KANTON AARGAU

REGIERUNGSRAT

Regierungsgebäude, 5001 Aarau
Telefon zentral 062 835 12 40
Fax 062 835 12 50
regierungsrat@ag.ch
www.ag.ch/regierungsrat

A-Post Plus
Generalsekretariat VBS
Bundeshaus Ost
3003 Bern

23. November 2022

Ausführungsrecht zum Informationssicherheitsgesetz; Vernehmlassung

Sehr geehrte Damen und Herren

Die Kantonsregierungen wurden mit Schreiben vom 24. August 2022 eingeladen, zum Ausführungsrecht zum Informationssicherheitsgesetz (ISG) Stellung zu nehmen. Der Regierungsrat des Kantons Aargau bedankt sich für diese Gelegenheit und nimmt wie folgt Stellung:

1. Ausgangslage

Das Ausführungsrecht zum ISG umfasst drei neue Verordnungen (Informationssicherheitsverordnung [ISV], Verordnung über die Personensicherheitsprüfungen [VPSP], Verordnung über das Betriebssicherheitsverfahren [VBSV]) und eine teilrevidierte Verordnung (Verordnung über die Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes [IAMV]). Das Inkrafttreten des ISG mitsamt diesen Ausführungsverordnungen ist auf Mitte 2023 geplant.

Ein wichtiges Ziel der Vernehmlassung besteht darin, die Praxistauglichkeit der neuen Bestimmungen und die Kosten für die Kantone zu beurteilen. Aus diesem Grund stellt das Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) im Auftrag des Bundesrats den Kantonen folgende Fragen:

1. Ist die Umsetzung der Verordnungen für die Kantone verständlich?
2. Wie gedenken die Kantone, die Verordnungen umzusetzen?
3. Mit welchen finanziellen Auswirkungen rechnen die Kantone?
4. Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?

2. Grundsätzliches

Der Regierungsrat des Kantons Aargau unterstützt die Vorlage zum Ausführungsrecht zum ISG. Er begrüsst, dass die Kantone im Rahmen der Projektarbeiten vertreten waren.

Gestützt auf die vorliegenden Unterlagen gehen wir davon aus, dass die Kantone von der Vorlage lediglich in beschränkter Weise betroffen sind, nämlich insbesondere in folgenden Punkten:

- Für die Kantone gelten gemäss Art. 2 Abs. 6 E-ISV lediglich die Bestimmungen der E-ISV betreffend klassifizierte Informationen (4. Abschnitt) und die Art. 28-30 sowie 34, sofern sie keine gleichwertige Informationssicherheit gewährleisten. Das heisst, diese Bestimmungen gelten für diejenigen kantonalen Stellen, die auf Informatikmittel des Bundes zugreifen oder klassifizierte Informationen des Bundes bearbeiten. Die Umsetzung dieser Vorgaben erfolgt im Kanton Aargau zumindest vorläufig voraussichtlich auf der operativen Ebene durch Anpassung der entsprechenden Vorgaben. Geplant ist jedoch, dass im Kanton Aargau bis im Jahr 2025 die gesetzlichen Grundlagen für die Informationssicherheit geschaffen werden. Im Rahmen der entsprechenden Rechtssetzungsarbeiten sollen das ISG und dessen Ausführungsrecht berücksichtigt und umgesetzt werden.
- Aus der E-VPSP sind für die Kantone die Art. 8 Abs. 1 E-VPSP und Art. 35 E-VