anfallen, die sie im Auftrag des Bundes ausübten, müssten vollständig entschädigt werden. Dies sollte im Gesetz ausdrücklich und unmissverständlich so festgehalten werden.

Für TG ist bei der Kostentragung der Grundsatz zu erwähnen, dass die Kosten für eine Sicherheitsüberprüfung nicht der zu überprüfenden Privatperson angelastet werden dürften, da sonst die Gefahr bestehe, dass Sicherheitsüberprüfungen in finanzieller Rücksicht auf die einem allenfalls bekannten Personen möglichst selten vorgenommen würden.

TI weist darauf hin, dass für die Grundsicherheitsprüfung die zuständigen Fachstellen für Personensicherheitsprüfungen zur Beurteilung des Sicherheitsrisikos Daten über die zu prüfende Person erheben können, indem sie auch auf diverse Register zugreifen können (s. Bst. d und e). Insbesondere für die Polizei, die über zahlreiche Datenbanken mit sehr vielen Informationen verfügt (z.B. Kantonsjournal), sei eine genaue Definition dieses Begriffs unerlässlich, damit die Verwendung von Daten, welche mit dem Zweck nichts zu tun haben, vermieden werde.

**Artikel 41** Einstellung

TG vermisst eine Regelung darüber, was mit den erhobenen Daten bei erfolgreicher Sicherheitsüberprüfung geschehen soll. Es werde beispielsweise nicht geregelt, wie lange diese Daten aufbewahrt werden dürften. Dies sollte gesetzlich geregelt werden. Ebenso sollte das Recht auf eine umfassende Löschung alter Daten erwähnt werden, damit Personen, welche früher die Vorgaben nicht erfüllten, zu einer späteren Zeit allenfalls wieder die Gelegenheit zu einer Neubeurteilung erhielten.

**Artikel 42** Sicherheitsrisiko

Die CVP spricht sich für eine Definition, was als Sicherheitsrisiko anzusehen ist, aus.

Für LB ist nicht ganz klar, wie das Sicherheitsrisiko beurteilt werde, wenn die zu prüfende Person ihre Einwilligung zur erstmaligen Prüfung oder zu deren Wiederholung nach Artikel 50 ISG verweigere, zurückziehe oder an der Prüfung nicht mitwirke (Artikel 41 Absatz 1 ISG): Die Person gilt in diesen Fällen als “nicht geprüft“ (Artikel 41 Absatz 2 Satz 2 ISG): Kann die betreffende Person dann für eine sicherheitsempfindliche Tätigkeit nach Artikel 33 ISG überhaupt nicht eingesetzt werden, bzw. ist sie bei Weigerung der Wiederholung der Prüfung aus dieser Tätigkeit zu entfernen? Die Entscheidung über den Einsatz der betreffenden Person obliegt dann offenbar gemäss Artikel 46/47 ISG der übertragenden Stelle

**Artikel 43** Ergebnis der Beurteilung

Artikel 43 Absatz 1 Buchstabe d ist für TI unbefriedigend, denn nicht einmal durch den Kommentar im Erläuternden Bericht werde klar, ob aufgrund einer solchen Erklärung nach Verstreichen einer bestimmten Zeitspanne das Ergebnis der Beurteilung neuerlich geprüft wird.

**Artikel 44** Mitteilung der Beurteilung

ZG beantragt, die «Kann-Bestimmung» von Artikel 44 Absatz 4 durch eine «Muss-Bestimmung» zu ersetzen. Bei potentiell gewalttätigen Personen seien die für das Überlas-

sen oder den Entzug der persönlichen Armeewaffe zuständigen Stellen zwingend zu informieren. Die Meldung derartiger Personen dürfe nicht dem Ermessen der prüfenden Stelle überlassen werden. Die damit verbundenen Risiken wären viel zu gross.

SG weist darauf hin, dass Artikel 14 des Militärgesetzes (SR 510.10) auf den im erläuternden Bericht auf S. 58, Bemerkungen zu Artikel 44 Absatz 3 ISG, verwiesen werde, nicht mehr existiere und per 1. Januar 2004 aufgehoben worden sei.

**Artikel 47** Mitteilungspflicht

Die Erklärungen der Fachstellen PSP haben empfehlenden Charakter (Artikel 46 ISG). Gleichwohl hat die übertragende Stelle der zuständigen Fachstelle PSP mitzuteilen, ob sie die Ausübung von sicherheitsempfindlichen Tätigkeiten einer Person überträgt oder nicht und ob bei der Übertragung der Tätigkeiten von allfälligen von der Fachstelle PSP empfohlenen Auflagen abgewichen wird. Grund für diese Mitteilungspflicht sei, so die Erläuterungen zu Artikel 47 ISG, dass die Fachstelle PSP einen Überblick über die Praxis der übertragenden Stellen behalte und die notwendigen Lehren ziehe. Diese Argumentation ist für BS nicht schlüssig: Weshalb sollten die Fachstellen PSP, die ihre Beurteilung anhand objektiver Kriterien vornehmen sollen, ihre Praxis anpassen, wenn sie feststellen, dass die übertragenden Stellen ihre Empfehlungen nicht oder jeweils nur teilweise befolgen? Es bestehe die Gefahr, dass die Fachstellen PSP ihre Prüfungen nicht mehr mit der notwendigen Objektivität ausführten. Es sei sogar denkbar, dass dies dazu führe, dass sich die Fachstelle PSP nach den Wünschen und Bedürfnissen der übertragenden Stellen richte. Dies wiederum würde zu neuen Sicherheitsrisiken führen.

Für privatim ist nicht schlüssig, weshalb die Fachstellen PSP, die ihre Beurteilung anhand objektiver Kriterien vornehmen sollen, ihre Praxis anpassen sollten, wenn sie feststellen, dass die übertragenden Stellen ihre Empfehlungen nicht oder jeweils nur teilweise befolgen. Führt dies letztendlich nicht dazu, dass die Fachstellen PSP sich den Wünschen und Bedürfnissen der übertragenden Stellen beugen und ihre Kernaufgabe, die Beurteilung eines allfälligen Sicherheitsrisikos, welches von einer Person ausgehen kann, nicht mehr mit der notwendigen Objektivität ausführen? Sollte den Fachstellen PSP nicht vielmehr verbindlichere Mittel an die Hand gegeben werden, um bei allfältigen Sicherheitsrisiken wirksam agieren und nicht bloss mit Empfehlungen handeln zu können? Diese Fragen müssten in den Erläuterungen zu Artikel 46 ff geklärt werden.

Die Nationalbank steht der in Artikel 47 statuierten schriftlichen Mitteilungspflicht, wenn die für die Übertragung der sicherheitsempfindlichen Tätigkeit zuständige Stelle sich über eine Risiko- oder Feststellungserklärung der Prüfstelle hinwegsetzt oder von empfohlenen Auflagen abweicht, kritisch gegenüber und lehnt sie als unzulässigen Eingriff in die Vollzugsautonomie der Behörden ab. Diese Mitteilungspflicht stehe auch im Widerspruch zu Artikel 46, wonach die Erklärungen der Prüfstelle (lediglich) empfehlenden Charakter haben und der Entscheid über die Übertragung sicherheitsempfindlicher Aufgaben ausschliesslich bei der übertragenden Stelle liege.

**Artikel 50** Wiederholung

TI hält die angegebenen Zeiträume für die Wiederholung der Sicherheitsprüfung für zu weit gefasst. TI schlägt vor, die Grundsicherheitsprüfungen innerhalb von 5 Jahren und die erweiterte Prüfung innerhalb von 3 Jahren durchzuführen.

**Artikel 51** Rechtsschutz

Die Regelung, wonach die geprüfte Person innert 30 Tagen nach Erhalt der Erklärung eine Verfügung der Fachstelle PSP verlangen könne, läuft aus Sicht von TG der vorherigen Bestimmung entgegen, wonach nur während zehn Tagen in die Prüfungsunterlagen Einsicht genommen werden dürfe. Wer ein Rechtmittel ergreife, sollte während der gesamten Rechtsmittelfrist in die Akten Einblick nehmen dürfen. Die in Absatz 1 genannte Frist von zehn Tagen sei somit auf 30 Tage auszuweiten. Es mache keinen Sinn, wenn eine Person beispielsweise nach zwei Wochen einen Anwalt beiziehen will, dieser dann aber, weil die Einsichtsfrist von 10 Tagen bereits abgelaufen ist, ein Rechtsmittel einlegt, ohne die Akten kennen zu dürfen.

Mit Bezug auf die Aufsichtsbehörde bzw. die Bundesanwaltschaft, ergibt sich für AB-BA aus dem Gesetzestext nicht bei welcher Behörde eine Verfügung der Prüfstelle angefochten werden könne.

Das BVGer kann versichern, dass es nichts gegen die neue Konzeption des Rechtsschutzes im Sinne von Artikel 51 Absatz 3 ISG einzuwenden habe.

**Artikel 52** Informationssystem zur Personensicherheitsprüfung

Clusis begrüsst diesen Artikel, der eine genügende gesetzliche Grundlage für die Bearbeitung von Personendaten, insbesondere auch von besonders schützenswerten, schafft.

Für LB ist gemäss der Formulierung von Artikel 52 Absatz 1 ISG nicht ganz klar, ob das von den PSP Fachstellen einzusetzende “Informationssystem“ nach einer einheitlichen, vom Bund vorgegebenen Struktur aufgebaut wird - was den Zugriff durch die gemäss Artikel 53 ISG berechtigten Stellen erleichtern würde - oder der ISG es den PSP Fachstellen überlässt, ein Informationssystem nach eigenen Vorgaben einzurichten und zu betreiben.

LB hat aus Gründen des Datenschutzes erhebliche Bedenken gegen die Aufnahme der AHV-Versichertennummer in das Informationssystem, weil im System ja gemäss Artikel 52 Absatz 4 Buchstabe a ISG bereits Daten zur Identität der erfassten Personen enthalten sind und die Aufnahme der AHV Versichertennummer ausserhalb des Bereichs der Sozialversicherung gemäss Artikel 36 Absatz. 4 Buchstabe c DSG und Artikel 50e AHVG strengen Auflagen und Beschränkungen unterliegt, weil sie die Zusammenführung von Informationen betroffener Personen und das sog. “Profiling“ erleichtert. Es besteht aus Sicht von LB kein berechtigtes Interesse, dass die AHV-Versichertennummer in den Informationssystemen zur Personensicherheitsprüfung aufgenommen wird: Die Erleichterung des Zugriffs auf erfasste Personen gemäss Artikel 53 ISG ist kein ausreichender Rechtfertigungsgrund für diese zusätzliche unter dem Gesichtspunkt des Datenschutzes fragwürdige Verwendung der AHV-Versichertennummer ausserhalb des Bereichs der Sozialversicherung. Im Übrigen empfiehlt LB in Analogie zu Artikel 77 Absatz 4 ISG, dass Artikel 52 Absatz 2 ISG um die “Verantwortung der Fachstelle PSP für die Sicherheit des Informationssystems“ ergänzt wird, denn für die im Informationssystem der Fachstelle PSP gespeicherten Personendaten bestehe im Vergleich zu den im Informationssystem über die Ergebnisse des Betriebssicherheitsverfahrens gespeicherten Daten höhere Anforderungen für die Sicherheit.

**Artikel 53** Datenbekanntgabe

Die Bestimmung von Artikel 53 Absatz 2 Buchstabe c. Ziff. 1 des Entwurfes ISG, wonach der Führungsstab der Armee zur Kontrolle des Zutritts zu Sicherheitszonen über eine Schnittstelle zum Informationssystem verfügen solle, geht TG zu weit. So handle es sich bei Schutzzone 1 nach Artikel 3 der Anlageschutzverordnung (SR 510.518.1) um Anlagen, welche teilweise sogar frei zugänglich seien. Der Führungsstab der Armee sollte somit erst ab Schutzzone 2 die Berechtigung erhalten, auf die Daten der Personensicherheitsüberprüfung zugreifen zu können. Dies sei entsprechend anzupassen. Ebenso lasse sich die Frage stellen, inwieweit der Führungsstab der Armee zur Durchführung der Rekrutierung der Stellungspflichtigen über einen entsprechenden Zugang zu den Personenüberprüfungen verfügen soll, zumal es sich bei den Stellungspflichtigen meist um junge Personen handle, welche vorgängig wohl kaum schon eine Personensicherheitsüberprüfung absolviert hätten.

Für privatim geht aus dem Erläuternden Bericht nicht hervor, weshalb die Kontrollbehörde ganz grundsätzlich auf «scharfe» Personendaten zugreifen können muss, um ihre Aufgabe zu erfüllen: Kann die Kontrolle über die Durchführung der PSP nicht auch anhand anonymisierter Daten erfolgen? Bestünde nicht allenfalls die Möglichkeit, nur in Ausnahmefällen auf «scharfe» Daten zurückzugreifen, und im Regelfall die Kontrolltätigkeit mit Datensätzen ohne weiteren Personenbezug vorzunehmen? Diese Fragen gelte es zu klären.

Clusis begrüsst diesen Artikel, der eine genügende gesetzliche Grundlage für die Bearbeitung von Personendaten, insbesondere auch von besonders schützenswerten, schafft. Die Übertragung elektronischer Daten muss auf gesicherte Weise erfolgen. Dies muss noch präzisiert werden.

**Artikel 54** Datenaufbewahrung und -vernichtung

Das bereits heute bestehende Informationssystem zur Personensicherheitsprüfung hat sich gemäss SG bewährt. Betreffend die Löschfristen in Artikel 54 Absatz 2 ISG gelte es allerdings zu berücksichtigen, dass dadurch die vorgelagerten Löschfristen faktisch verlängert würden. Aus Datenschutzgründen sei es wichtig, dass sich der Gesetzgeber dieser faktischen Fristverlängerung bewusst sei. Entsprechend regt SG an, diese Problematik im Bericht zu den Ergebnissen der Vernehmlassung bzw. in der zu erstellenden Botschaft ausdrücklich zu erwähnen und allenfalls zu bewerten.

Für TG ist Absatz 6 nach Absatz 2 anzufügen, damit sichergestellt werde, dass nicht die zu vernichtenden Daten vom Vorbehalt der Lieferung an das Staatsarchiv erfasst würden.

Der in Absatz 6 vorgeschlagene Archivierungs-Vorbehalt nach den Vorschriften des Archivierungsgesetzes ist der SP zu schwach ausgestaltet. Indem dieser Vorbehalt nicht bereits unmittelbar nach Absatz 2 sowie im Titel erwähnt werde, könnte der Eindruck entstehen, dass zur Vernichtung bestimmte Akten nicht archivierungspflichtig seien. Diese Interpretation würde aber klar gegen die Archivierungspflicht gemäss aktuellem Archivierungsgesetz verstossen. Der Vorbehalt des Archivierungsgesetzes müsse deshalb unmittelbar nach Absatz 2 platziert und auch im Titel explizit erwähnt werden. Zudem brauche es eine explizite Norm, dass die Archivierungspflicht nach aktuellem Archivierungsgesetz nicht durch die willkürliche Vernichtung von Akten umgangen werden dürfe. Auch sei dem Bundesarchiv das explizite Recht einzuräumen, die Einhaltung der Archivierungspflicht zu überprüfen. Die SP schlägt deshalb folgenden neuen Titel von Artikel 54, die neuen Absätze $2^{bis}$ und $2^{ter}$ sowie die Verschiebung von Absatz 6 (neu: Absatz $2^{quater}$) vor:

> Artikel 54 Titel neu: „Archivierungspflicht und Datenaufbewahrung und –vernichtung“
>
> Absatz $2^{bis}$ (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.
>
> Absatz $2^{ter}$ (neu) Die Fachstellen PSP gewähren dem Bundesarchiv mit Blick auf die langfristige Sicherung der Unterlagen Einblick in den Index des Informationssystems nach Artikel 52.
>
> Absatz $2^{quater}$ Die Vorschriften des Archivierungsgesetzes (SR 152.1) und des Bundesgesetzes über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (SR 121, Artikel 7a) zur Archivierung der Daten bleiben vorbehalten.

Clusis begrüsst diesen Artikel, der eine genügende gesetzliche Grundlage für die Bearbeitung von Personendaten, insbesondere auch von besonders schützenswerten, schafft.

**Artikel 55** Ergänzende Bestimmungen des Bundesrats

Für TG wäre es im Sinne der Erpressbarkeit und der Sicherheit allenfalls sinnvoll, dass Bestimmungen über Reisebeschränkungen für Personen mit sicherheitsempfindlichen Tätigkeiten erlassen werden dürften. Dies könne zwar die Einzelpersonen einschränken, aber bei einer umfassenderen Würdigung ebenso einen Schutz für diese Personen und für die Sicherheit der Daten darstellen.

## 4. Kapitel: Betriebssicherheitsverfahren

### Allgemein

Economiesuisse vermerkt bezüglich des Betriebssicherheitsverfahrens (BSV) positiv, dass das ISG von einem Betriebs- und nicht von einem Unternehmenssicherheitsverfahren spricht. So lasse sich der zu prüfende Bereich eingrenzen, was die Durchsetzung erforderlicher Sicherheitsmassnahmen erleichtere und kostengünstiger machen sollte. Positiv sei auch zu beurteilen, dass der beschränkte Anwendungsbereich des heutigen Geheimnisschutzverfahrens, das auf klassifizierte Aufträge aus dem militärischen Bereich beschränkt sei, ausgeweitet werde. Indem mit dem ISG für den militärischen und zivilen Bereich ein einheitliches BSV eingeführt werde und die Fachstelle offizielle Betriebssicherheitsbescheini-

gungen für internationale Verhältnisse ausstellen könne, werde die Wettbewerbsfähigkeit der Schweizer Unternehmen in Vergabeverfahren im Ausland gestärkt.

CP und CVAM stellen fest, dass das 4. Kapitel des ISG-Entwurfs (Art. 56-79) über das Betriebssicherheitsverfahren für die Wirtschaftsakteure keine grösseren Hindernisse schafft, sondern sich im Gegenteil an die Prinzipien der Objektivität und Gleichbehandlung hält, und ebenso das Recht auf Gehör und die Rechtsmittel der Schweizer Unternehmen betont, wenn sie sich um einen sensiblen Auftrag des Bundes bewerben möchten. Die Möglichkeit ein offizielles Sicherheitszertifikat nach Artikel 57 Absatz 1 Buchstabe b ISG von den zuständigen Bundesstellen zu erhalten, um sich für sensible Aufträge im In- und Ausland bewerben zu können, wird die Wettbewerbsfähigkeit der Schweizer Unternehmen stärken.

Insecor begrüsst eine einheitliche und klare Regelung des Betriebssicherheitsverfahrens.

Für den ETH-Rat herrscht im neuen Entwurf des ISG Unklarheit darüber, wann ein Auftrag als sicherheitsempfindlich einzustufen ist und wann nicht: während in Artikel 62 ff. ISG klargestellt werde, dass die Fachstelle BS über die Eignung eines Betriebs zu befinden habe, bleibe nun im neuen Entwurf unklar, welche Instanz die Beurteilung vornehme, ob der Auftrag selber als sicherheitsempfindlich einzustufen sei oder nicht. Das Nichtvorhandensein der diesbezüglichen entsprechenden klaren Kompetenzzuteilung lasse viel zu viel Raum für willkürliche Entscheide. Insbesondere suggeriere der jetzige Wortlaut von Artikel 59 ISG, dass eine verpflichtete Behörde oder Organisation selber darüber entscheiden könne, ob ein Auftrag sicherheitsempfindlich sei oder nicht. Wenn man ihr diese Beurteilung ohne entsprechende Hilfsmöglichkeit der Überprüfung durch die Bundessicherheitsbehörden überlasse, müsse sichergestellt sein, dass ihr beim späteren Auftauchen einer Problemsituation keine Nachteile erwachsen würden. Der ETH-Rat schlägt vor, im Gesetz klar zu stellen, welche Instanz diese Beurteilung vornehme bzw. an wen sich eine Organisation zwecks Überprüfung wenden könne, ob ein Auftrag als sicherheitsempfindlich gelte oder nicht. Der entsprechende Entscheid bedürfe ebenfalls eines Anfechtungsobjekts, falls dies nicht die betroffene Organisation selber entscheiden dürfe und sie mit dem Entscheid nicht einverstanden sei. Die Kriterien, die zur Durchführung eines Betriebssicherheitsverfahrens verpflichteten, seien genau festzulegen. Für das Betriebssicherheitsverfahren sei eine (kurze) Maximaldauer festzuschreiben, um Auftragsvergaben nicht unverhältnismässig zu verzögern.

**Artikel 62 ff.** Eignung der Betriebe in Bezug auf die Informationssicherheit

Die Beurteilung der Eignung gemäss Artikel 62 ff. ISG hat für den ETH-Rat idealerweise vor der Ausschreibung eines Auftrags zu erfolgen, ebenso müsse die Betriebssicherheitserklärung gemäss Artikel 69 ISG vor der Ausschreibung gemäss Submissionsgesetzgebung ausgestellt werden. Ansonsten bestehe bei einem erst nachträglich erfolgten Sicherheits- bzw. Eignungscheck des sich auf eine Ausschreibung meldenden Betriebs die Gefahr, dass derjenige Betrieb, der den Zuschlag im Ausschreibungsverfahren bekommen habe, im Falle eines negativen Ergebnisses beim Sicherheitscheck den Auftrag nicht durchführen könnte. Der ETH-Rat schlägt vor, im ISG eine spezialgesetzliche Bestimmung aufzustellen, welche besage, dass der Betrieb im Falle einer negativen Sicherheitsprüfung und einer damit einhergehenden Verhinderung bzw. Auflösung eines Vertrags keinen Anspruch auf Entschädigung habe, und zwar unabhängig davon, ob die Sicherheitsprüfung vor oder nach einem Ausschreibungsverfahren stattgefunden habe oder nicht. Dasselbe sollte auch für den Fall gelten, wenn aufgrund eines negativen Befunds bei einer Personensicherheitsprüfung ein Vertrag aufgelöst bzw. nicht abgeschlossen werden könne.

**Artikel 62** Beurteilung der Eignung

Aufgrund des heiklen Verhältnisses der Vergebung von sicherheitsempfindlichen Aufträgen zur nationalen und internationalen Ordnung über das öffentliche Beschaffungswesen (siehe vorne allg. Bemerkungen) erscheint es LB etwas befremdlich, dass die Auftraggeberin gemäss Artikel 62 Absatz 1 VE IGS das Recht und die Pflicht habe, vor bzw. ausserhalb von der nach Beschaffungsrecht grundsätzlich vorgeschriebenen Ausschreibung von Beschaffungsvorhaben der öffentlichen Hand der Fachstelle BS mitzuteilen, welche Betriebe für die Ausführung der Auftrags in Frage kommen würden, womit alle übrigen Betriebe von der Vergebung des Auftrags ausgeschlossen sind. Den Auftraggeberinnen werde hier eine sehr

weitgehende Kompetenz eingeräumt, in sicherheitsempfindlichen Bereichen nach eigenem Ermessen über die Einladung der für die Ausführung von sicherheitsempfindlichen Aufträgen in Frage kommenden Betriebe zu entscheiden.

**Artikel 63** Datenerhebung

Der NDB verlangt, dass auf Ebene der Ausführungsbestimmungen festzuhalten sei, dass der Informationsaustausch dann über den NDB stattzufinden habe, wenn die ausländische Dienststelle Teil einer nachrichtendienstlichen Organisation ist.

**Artikel 64** Sicherheitsrisiko

Economiesuisse fordert, dass insbesondere bei Artikel 64 ISG der Ermessenspielraum in der noch zu erlassenden Verordnung durch genauere Begriffsbestimmungen und klare Beurteilungskriterien begrenzt werde. Der vorliegende Entwurf enthalte zahlreiche unbestimmte und zu weit gefasste Begriffe. So verfüge die Behörde bei Artikel 64 (Sicherheitsrisiko), insbesondere bei Absatz 2 Buchstabe b (ausländisch beeinflusste Betriebe) mangels klar formulierter Beurteilungskriterien über einen zu grossen Ermessensspielraum bei der Prüfung des Sicherheitsrisikos, das von der Auftragsausführung durch einen Betrieb ausgehe. Die Bestimmung ermögliche es der Behörde, unwillkommene Anbieter ohne sachlichen Grund vom Vergabeverfahren auszuschliessen. Damit berge sie ein Potenzial für (protektionistisch motivierte) Ungleichbehandlungen und Wettbewerbsverzerrungen. Jede künstliche Verringerung der Anzahl Anbieter führe jedoch zu höheren Preisen. Dies schwäche den Wirtschaftsstandort Schweiz.

Die swico hält, unter Verweis auf einen Zwischenentscheid des Bundesverwaltungsgerichts vom 21. Mai 2014 (Dossiernummer B-998/2014), die Bestimmung, dass die Wahrscheinlichkeit einer vorschriftswidrigen und unsachgemässen Ausführung des sicherheitsempfindlichen Auftrags insbesondere dann als hoch gelten könne, wenn der Betrieb von ausländischen Staaten oder ausländischen Organisationen des öffentlichen oder privaten Rechts kontrolliert oder beeinflusst werde, für wettbewerbs- und beschaffungsrechtlich fragwürdig. Sie dürfte die Beschaffungsproblematik noch weiter verschärfen. Wie jede künstliche Verknappung der Anzahl Anbieter führe dies zu höheren Preisen. Dies schwäche die Volkswirtschaft und den Wirtschaftsstandort Schweiz. Die vorliegende Gesetzesbestimmung öffne Tür und Tor zu willkürlicher oder sogar missbräuchlicher Auslegung durch die Behörden. Durch den viel zu weiten Interpretations- und Ermessensspielraum bestehe die Gefahr, dass unwillkommene Anwender auf Distanz gehalten werden könnten. Die swico fordert daher, dass in der noch zu erlassenden Verordnung der Ermessensspielraum klar begrenzt und klare Kriterien und Begriffsbestimmungen festgelegt würden.

Wie allgemein bekannt sei, seien die Muttergesellschaften vieler der im Bereich der Informationsverarbeitung und -übermittlung tätigen Betriebe im Ausland domiziliert und würden von ausländischen Anteilseigner und Aktionären kontrolliert. Aus Artikel 64 Absatz 2 Buchstabe b ISG könne nun der Schluss gezogen werden, dass bei solchen Betrieben zum vornherein eine hohe Wahrscheinlichkeit der vorschriftswidrigen Ausführung eines sicherheitsempfindlichen Auftrags bestehe. Sie wären damit gemäss Artikel 65 Absatz 2 ISG vom Vergabeverfahren auszuschliessen. Nach Erachten von LB könnte die vorstehende Annahme als nach dem internationalen Beschaffungsrecht als sachlich nicht gerechtfertigte Diskriminierung der ausländischen Anbieter im Bereich Informationsverarbeitung und -übermittlung qualifiziert werden. Jedenfalls sollte im Gesetzgebungsverfahren durch eine fachkundige Stelle geprüft werden, ob und inwieweit Artikel 64 Absatz 2 Buchstabe b VE IGS mit den Normen des internationalen Beschaffungsrechts vereinbar sei. Überdies könnte die strenge Anwendung der Regel von Artikel 64 Absatz 2 Buchstabe b ISG dazu führen, dass der Kreis der für die Ausführung sicherheitsempfindlicher Aufträge qualifizierten Betriebe übermässig eingeengt würde und nur noch wenige - oder gar keine - fachlich qualifizierten Anbieter zur Verfügung stünden. Es könnte somit zu einem Konflikt des Interesses an optimaler Sicherheit mit dem Interesse an der Auswahl des für eine bestimmte Anwendung am besten qualifizierten Anbieters kommen.

**Artikel 66** Sicherheitskonzept

LB erachtet es als sachfremd und als unnötigen Eingriff in die betriebliche Autonomie, dass das betriebliche Sicherheitskonzept für das mit der Ausführung eines sicherheitsempfindlichen Auftrages betraute Unternehmen von einer Verwaltungsstelle, der Fachstelle BS, zu erstellen sei. Sachgemäss würde eine Regelung erscheinen, wonach der für die Ausführung eines sicherheitsempfindlichen Auftrages ausgewählte Betrieb ein Sicherheitskonzept erstelle, welches von der Fachstelle BS zu prüfen und zu genehmigen sei.

**Artikel 68** Betriebssicherheitserklärung / **Artikel 69** Ausführung des sicherheitsempfindlichen Auftrags

Für Privatim müsste zwingend geklärt werden weshalb bei der Betriebssicherheitserklärung eine Verfügung erlassen werde, bei den Personensicherheitsprüfungen aber nur Empfehlungen abgegeben werden. Diese Differenzierung sei zu erläutern.

**Artikel 69 ff**. Folgen der Betriebssicherheitserklärung

Nach Ansicht von Clusis wird nirgendwo das Problem der Vergabe von Aufträgen an Zulieferer behandelt. Oder soll eine solche Vergabe aufgrund des sensiblen Charakters der Aufträge ausgeschlossen sein? Es sollten daher zumindest strenge Voraussetzungen im Gesetz genannt werden.

**Artikel 69** Ausführung des sicherheitsempfindlichen Auftrags

Diese Bestimmung greift dem ETH-Rat zu stark in die Autonomie der Institutionen des ETH-Bereichs ein. Zudem führe sie speziell für die Institutionen des ETH-Bereichs, die ja nicht der Org-VöB unterstünden, zu einem beträchtlichen administrativen Mehraufwand und unverhältnismässigen zeitlichen Verzögerungen, insb. wenn man bedenke, dass parallel zu den Bestimmungen des ISG die beschaffungsrechtlichen Vorgaben einzuhalten seien.

**Artikel 76** Rechtsschutz

Wie bereits zu Artikel 51 des Entwurfes ISG erwähnt, sieht es TG auch hier nicht angebracht, die Frist zur Akteneinsicht anders als die Beschwerdefrist zu regeln. Gemäss Artikel 50 VwVG (SR 172.021) können Beschwerden gegen Verfügungen des Bundes grundsätzlich innert 30 Tagen beim Verwaltungsgericht eingereicht werden, weshalb die vorgesehene Zehntagesfrist entsprechend zu erweitern ist.

**Artikel 79** Datenaufbewahrung und -vernichtung

Absatz 2 und 3 sind gemäss TG zu tauschen (und grammatikalisch anzupassen), damit sichergestellt werde, dass nicht die zu vernichtenden Daten vom Vorbehalt der Lieferung an das Staatsarchiv erfasst würden.

Für die SP sind dieselben Überlegungen wie bei Artikel 54 auch bei Artikel 79 ISG zu berücksichtigen, wo es um die Aufbewahrung und Vernichtung von Daten gehe, welche die für die Durchführung des Betriebssicherheitsverfahrens zuständige Fachstelle für Betriebssicherheit (Fachstelle BS) erhebe:

> Artikel 79 Titel neu: „Archivierungspflicht und Datenaufbewahrung und –vernichtung“
>
> Absatz $2^{bis}$ (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.
>
> Absatz $2^{ter}$ (neu) Die Fachstelle BS gewährt dem Bundesarchiv mit Blick auf die langfristige Sicherung der Unterlagen Einblick in ihr internes Registratursystem.
>
> Absatz $2^{quater}$ Die Vorschriften des Archivierungsgesetzes (Ar. 152.1) und des Bundesgesetzes über die Zuständigkeiten im Bereich des zivilen Nachrichtendienstes (SR 121, Artikel 7a) zur Archivierung der Daten bleiben vorbehalten.

## 5. Kapitel: Informationssicherheit bei kritischen Infrastrukturen (KI)

Aus Sicht der SP muss das ganze 5. Kapitel über die Informationssicherheit bei kritischen Infrastrukturen (ISG Artikel 81 – Artikel 83) grundsätzlich überarbeitet werden. Der Entwurf ISG enthalte in diesem Kapitel unannehmbare pauschale Ermächtigungen zu nachrichtendienstlichen Tätigkeiten und kläre die Schnittstellen ungenügend zwischen der Gewährleistung der Informationssicherheit bei kritischen Infrastrukturen und dem Schutz kritischer Infrastrukturen an und für sich. Der Schutz kritischer Infrastrukturen sei aus sicherheitspolitischer Sicht eine viel zu wichtige Aufgabe, um ihn in derart unsorgfältiger, pauschaler Weise abzuhandeln, wie dies im Entwurf ISG gemacht werde.

**Artikel 81** Aufgaben des Bundes

Absatz 3 ermächtigt aus Sicht der SP 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 sei folgender neuer Absatz 4 einzufügen: „[4] Die Bestimmungen des Datenschutzgesetzes bleiben vorbehalten."

Unterstützen genügt für it-rm bei weitem nicht, denn das Sabotieren der kritischen Infrastrukturen könne einen viel grösseren Schaden für das Wohlergehen unseres Staates bewirken als unter Umständen die Bekanntgabe vertraulicher Informationen. Es bedürfe folglich der Mindestvorschriften und dann unter Umständen auch der finanziellen Unterstützung des Bundes für die Umsetzung dieser Vorgaben. It-rm schlägt vor, eine entsprechende Legitimation dazu im Gesetz aufnehmen.

**Artikel 82** Bearbeitung von Personendaten

Diese Bestimmung erlaubt gemäss SO ein Bearbeiten von Personendaten, ohne dass dies für die betroffene Person erkennbar sei. Dies stelle einen erheblichen Eingriff in die Persönlichkeitsrechte dar. Spätestens nach dem Wegfall der vermuteten Gefahr, müsse die Person darüber informiert werden. Es dränge sich deshalb eine vergleichbare Regelung auf, wie sie Artikel 283, 298 und 298d der Strafprozessordnung für die Observation und verdeckte Ermittlung kenne).

TG beantragt die Streichung der Bestimmung von Artikel 82 des Entwurfes ISG, wonach die zuständigen Stellen bei kritischen Infrastrukturen zur Abwehr von Gefahren Personendaten, insbesondere Adressierungselemente im Fernmeldebereich bearbeiten und weitergeben dürften und dies sogar noch ohne dass es für die betroffenen Personen ersichtlich sei. Hier werde unter dem Vorwand der Informationssicherheit ein Instrument geschaffen, um besonders schützenswerte Personendaten einer Vielzahl von Personen bearbeiten zu dürfen. Es fehle an jeglicher Kontrolle oder rechtlicher Möglichkeit, einem allfälligen Missbrauch Einhalt gebieten zu können. Beim Bundesgesetz über die Informationssicherheit gehe es darum, den sicheren Umgang mit Informationen zu gewährleisten. Dieses Gesetz dürfe nicht als Hintertüre verwendet werden, um nachrichtendienstlich tätig zu werden.

TI schlägt vor, Artikel 82 des ISG mit einem vierten Absatz zu ergänzen, der im Falle einer Identifizierung des Nutzers vorsieht, dass dieser darüber informiert wird und die entsprechenden Daten den zuständigen Behörden mitgeteilt werden können. Für den Fall, dass eine Person auf der Basis der Personendaten nach Artikel 82 identifiziert würde, müsse sie informiert werden, zumindest nach Wegfall der Gefahr (analog zu den Verfahren für die Observierung von Personen, verdeckte Ermittlungen und verdeckte Fahndung, welche von den Art. 283, 298 bzw. 298d StPO geregelt werden). In dieser Hinsicht erscheine die Formulierung von Abs. 1 als zu schwach und selbst die punktuelle Beschreibung im Erläuternden Bericht sei nicht ausreichend.

Die SP fordert Artikel 82 zu streichen. Gemäss dieser Regelung dürften 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 würde. Damit werde unter dem Vorwand der Informationssicherheit ein Instrument geschaffen, um besonders schützenswerte

Personendaten von einer Vielzahl von Personen bearbeiten zu dürfen. Es fehle an jeglicher Kontrolle oder rechtlicher Möglichkeit, einem allfälligen Missbrauch Einhalt gebieten zu können. Beim vorliegenden Gesetz gehe es indessen darum, den sicheren Umgang mit Informationen zu gewährleisten. Es dürfe nicht als Hintertüre verwendet werden, um nachrichtendienstlich tätig zu werden.

Für privatim lässt sich in Anbetracht des verfassungsmässigen Grundsatzes von Treu und Glauben und daraus abgeleitet des datenschutzrechtlichen Transparenzgebots die Bearbeitung von Personendaten zur Abwehr von Gefahren, ohne dass dies für die betroffenen Personen ersichtlich sein soll, nur dann rechtfertigen, wenn nach dem Wegfall der vermuteten Gefahr — analog zum Vorgehen z.B. bei der Observation, bei verdeckter Ermittlung oder bei verdeckter Fahndung (Artikel 283, Artikel 298 bzw. Artikel 298d StPO) — eine Mitteilung an die betroffene Person erfolge. Artikel 82 ISG sei dahingehend zu ergänzen.

Für LB steht es ausser Frage, dass der Schutz von Infrastrukturen, die gemäss Artikel 3 Absatz 3 ISG für das Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlich seien, einen hohen Stellenwert haben müssen. Dennoch müsse auch in diesem Bereich der Grundsatz der Verhältnismässigkeit des staatlichen Handelns (Art. 5 Abs. 2 BV) beim Eingriff in die durch die Verfassung geschützten Grundrechte beachtet werden. Es sei daher schwer verständlich, wie der Vorentwurf des ISG in Zeiten erhöhter Bedenken der Bürger gegen staatliche Überwachungsmassnahmen den Betreiberinnen kritischer Infrastrukturanlagen die Kompetenz erteilen könne:

- von sich aus ohne besonderen Anlass wie Verdacht eines Verbrechens
- ohne Ermächtigung einer richterlichen Instanz oder mindestens einer politisch zuständigen und verantwortlichen Behörde
- Personendaten, insbesondere Adressierungselemente, aber auch besonders schützenswerte Daten im Sinne von Artikel 3 Buchstabe c DSG im gesamten Fernmeldebereich
- ohne zeitliche und sachliche Beschränkung
- zu bearbeiten (vgl. Art. 3 Bst. e/f DSG) d.h. zu beschaffen, zu speichern, zu verwenden, auszuwerten, und auf unbestimmte Dauer zu archivieren
- die erfassten Daten den verpflichteten Behörden und Organisationen, den zuständigen Stellen der Kantone und sogar Dritten (natürlich im Rahmen der Aufgabenerfüllung) bekanntzugeben
- die betroffenen Personen darüber im Gegensatz zu Artikel 279 StPO nach Durchführung der Überwachung nicht zu informieren
- wobei die Betreiberinnen der Infrastrukturanlagen für diese Überwachungstätigkeiten keinerlei unabhängiger Kontrolle unterstehen sollen.

Der Schutz der kritischen Infrastrukturen sei für Staat, Wirtschaft und Gesellschaft von elementarer Bedeutung. Dennoch sollten auf dem Altar des Schutzes dieser kritischen Infrastrukturen nicht elementare Grundsätze staatlichen Handelns und die Wahrung der Grundrechte geopfert werden. Sicherheit und Schutz der Grundrechte sollten in ein ausgewogenes Verhältnis gebracht werden.

**Artikel 83** Ergänzende Bestimmungen des Bundesrats

TG beantragt analog zu den Bemerkungen zu Artikel 82 des Entwurfes ISG von der nachrichtendienstlichen Tätigkeit abzusehen.

Die SP lehnt die in Artikel 83 ISG vorgenommene Kompetenzdelegation an den Bundesrat ab. Ein Informationssicherungsgesetz habe 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 Artikel 81 wahrnehmen, und dem Nachrichtendienst des Bundes, müsse auf Gesetzesstufe geregelt werden. Die Stellen, welche die Kompetenz erhalten sollen, nachrichtendienst-

liche Informationen auszutauschen, seien aus datenschutzrechtlichen Gründen einzeln zu benennen. Auch sei zu spezifizieren, welche Informationen diese Stellen mit dem Nachrichtendienst austauschen könnten. Weil es dabei oft um besonders schützenswerte Personendaten gehe, sei im ISG die übliche hohe Normendichte einzuhalten. Könne dieses Ziel nicht erreicht werden, sei in Artikel 83 ISG explizit jegliche nachrichtendienstliche Tätigkeit auszuschliessen.

### 6. Kapitel: Organisation und Vollzug

**Artikel 84** Informationssicherheitsbeauftragte / **Artikel 85** Konferenz der Informationssicherheitsbeauftragten

GL beantragt, dass ein Vertreter der Schweizerischen Informatikkonferenz als Informationssicherheitsbeauftragter der Kantone bezeichnet wird, der sich ebenfalls in die Konferenz der Informationssicherheitsbeauftragten gemäss Artikel 85 einbringen könne.

ZG beantragt, Artikel 84 Absatz 1 mit einem Buchstaben „g. die Kantone“ zu ergänzen. Die im ISG vorgeschlagene lose Organisation mit kantonalen Anlaufstellen könne eine funktionierende Koordination und Abstimmung zwischen Bund und Kantonen nicht bewerkstelligen. Eine engere und institutionalisierte Anbindung der Kantone sei notwendig und zielführender. Dies könnte mit einem permanenten Einsitz einer Kantonsvertretung in der beabsichtigten Konferenz der Informationssicherheitsbeauftragten gemäss Artikel 85 angestrebt werden, ähnlich wie dies beispielsweise in der Europapolitik der Fall sei (ständige Kantonsvertretung in der Direktion für Europäische Angelegenheiten). Die Kantone müssten dazu gemeinsame Informationssicherheitsbeauftragte ernennen, gleich wie die einzelnen eidgenössischen Organe (Artikel 84).

Um Doppelspurigkeiten bei Anfragen zu Sicherheitsproblemen zu vermeiden, beantragt TG, Artikel 85 des Entwurfes ISG dahingehend zu erweitern, dass die Konferenz der Informationssicherheitsbeauftragten nicht nur die Koordination mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten sucht, sondern dass auch eine Koordination mit den jeweils betroffenen kantonalen Datenschutzbeauftragten stattfinden soll.

Für die Bereiche, auf die das Gesetz auf vom Bund beauftragte kantonale Behörden anwendbar ist, stellt sich für VD die Frage der Repräsentation dieser Behörden in der Konferenz der Informationssicherheitsbeauftragten.

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

Clusis begrüsst die neue Funktion des Informationssicherheitsbeauftragten. Warum wird diese aber nicht mit der Funktion des Datenschutzbeauftragten nach DSG verbunden, zumal erwähnt wird, dass «der Informationssicherheitsbeauftragte gegebenenfalls eng mit dem Datenschutzbeauftragten des Unternehmens zusammenarbeitet.» Damit würden auch die Aufgaben des einen besser mit denen des anderen koordiniert.

Der NDB verlangt, dass operative Systeme und operativ beschaffte nachrichtendienstliche Daten von der Überprüfung durch den Informationssicherheitsbeauftragten VBS ausgenommen werden, da aus Gründen des Quellenschutzes der NDB bei operativ beschafften Informationen besondere Schutzmassnahmen anwende. Diese Massnahmen werden durch eine VBS-interne Aufsichtsinstanz (ND-Aufsicht) regelmässig überprüft.

**Artikel 86** Fachstelle des Bundes für Informationssicherheit

Für TI sind im Hinblick auf die einzige, zentrale Struktur, die verschiedenen Rollen der „behördenübergreifenden“ Stellen nicht klar definiert und in gewisser Hinsicht widersprüchlich oder - noch schlechter sogar - redundant.

**Artikel 87** Ausführungsbestimmungen

Aufgrund der vorgesehenen «Opting-out»-Regelung (Artikel 87 Absatz 3 ISG), wonach jede der verpflichteten Behörden eigenes Verordnungsrecht erlassen kann und die vom Bundesrat festgelegten Standardanforderungen und -massnahmen nur Empfehlungscharakter haben, sieht ZH die Gefahr, dass die teilweise sehr offenen Begriffe unterschiedlich ausgelegt und in den Ausführungsbestimmungen der verschiedenen Behörden unterschiedlich geregelt werden. ZH ist deshalb der Ansicht, dass das an sich sehr detaillierte Gesetz zumindest in Bezug auf die in Artikel 1 Absatz 2 ISG definierten, zu schützenden öffentlichen Interessen und die vorgesehenen Klassifizierungsstufen näher spezifiziert werden sollte.

BE beantragt, Artikel 87 mit einem neuen Absatz 5 wie folgt zu ergänzen: „[5] Der Bundesrat legt die Tätigkeiten gemäss Artikel 2 Absatz 2 Buchstabe f durch Verordnung fest.“ Zudem solle die Botschaft zum ISG eine Fassung der Liste dieser Tätigkeiten aus heutiger Sicht enthalten. Gemäss Artikel 2 Absatz 2 Buchstabe f gelte das ISG auch für kantonale Behörden und Stellen, die im Auftrag des Bundes und unter seiner Aufsicht sicherheitsempfindliche Tätigkeiten ausübten. Welche Tätigkeiten das seien, sei aber aus den Erläuterungen nicht ersichtlich. Damit die Kantone und Gemeinden klar wüssten, in welchem Umfang sie durch das ISG verpflichtet seien, sei dies in einer Liste auf Verordnungsebene festzuhalten. Um die Auswirkungen des ISG auf die Kantone und Gemeinden abschätzen zu können, sollte bereits die Botschaft zum ISG eine Fassung dieser Liste aus heutiger Sicht enthalten. Sie sollte auch klarstellen, was unter „unter Aufsicht“ zu verstehen sei.

ZG stellt in Frage, ob die vorgeschlagene «Opting Out»-Regelung zielführend sei, wonach jede Behörden den Erlass in ihrem Bereich selbständig vollzieht und entsprechendes Verordnungsrecht erlasse. Das Gesetz müsse mehr als nur Mindeststandards festlegen, wenn die Informationssicherheit in allen angegliederten Behörden gewährleistet werden soll. Übergreifende Standards und Normen wären diesbezüglich notwendig und wichtig. Auch die Einbindung der Kantone sei daher grundsätzlich sinnvoll.

Für BS ergibt sich weder aus dem vorgeschlagenen Gesetzeswortlaut (Art. 2 Abs. 2 Bst. f ISG) noch aus den Erläuterungen klar, welche Tätigkeiten kantonaler Behörden in den Geltungsbereich fielen. BS regt an, Artikel 87 ISG um eine Bestimmung zu ergänzen, wonach der Bundesrat die Tätigkeiten gemäss Artikel 2 Absatz 2 Buchstabe f durch Verordnung festzulegen habe. Damit die Auswirkungen auf den Kanton abgeschätzt werden können, sollte bereits die Botschaft eine Fassung dieser Liste aus heutiger Sicht enthalten. Ausserdem sollte die Botschaft auch klarstellen, was unter «unter Aufsicht» zu verstehen ist.

TI stellt zur „Opting-out“-Regelung fest, dass der selbständige Erlass von Ausführungsbestimmungen, der in Verbindung dazu sinngemäss auch für die übrigen Bundesbehörden gelten soll, die Grundlage für eine Ungleichheit im Vollzug schaffe. Für die Sicherheitsthematik sei dies keine ideale Lösung.

Die CVP begrüsst, dass die Behördenautonomie durch den vorliegenden Gesetzesentwurf nicht eingeschränkt werden soll, indem die verpflichteten Behörden selber Ausführungsbestimmungen erlassen können. Die CVP unterstützt ebenfalls, dass die Ausführungsbestimmungen des Bundesrates für die verpflichteten Behörden sinngemäss gelten, sollten diese keine eigenen Ausführungsbestimmungen erlassen.

AB-BA nimmt zur Kenntnis, dass die Aufsichtsbehörde, welche gemäss Artikel 2 Absatz 2 Buchstabe d als verpflichtete Behörde aufgeführt ist, nach Artikel 87 Absatz 1 ihre eigenen Ausführungsbestimmungen erlassen kann. Damit entfielen einige der Vorbehalte, welche die Behörde in der Ämterkonsultation vom 2. April 2013 angebracht habe.

Weder aus dem vorgeschlagenen Gesetzeswortlaut von Artikel 2 Absatz 2 Buchstabe f ISG noch aus den Erläuterungen ergibt sich für privatim klar, welche Tätigkeiten kantonaler Behörden in den Geltungsbereich fallen. Privatim stellt deshalb den Antrag, Artikel 87 ISG um eine Bestimmung zu ergänzen, wonach der Bundesrat die Tätigkeiten gemäss Artikel 2 Absatz 2 Buchstabe f durch Verordnung festzulegen habe. Damit die Auswirkungen auf die Kantone abgeschätzt werden könnten, solle bereits die Botschaft eine Fassung dieser Liste

aus heutiger Sicht enthalten. Ausserdem solle die Botschaft auch klarstellen, was unter «unter Aufsicht» zu verstehen sei.

Die SIK beantragt, Artikel 87 mit einem neuen Absatz 5 wie folgt zu ergänzen: „[5] Der Bundesrat legt die Tätigkeiten gemäss Artikel 2 Absatz 2 Buchstabe f durch Verordnung fest.“ Die Botschaft zum ISG solle zudem eine Fassung der Liste dieser Tätigkeiten aus heutiger Sicht enthalten. Es sei aus den Erläuterungen nicht ersichtlich, welche Tätigkeiten als sicherheitsempfindliche Tätigkeiten kantonaler Behörden und Stellen im Auftrag und unter Aufsicht des Bundes im Sinne des Artikels 2 Buchstabe f gelten würden. Damit die Kantone und Gemeinden klar wüssten, in welchem Umfang sie durch das ISG verpflichtet seien, sei dies in einer Liste auf Verordnungsebene festzuhalten und solle bereits die Botschaft zum ISG eine Fassung dieser Liste aus heutiger Sicht enthalten.

Die SNB begrüsst ausdrücklich den eigenständigen Vollzug gemäss Artikel 87 des Gesetzesentwurfs. Trotzdem führten die Erläuterungen aus, dass dieser eigenständige Vollzug einen Nachteil habe: "Die minimalen organisatorischen Anforderungen der Informationssicherheit, die von allen Bundesbehörden erfüllt werden sollen, müssen zwingend auf Gesetzesebene verankert werden. Demzufolge enthält die Vorlage auch zahlreiche Bestimmungen, die von der Normenhierarchie eher dem Verordnungsrecht entsprechen." Die SNB versteht durchaus das Bestreben des Gesetzesentwurfs, gewisse organisatorische Anforderungen auch für die verfassungsmässig unabhängigen verpflichteten Behörden zu regeln. Aber gerade die Rücksichtnahme auf die in Artikel 87 statuierte, der Verordnungskompetenz des Bundesrates entzogene Vollzugsautonomie dieser Behörden gebiete Zurückhaltung bei der im Entwurf praktizierten Verankerung von Verordnungsmaterie auf Gesetzesstufe. Letzteres tangiere eben diese Vollzugsautonomie.

Das BGer macht darauf aufmerksam, dass dieser Artikel für das BGer wesentlich sei und deshalb nicht zu seinem Nachteil verändert werden dürfe.

Insecor erachtet das Vorgehen, dass die jeweiligen Bundesbehörden ihre eigenen Ausführungsbestimmungen erlassen sollen, als nur bedingt zielführend. Gerade in Verordnungen stünden jeweils wichtige Präzisierungen des Gesetzestextes, welche im Bereich der Informationssicherheit nicht erneut „verzettelt“ werden dürften. Schliesslich gebe es immer noch die Möglichkeit jeweiliger Departementsverordnungen oder Weisungen, welche den spezifischen Bedürfnissen einer Verwaltungseinheit entsprechend Rechnung tragen könnten.

Für den ETH-Rat wird es zu prüfen sein, von welchen Teilen des Gesetzes die Institutionen des ETH-Bereichs und der ETH-Rat ausgenommen werden könnten; zumindest das Kapitel betr. Betriebssicherheitsprüfung sollte nicht auf die Institutionen des ETH-Bereichs und auf den ETH-Rat anwendbar sein (vgl. dazu insb. Rückmeldung zu Artikel 65 ff. oben).

**Artikel 88** Standardanforderungen und -massnahmen

BE beantragt, Artikel 88 mit einem neuen Absatz 4 wie folgt zu ergänzen: „[4] Der Bundesrat regelt durch Verordnung, welche verpflichteten Behörden einzeln oder gemeinsam zur Verbindlicherklärung von Standardanforderungen und -massnahmen zuständig sind, die Tätigkeiten oder Systeme betreffen, die von mehreren verpflichteten Behörden gemeinsam ausgeführt oder genutzt werden. Soweit kantonale verpflichtete Behörden betroffen sind, ist deren Zustimmung erforderlich.“ In verschiedenen Bereichen arbeiteten Bundes- und kantonale Behörden eng zusammen oder erfüllten kantonale Behörden Aufträge des Bundes, etwa im Polizeibereich. Zudem müssten Datensammlungen oder ICT-Systeme (z.B. Netzwerke) verschiedener Behörden oft zur Aufgabenerfüllung miteinander verbunden werden. In diesen Fällen sei es nicht sinnvoll, wenn die Partnerbehörden unterschiedliche Sicherheitsniveaus anwendeten. Daher sollte eine vom Bundesrat bestimmte Leitbehörde das für die ganze Tätigkeit geltende Sicherheitsniveau festlegen. Um allerdings zu verhindern, dass eine Bundesbehörde einseitig Massnahmen festlege, die kantonsseitig zu hohen Mehrkosten führten, müsse stets die Zustimmung allfällig betroffener kantonaler Behörden eingeholt werden.

Es ist nach Meinung der CVP wichtig, dass der Bundesrat standardisierte Sicherheitsanforderungen sowie standardisierte organisatorische, personelle, technische und bauliche Mass-

nahmen der Informationssicherheit nach dem Stand der Lehre und der Technik festlegt, welche den verpflichtenden Behörden als Empfehlungen dienen.

Privatim empfiehlt dringend zu prüfen, inwieweit die Standardanforderungen und -massnahmen für sämtliche dem ISG unterworfenen Behörden und Organisationen für verbindlich zu erklären seien. Bleibe es beim Empfehlungscharakter und der freiwilligen Verbindlichkeitserklärung, könne kein einheitliches Schutzniveau erreicht werden.

Da in verschiedenen Bereichen Bundes- und kantonale Behörden eng zusammenarbeiten oder kantonale und kommunale Behörden Aufträge des Bundes erfüllen würden und Datensammlungen oder ICT-Systeme verschiedener Behörden oft zur Aufgabenerfüllung miteinander verbunden werden müssten, sei es nicht sinnvoll, wenn die Partnerbehörden unterschiedliche Sicherheitsniveaus anwendeten. Daher sollte eine vom Bundesrat bestimmte Leitbehörde das für die ganze Tätigkeit geltende Sicherheitsniveau festlegen. Um allerdings zu verhindern, dass eine Bundesbehörde einseitig Massnahmen festlege, die kantonsseitig zu hohen Mehrkosten führten, müsse die Zustimmung allfällig betroffener kantonaler Behörden stets eingeholt werden. Die SIK beantragt daher, Artikel 88 mit einem neuen Absatz 4 wie folgt zu ergänzen:

> [4] Der Bundesrat regelt durch Verordnung, welche verpflichteten Behörden einzeln oder gemeinsam zur Verbindlicherklärung von Standardanforderungen und -massnahmen zuständig sind, die Tätigkeiten oder Systeme betreffen, die von mehreren verpflichteten Behörden gemeinsam ausgeführt oder genutzt werden. Soweit kantonale verpflichtete Behörden betroffen sind, ist deren Zustimmung erforderlich.

Das BGer macht darauf aufmerksam, dass dieser Artikel für das BGer wesentlich sei und deshalb nicht zu seinem Nachteil verändert werden dürfe.

Für it-rm bedarf es zwingend einer Institution (Koordinationsstelle), welche Ausführungsvorschriften erlässt, welche für alle von diesem Gesetz betroffenen Behörden verpflichtend und folglich einzuhalten sind (Widerspruch zu Artikel 88 Absatz 3 ISG). Ansonsten könne dies zu Inhomogenitäten im Sicherheitsdispositiv führen und zudem dazu beitragen, dass dem Wandel der Technik und somit den daraus erwachsenden veränderten Sicherheitsbedürfnissen zu wenig Rechnung beigemessen wird. Es wäre unwirtschaftlich, wenn beim Behörden übergreifenden Informationsaustausch unterschiedliche Massnahmen zum Schutz derselben Rechtsgüter ergriffen würden. Eine Inhomogenität im Sicherheitsdispositiv sei zudem aus Sicht derjenigen Behörde unwirtschaftlich, welche die wirksameren und somit teureren Sicherheitsmassnahmen umgesetzt hat. Die Sicherheit der Information lasse sich bekanntlich an der schwächsten Massnahme ableiten. Nur in Ausnahmefällen und mit einem schriftlich begründeten Gesuch sollte davon abgewichen werden dürfen.

Aus Sicht des NDB rechtfertige es sich, die Erarbeitung und Verarbeitung von Sicherheitsstandards an den NDB zu delegieren (analog fedpol, siehe erläuternder Bericht zu Artikel 88 Absatz 2 ISG, S. 71). Der NDB verfüge wie das fedpol über besondere Bedürfnisse hinsichtlich der Datenbearbeitung bzw. Aufbewahrung. Insbesondere der Datenaustausch zwischen verschiedenen staatlichen Stellen im In- und Ausland sei beim NDB von besonderer Bedeutung und mit anderen Bundesstellen nicht vergleichbar. Auch hinsichtlich des Quellenschutzes seien NDB-spezifische Sicherheitsstandards unabdingbar.

**Artikel 89** Kantone

Gemäss Artikel 89 ISG sollen kantonale Behörden und Stellen dem Gesetz nur dann unterstehen, wenn sie im Auftrag des Bundes und unter seiner unmittelbaren Aufsicht sicherheitsempfindliche Tätigkeiten ausüben. Setzen kantonale Behörden und Stellen das Bundesrecht in eigener Kompetenz um, werden sie vom Gesetz nicht erfasst (Erläuternder Bericht, S. 36). Diese für ZH zentrale, den Geltungsbereich betreffende Regelung werfe mehr Fragen auf, als sie beantworte. Welche Tätigkeiten der Kantone seien gemeint? In welchen Bereichen seien die Kantone unter welcher unmittelbaren Aufsicht tätig? Da im Erläuternden Bericht kein einziges konkretes Beispiel dafür erwähnt werde, sei davon auszugehen, dass auch beim Bund darüber keine Klarheit herrsche. Es sei aber notwendig, abschätzen zu können,

ob und in welchem Umfang das Gesetz auf kantonale Tätigkeiten anwendbar sei und welche Konsequenzen – insbesondere auch finanzieller Art – eine Geltung nach sich zöge. Spätestens die Botschaft an die eidgenössischen Räte müsse diesbezüglich Klarheit schaffen.

ZH und BE beantragen, Artikel 89 ISG um eine Regelung zu ergänzen, die vorsieht, dass kantonale Behörden und Stellen die Leistungen der im ISG vorgesehenen Fachstellen des Bundes in Anspruch nehmen können. ZH begründet dies damit, dass das ISG Massnahmen vorsehe (namentlich Personensicherheitsprüfung und Betriebssicherheitsverfahren), die auf der Stufe Kanton (und Gemeinde) gar nicht oder anders geregelt seien. Daher müssten die Kantone (und Gemeinden) die Dienste der Bundesfachstellen in Anspruch nehmen können. BE schlägt einen konkreten Text vor: „[4] Kantonale Behörden und Stellen können die Leistungen der in diesem Gesetz vorgesehenen Fachstellen des Bundes in Anspruch nehmen. Der Bundesrat kann vorsehen, dass für Leistungen an andere Behörden und Stellen als an diejenigen gemäss Absatz 1 kostendeckende Gebühren erhoben werden.“ Es sei nicht sinnvoll und wäre teils wohl auch nicht möglich, das für die Aufgaben der Fachstellen PSP und BS notwendige spezialisierte Fachwissen vielfach dezentral in den Kantonen und Gemeinden aufzubauen. Daher müssten die Kantone die Dienste der Bundesfachstellen in Anspruch nehmen können. Soweit das ISG kantonale und kommunale Stellen direkt verpflichte (Art. 2 Abs. 2 Bst. f bzw. Art. 89 Abs. 1 ISG), müssten die entsprechenden Leistungen (z.B. die Durchführung von PSP) vom Bund finanziert werden. Soweit die Kantone das ISG in ihrem eigenen Verantwortungsbereich autonom umsetzten, z.B. durch die Einführung von PSP für weitere Kantonsangestellte, erscheine es angebracht, dass sie die dem Bund dafür entstehenden Kosten durch Gebühren tragen.

Für ZH ermächtigt Artikel 89 Absatz 2 Buchstabe a ISG den Bundesrat, Personensicherheitsprüfungen für kantonale Organe zu regeln. Weil mit einer Personensicherheitsprüfung ein Eingriff in die Grundrechte der betroffenen Person verbunden sei, müsse die entsprechende Regelung – zumindest in den Grundzügen – auf Gesetzesstufe erfolgen. Der Gesetzesentwurf sei entsprechend anzupassen.

OW erachtet es als sinnvoll, dass die Kantone für Fragen der lnformationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden zu bezeichnen hätten (Art. 89 Abs. 3 ISG). Damit könne sichergestellt werden, dass der Informationsaustausch systematisch stattfinde und die Umsetzung der Massnahmen koordiniert erfolge.

NW wird die Bezeichnung einer kantonalen Dienststelle als Ansprechpartner in einer Einführungsverordnung zum ISG regeln. Bei NW sei die Informatiksicherheit dem Informatikleistungszentrum ILZ OVV/NW, mit Sitz in Sarnen, zugeteilt.

GL bezeichnet als kantonalen Ansprechpartner für Fragen der Informationssicherheit gegenüber der Bundesbehörde den Informatikdienst, Rathaus, 8750 Glarus.

ZG beantragt, Artikel 89 Absatz 1 und 3 wie folgt zu ändern bzw. zu ergänzen:

> «[1] Die Kantone sorgen dafür, dass kantonale Behörden und Stellen, die ~~im Auftrag des Bundes und unter seiner Aufsicht~~ in Zusammenarbeit mit dem Bund sicherheitsempfindliche Tätigkeiten ausüben, die Massnahmen nach diesem Gesetz umsetzen.
> [2] …
> [3] Die Kantone bezeichnen für Fragen der Informationssicherheit je eine Dienststelle als Ansprechpartner für die Bundesbehörden und die kantonalen Koordinationsorgane.»

Die Kantone ihrerseits sollen ein zentrales Organ als zuständige Kontakt- und Koordinationsstelle bezeichnen, zum Beispiel die bereichsübergreifende Konferenz der Kantonsregierungen KdK. So könnten die Auswirkungen auf die Kantone und die Fragen der Zusammenarbeit und Koordination zwischen Bund und Kantonen frühzeitig und fundiert angegangen werden. Generell regt ZG daher an, dass der Bund die Zusammenarbeit mit den Kantonen frühzeitig suche, wie dies Ziffer 3 der Rahmenordnung über die Arbeitsweise der KdK und der Direktorenkonferenzen bezüglich der Kooperation von Bund und Kantonen vom 28. September 2012 vorsehe.

SO geht davon aus, dass nur sehr wenige kantonale Mitarbeitende vom Gesetz erfasst würden. Der Botschaft liessen sich jedoch diesbezüglich keine näheren Angaben entnehmen. Auch wenn nur einzelne Kantonsmitarbeitende Aufgaben für den Bund wahrnehmen würden, habe dies zur Folge, dass die ganzen kantonalen ICT-Systeme den Anforderungen des ISG genügen müssten. Dies wäre mit sehr hohem Aufwand verbunden. SO bittet deshalb, zu prüfen, ob nicht analog der Regelung in Artikel 37 Absatz 1 des Datenschutzgesetzes die Zuständigkeit für die Informationssicherheit den Kantonen übertragen werden kann, sofern sie bestimmte Minimalstandards einhalten. Diese müssten im ISG oder in der Verordnung abschliessend aufgezählt werden.

BS sieht sich vom ISG nur betroffen, wenn nach Artikel 2 Absatz 2 Buchstabe f. ISG im Auftrag des Bundes sicherheitsempfindliche Tätigkeiten im Sinne von Artikel 2 Absatz 3 ISG ausgeübt würden. In diesem Fall müssten die Massnahmen gemäss Artikel 89 Absatz 1 ISG umgesetzt werden. Die Abteilung Informatiksteuerung und Organisation (ISO) habe mit der systematischen Vorbereitung des ISMS.BS (Informations-Sicherheits-Management-System) bereits Vorarbeiten geleistet, um das Gesetz bzw. die Massnahmen in BS umsetzen zu können. Die Kantone würden verpflichtet, eine Dienstelle für Fragen bezüglich Informationssicherheit zu definieren (Artikel 89 Absatz 3 ISG). Diese Dienststelle fungiere als Ansprechpartner für die Bundesbehörden. Mit dem kantonalen IT-Sicherheitsverantwortlichen in der ISO werde dies erfüllt.

AI beantragt, in Artikel 89 festzuhalten, dass der Bund die Kantone für sicherheitsempfindliche Tätigkeiten, die im Auftrag des Bundes und unter seiner Aufsicht ausgeübt würden, einschliesslich der dafür erforderlichen Infrastruktur vollständig entschädige. Die Aufwendungen der Kantone, die ihnen mit Tätigkeiten anfielen, die sie im Auftrag des Bundes ausübten, müssten vollständig entschädigt werden. Dies sollte im Gesetz ausdrücklich und unmissverständlich so festgehalten werden. Im weiteren sollten die Kantone für Leistungen gemäss Informationssicherheitsgesetz direkt und unentgeltlich auf die entsprechenden Fachstellen des Bundes zugreifen können. Auch diese Ergänzung sei in Artikel 89 vorzunehmen.

TG beantragt, Artikel 89 Absatz 2 des Entwurfes ISG ersatzlos zu streichen. Die Kantone seien bei der Auswahl des eigenen Personals unabhängig. Es gehe nicht, dass der Bund dem Kanton vorschreibe, wie dieser das eigene Personal auszuwählen habe. Selbst wenn es vorliegend nur darum gehe, dass Kantone im Auftrag des Bundes sicherheitsempfindliche Tätigkeiten ausführten, müsse es weiterhin in der Kompetenz der einzelnen Kantone liegen, welches Personal für welche Aufgaben eingesetzt werden dürfe. Zudem sei der Kanton aufgrund der Nähe zum eigenen Personal auch viel besser in der Lage, die Gefahrenpotenziale in den eigenen Reihen abschätzen zu können. Der Bund wird gebeten, die kantonale Hoheit zu beachten.

VD möchte Absatz 2 präzisieren: «Der Bundesrat regelt in Absprache mit den Kantonen …». Die Verordnung müsse die Tatsache berücksichtigen, dass eine unabhängige Stelle, wie etwa die kantonale Finanzkontrolle (beispielsweise in Fällen nach Art. 11 Abs. 2), gestützt auf einen speziellen Auftrag der kantonalen Exekutive ermächtigt sein kann, Massnahmen zu kontrollieren.

Entsprechend dem Auftrag nach Artikel 89 Absatz 3 bezeichnet GE die Generaldirektion für Informationssysteme als kantonale Ansprechstelle für die Informationssicherheit.

Die SIK beantragt, Artikel 89 mit einem neuen Absatz 4 wie folgt zu ergänzen:

> [4] Kantonale Behörden und Stellen können die Leistungen der in diesem Gesetz vorgesehenen Fachstellen des Bundes in Anspruch nehmen. Der Bundesrat kann vorsehen, dass für Leistungen an andere Behörden und Stellen als an diejenigen gemäss Absatz 1 kostendeckende Gebühren erhoben werden.

Es sei nicht sinnvoll und wäre teils wohl auch nicht möglich, das für die Aufgaben der Fachstellen PSP und BS notwendige spezialisierte Fachwissen vielfach dezentral in den Kantonen und Gemeinden aufzubauen. Daher müssten die Kantone die Dienste der Bundesfachstellen in Anspruch nehmen können. Soweit das ISG kantonale und kommunale Stellen direkt verpflichte (Art. 2 Abs. 2 Bst. f bzw. 89 Abs. 1 ISG), müssten die entsprechenden Leis-

tungen (z.B. die Durchführung von PSP) vom Bund finanziert werden. Soweit die Kantone das ISG in ihrem eigenen Verantwortungsbereich autonom umsetzten, z.B. durch die Einführung von PSP für weitere Kantonsangestellte, erscheine es angebracht, dass sie die dem Bund dafür entstehenden Kosten durch Gebühren tragen. Werde dieser Antrag nicht umgesetzt, seien Artikel 2 Buchstabe f und Artikel 89 zu streichen und stattdessen die Lösung des Datenschutzgesetzes vorzuziehen, wonach die Kantone für den Datenschutz auch im Rahmen der Erfüllung von Bundesaufgaben selbst zuständig seien, solange Minimalstandards eingehalten würden (Art. 37 DSG).

**Artikel 90** Völkerrechtliche Verträge

Der NDB weist darauf hin, dass sich der nachrichtendienstliche Informationsaustausch nach Artikel 12 Entwurf Nachrichtendienstgesetz richte.

### 7. Kapitel: Schlussbestimmungen

**Artikel 93** Übergangsbestimmungen

BE und die SIK beantragen, Artikel 93 mit einem neuen Absatz 3 wie folgt zu ergänzen: „[3] Verpflichtete Behörden der Kantone setzen dieses Gesetz bis spätestens fünf Jahre nach seinem Inkrafttreten um, soweit der Bundesrat nicht längere Übergangsfristen festlegt.“ Insbesondere im Bereich der ICT-Systeme könne die Umsetzung von Sicherheitsmassnahmen mit hohen Kosten verbunden sein, weil Anpassungen von Hard- und Software erforderlich seien. Oft werde es nicht mehr wirtschaftlich sein, ein altes System an neue Sicherheitsanforderungen anzupassen, weil die Beschaffung eines neuen Systems günstiger sei. Die Anpassung könne auch unmöglich sein, weil die Herstellerunternehmung den Support eingestellt habe oder nicht mehr existiere. Die Umsetzung der Anforderungen und Massnahmen gemäss ISG werde daher in der Regel im Rahmen der Ablösung alter Systeme durch neue erfolgen müssen. Die Übergangsfristen seien daher so festzulegen, dass sie dem typischen Lebenszyklus von ICT-Systemen Rechnung tragen. Die SIK möchte zudem noch einen zweiten Satz anfügen: „Das kantonale Recht kann in Abweichung von den Vorschriften des Bundes eine Übergangsfrist von bis zu zehn Jahren vorsehen, wenn eine frühere Umsetzung unverhältnismässig hohe Kosten verursachen würde.“

Für AB-BA besteht noch keine befriedigende Lösung für Personen, die derzeit nicht personensicherheitsüberprüft sind, dies aber nach den neuen Bestimmungen wohl sein müssten. Sie bekleideten aktuell Funktionen, die sicherheitsempfindliche Tätigkeiten beinhalten. Müsste für diese Personen nicht explizit eine Regelung getroffen werden? Hat für diese Personen nachträglich eine PSP stattzufinden, wäre in den Übergangsbestimmungen eine entsprechende Frist anzusetzen.

## 5.2 Änderung anderer Erlasse

Insecor vermisst im Entwurf weitergehende Abstimmungen mit Bundesgesetzen, welche Bezug zur Informationssicherheit haben (z.B. DSG, ZertES, FMG oder StGB) – insbesondere in Anbetracht aktueller Bedrohungen und Gefahren. Insecor empfiehlt dies weitestgehend zu überprüfen, insbesondere auch daraufhin, ob allenfalls gewisse Inhalte von Verordnungen (insb. BinfV, ISchV, VDSG) auf Gesetzesstufe angehoben werden sollten.

Insecor sieht folgende Aussage (vgl. Erläuternder Bericht, S. 15) als widersprüchlich an: „…die Verantwortlichen werden nur selten zur Rechenschaft gezogen“. Der vorliegende Entwurf enthalte weder Strafbestimmungen noch eine entsprechende Anpassung des Strafgesetzbuches (StGB; SR 311.0). Insecor regt an, diese Möglichkeit entsprechend zu prüfen.

## 6 Stellungnahmen zu den im erläuternden Bericht dargestellten Auswirkungen

Im Folgenden werden die Stellungnahmen zu den im erläuternden Bericht dargelegten Auswirkungen wiedergegeben. Es werden nur die Auswirkungen angeführt, zu denen explizit oder implizit Stellung genommen wurde.

**Allgemein**

TI hebt hervor, dass auf die Konsequenzen für Verfahren auf institutioneller Ebene, insbesondere verfahrensmässige Implikationen für die einzelnen beteiligten Stufen, auch wenn sie mit der Sicherheitsthematik nicht direkt in Zusammenhang stehen, nur unzureichend eingegangen werde und es im Übrigen keine spezifischen Anleitungen gebe.

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 bestünden heute weniger auf der konzeptionellen und legislativen Ebene, als in organisatorischen Mängeln und namentlich in der ungenügenden finanziellen und personellen Ausstattung der zuständigen Stellen.

## 6.1 Auswirkungen auf den Bund

Die CVP fordert, dass der Bundesrat in der Botschaft, wie im Bericht angekündigt, die Kosten, welche das Gesetz mit sich ziehen wird, detailliert erläutern wird. Speziell soll der Bundesrat die Kosten für die Konferenz der Informationssicherheitsbeauftragten sowie der Fachstelle des Bundes für Informationssicherheit darlegen. Die CVP verlangt zusätzlich, dass der Aufbau und der Betrieb des neuen Systems ohne zusätzliche Erhöhung des Personalbestandes erfolgen sollen.

Die FDP unterstreicht, dass die von diesem Gesetz ausgelösten realen technischen und organisatorischen Kosten noch nicht abgeschätzt werden können und dies frühestens am Ende des Konsultationsprozesses sein werden. Für die FDP ist es wichtig, dass zwischen dem Sicherheitsniveau und den dafür notwendigen Kosten ein Gleichgewicht gefunden wird, um eine Ausgabenexplosion zu verhindern.

Für die SP muss bei der Mittelverteilung die Priorität klar im zivilen und im alltäglichen Bereich gelegt werden. Es fehle 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 brauche 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 wolle, müsse 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 sei, zeige sich auch am erläuternden Bericht zum ISG, der sich um die Bezifferung der Folgekosten und zusätzlichen Stellen drücke. Ohne klare Antwort auf diese Frage würde aber auch das beste neue Gesetz nicht zu einem tatsächlichen Zugewinn an Sicherheit führen.

Die SP bekräftigt im Zusammenhang mit diesem konfliktträchtigen neuen Gesetz die Forderung, dem EDÖB endlich die nötigen Ressourcen zu geben. Der EDÖB nehme eine Schlüsselrolle bei der Etablierung einer guten Rechtspraxis betreffend Klassifizierung und Öffentlichkeitsprinzip ein. Denn es wäre niemandem gedient, aufgrund der Ressourcenknappheit nun oberflächlichere Empfehlungen zu Streitfällen abzugeben. Soweit das ISG dem EDÖB neue Aufgaben übertrage, müsse 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 werde, um diese wichtige, aber zusätzliche Aufgabe zu erfüllen.

Die Tatsache, dass im Bericht hinsichtlich der finanziellen und personellen Auswirkungen keine Zahlen genannt werden können (vgl. S. 75 des Erläuternden Berichts), macht für die swico deutlich, dass diese Gesetzesvorlage nicht ausgereift sei.

## 6.2 Auswirkungen auf die Kantone und Gemeinden

ZH beantragt, die Unklarheiten betreffend die Auswirkungen und den Einbezug der Kantone spätestens bei der Umsetzung des Gesetzes und dem Erlass der entsprechenden Ausführungsvorschriften auszuräumen. Dabei sei zwingend, dass den Belangen der Kantone im Allgemeinen und der ihnen zustehenden Organisationsautonomie im Besonderen gebührend Rechnung getragen wird.

Damit die Kantone und Gemeinden klar wüssten, in welchem Umfang sie durch das ISG verpflichtet seien, beantragt BE dies in einer Liste auf Verordnungsebene festzuhalten. Um die Auswirkungen des ISG auf die Kantone und Gemeinden abschätzen zu können, sollte bereits die Botschaft zum ISG eine Fassung dieser Liste aus heutiger Sicht enthalten. Sie sollte auch klarstellen, was unter „unter Aufsicht“ zu verstehen sei.

BE erwartet, dass die Kantone bzw. ihre Fachbehörden bei der Erarbeitung der Ausführungsbestimmungen des Bundes eng mit einbezogen würden, insbesondere soweit die Ausführungsbestimmungen auch die Kantone betreffen würden.

Für LU ist bezüglich der Kosten unklar, was auf die Kantone zukomme. Solange die bundesrätliche Verordnung mit den Ausführungsbestimmungen nicht bekannt sei, seien die Kostenfolgen für die Kantone schwierig abzuschätzen. LU fordert daher, dass vor der Verabschiedung dieses Gesetzes, klar dargelegt werde, was die Kostenfolgen für die Kantone seien und dass Gesetz und Ausführungsverordnungen so ausgestaltet würden, dass der Vollzug für die Kantone ohne grossen Verwaltungsaufwand erfolgen könne.

Für UR ist die zu erwartende Kostenfolge für die Kantone im Rahmen des Risikomanagements und der erforderlichen Sicherheits- und Schutzmassnahmen schwer abschätzbar. Hier sei vor allem von Seiten Bund das nötige Augenmass gefordert, damit Informationssicherheit auch für finanzschwächere Kantone tragbar sei. Sollte es allenfalls hierbei schon gewisse Vorstellungen des Bunds in Bezug auf die zu erwartenden Kosten und die Finanzierung generell geben, so sollten diese noch kommuniziert werden.

SZ kommt unter Würdigung von Botschaft und Vorlage zum Schluss, dass das ISG grundsätzlich keine Auswirkungen auf SZ habe. Die auf der gesetzlichen Grundlage folgenden Ausführungsbestimmungen könnten gewisse Auswirkungen im Bereich der erweiterten Personensicherheitsprüfung nach Artikel 39 Absatz 2 Buchstabe a i.V.m. Artikel 40 Absatz 1 ISG mit sich bringen. SZ gehe deshalb davon aus, dass SZ dannzumal auch zur Vernehmlassung der Ausführungsbestimmungen zur Stellungnahme eingeladen werde.

OW kann aus heutiger Sicht noch nicht beurteilen, welche konkreten Auswirkungen mit dem neuen Gesetz auf den Kanton zukommen werden, respektive von welchem Mehraufwand ausgegangen werden müsse. Gemessen am eher kleinen Anteil von Bundesaufgaben bezogen auf die gesamte Aufgabenerfüllung seiner Dienststellen, dürfte sich der Mehraufwand aber eher im engen Rahmen halten. Die kantonalen Strafverfolgungsbehörden seien bei ihrer Tätigkeit oft auf Informationen von Bundesbehörden angewiesen. Damit die an die kantonalen Behörden gelangenden Informationen den im Entwurf beabsichtigen Informationsschutz beibehalten würden, seien möglicherweise die Sicherheitsvorkehrungen auszubauen, was gerade bei kleineren Behörden zu entsprechendem Mehraufwand führen könnte. Dies müsse zu einem späteren Zeitpunkt geprüft werden.

NW geht davon aus, dass, falls dieses Gesetz gemäss der Vernehmlassungsfassung in Kraft trete, die für das ISG ausführenden Verordnungen für NW einen massiven operativen Aufwand verursachen könnten. Es gebe einige Artikel, welche je nach Geltungsbereich, ob einzelne Amtsstellen oder der ganze Kanton davon betroffen seien, unterschiedliche Anpassungen an Gesetzen, Verordnungen und Weisungen nach sich ziehen könnten. NW geht davon aus, dass NW auch bei der Vernehmlassung zu den entsprechenden Ausführungsbestimmungen wieder begrüsst werde.

Für GL schafft das neue Informationssicherheitsgesetz Klarheit für die Bundesbehörden. Für die Kantone wäre eine Zusammenfassung ihrer wesentlichsten Aufgaben, Kompetenzen und Verantwortlichkeiten ebenfalls nützlich. Hinsichtlich einzelner Begriffe bestehe zudem noch

Konkretisierungsbedarf. Insbesondere fehle es an Klarheit darüber, in welcher Form die einzelnen Kantone genau von Auflagen und von nötigen Ausbildungen betroffen seien.

Für ZG scheinen die Auswirkungen auf die Kantone im Gesetzesentwurf und im Bericht zu wenig durchdacht.

SO geht davon aus, dass nur sehr wenige kantonale Mitarbeitende vom Gesetz erfasst werden. Der Botschaft lasse sich jedoch diesbezüglich keine näheren Angaben entnehmen Auch wenn nur einzelne Kantonsmitarbeitende Aufgaben für den Bund wahrnehmen würden, habe dies zur Folge, dass die ganzen kantonalen ICT-Systeme den Anforderungen des ISG genügen müssten. Dies wäre mit sehr hohem Aufwand verbunden. SO bittet deshalb zu prüfen, ob nicht analog der Regelung in Artikel 37 Absatz 1 des Datenschutzgesetzes die Zuständigkeit für die Informationssicherheit den Kantonen übertragen werden kann, sofern sie bestimmte Minimalstandards einhalten. Diese müssten im ISG oder in der Verordnung abschliessend aufgezählt werden.

Für BS ergibt sich weder aus dem vorgeschlagenen Gesetzeswortlaut (Art. 2 Abs. 2 Bst. f ISG) noch aus den Erläuterungen klar, welche Tätigkeiten kantonaler Behörden in den Geltungsbereich fielen. BS regt an, Artikel 87 ISG um eine Bestimmung zu ergänzen, wonach der Bundesrat die Tätigkeiten gemäss Artikel 2 Absatz 2 Buchstabe f durch Verordnung festzulegen habe. Damit die Auswirkungen auf den Kanton abgeschätzt werden können, sollte bereits die Botschaft eine Fassung dieser Liste aus heutiger Sicht enthalten. Ausserdem sollte die Botschaft auch klarstellen, was unter «unter Aufsicht» zu verstehen ist.

Für BL dürfen den Kantonen aus der Unterstellung unter das neue Gesetz keine Kosten entstehen, da solche im erläuternden Bericht nicht ausgewiesen würden.

Da das neue Bundesgesetz zwar für die Ausübung sicherheitsempfindlicher Tätigkeiten den Rahmen vorgebe, aber für den Vollzug Spielräume enthalte, ist es für AI umso wichtiger, dass den Kantonen auch die Ausführungsverordnungen zur Vernehmlassung gegeben würden. Insbesondere erwartet AI, dass AI sich auch zur bundesrätlichen Verordnung äussern könne.

Für GR sind die Schnittstellen zwischen Bund und Kantonen im Entwurf nicht genügend klar geregelt. Es fehle eine genaue Umschreibung der Tätigkeiten und der Betroffenheit der Kantone. Damit keine Kompetenzschwierigkeiten bei der praktischen Umsetzung entstünden, seien diese bereits auf Gesetzesstufe differenziert zu regeln. Sollen die Kantone das ISG — direkt als verpflichtende Behörde oder im Rahmen der Übernahme von Vorschriften des ISG ins kantonale Recht — anwenden, so müsse den Kantonen die Möglichkeit eingeräumt werden, dass sie die gemäss ISG zu schaffenden zentralen Fachstellen des Bundes (insbesondere die Fachstellen Personensicherheitsprüfung und Betriebssicherheitsverfahren) ebenfalls beauftragen könnten. Die Anpassung der Systeme an die Sicherheitsmassnahmen könne zudem mit hohen Kosten verbunden sein. Der typische Lebenszyklus von ICT-Systemen betrage rund fünf bis zehn Jahre. Es seien deshalb für die Umsetzung des Gesetzes angemessene Übergangsfristen von mindestens fünf bis zehn Jahren vorzusehen.

Für AG bestehen im für die Kantone wesentlichen Bereich zum jetzigen Zeitpunkt mehrere offene Fragen. So solle erst im Ausführungsrecht geregelt werden, wie der Bund die Personensicherheitsprüfung für kantonale Angestellte regeln wolle. Folglich könnten heute keinerlei Rückschlüsse zur Art und Weise der Durchführung noch zu den konkreten Auswirkungen der Personensicherheitsprüfung auf das kantonale Personal gemacht werden. Ebenfalls noch nicht geklärt sei die Kontrolle der Umsetzung der Vorschriften in den Kantonen durch den Bund. Es sei unklar, wie sich das Prozedere und namentlich der Datenfluss in diesem Aufsichtsverfahren gestalten werden. Auch seien aus dem vorliegenden Erlassentwurf kaum Schnittstellen des Informationssicherheitsrechts mit der Datenschutzaufsicht der Kantone ersichtlich. Allerdings könne diese Frage nicht abschliessend beurteilt werden, da die wechselseitigen Beziehungen zwischen Datenschutz und Informationssicherheit – wenn überhaupt – im erläuternden Bericht nur marginal aufgezeigt würden. Immerhin sei dem Bericht konkludent ein Vorbehalt zugunsten des Bundesdatenschutzrechts zu entnehmen (vgl. erläuternder Bericht, Ziffer 1.3.1.2, Seite 28). AG geht davon aus, dass ein solcher Vorbehalt umso mehr für kantonales Datenschutzrecht gelte, nämlich in jenen Bereichen bundesrechtli-

chen Vollzugs durch die Kantone, die dem ISG unterstellt sein werden. Die dargelegten offenen Fragen müssten noch im Rahmen des Gesetzesverfahrens geklärt und in der Botschaft erläutert werden.

Für TI wird der Erlass des ISG selbstverständlich operative Konsequenzen auf Kantonsstufe haben. Die Auswirkungen, die das neue Gesetz, insbesondere die Klassifizierung der Informationen, auf die von der kantonalen Verwaltung verwendeten Systeme und gängigen Verfahren haben werde, seien zu prüfen; wahrscheinlich müsse die Vernetzung der Systeme Kanton – Bund angepasst werden, um den neuen Regelungen zu genügen. Die eventuelle Änderung der sektoriellen Gesetze in jenen Bereichen, in welchen Stellen der kantonalen Verwaltung Informationen an die Bundesverwaltung lieferten, müsse eingehender behandelt werden. Zum Beispiel: sind die Regelungen für die Betriebssicherheit auf die Wahl der Informatikprodukte anzuwenden, welche bei der Vernetzung mit dem Bund verwendet werden? Gibt es einen Bezug vom Kantonsgesetz über die Archivierung zu übergeordnetem Recht (Bundesgesetz über die Archivierung), wodurch Änderungen erforderlich würden?

### 6.3 Auswirkungen auf die Volkswirtschaft

Die meisten wirtschaftlichen Folgen dieses Gesetzes gehen in Richtung der Forderungen der FDP. Sie lassen sogar mit einer Verstärkung der Wettbewerbsfähigkeit der Unternehmen und einen besseren Schutz wirtschaftlicher Geheimnisse rechnen, die es unter den Schutz des Staates stellt.

Für CP und CVAM ist es im gegenwärtigen Stadium schwierig, sich zur Effektivität der vorgeschlagenen Massnahmen zu äussern. Immerhin lasse sich feststellen, dass anstelle von verschiedenen Bundesstellen angewandten unterschiedlichen Normen und Massnahmen zukünftig eine Rechtsregelung als Referenz gelten werde. Das werde die Sicherheit des Informationsflusses erleichtern, die Rechtssicherheit stärken und paradoxerweise das Öffentlichkeitsprinzip der Verwaltung begünstigen. Dieses bleibt jeweils vorbehalten, soweit keine auf dem ISG oder einem anderen Spezialgesetz basierende Massnahme anwendbar ist (Art. 3 Abs. 1 ISG)

## 7 Stellungnahmen zu den rechtlichen Aspekten

TI erachtet es als notwendig, dass die zukünftige Botschaft präzisiert, eventuell mit Bezug auf Art. 89 des Entwurfs, dass die Aufsicht durch den Bund die Kompetenzen der kantonalen Behörde zur Überwachung und Kontrolle des Datenschutzes nicht antastet und sie daher gewahrt blieben. Es sei wichtig hervorzuheben, dass die öffentlichen kantonalen Organe nicht zu Bundesorganen würden, unabhängig von der Art des Rechtsakts, mit welchem ihnen eine öffentliche Aufgabe des Bundes zugeteilt oder übertragen werde (Auftrag oder Delegation der Funktion). Ausser dem Spezialrecht des Bundes, welches das entsprechende Mandat oder die Delegation der Funktion festlege und eingrenze, blieben sie auch dem kantonalen Recht verpflichtet, d.h. dem des Datenschutzes.

Für CP und CVAM wirft der Entwurf des ISG weder unter verfassungsrechtlicher noch unter föderalistischer Sicht Probleme auf.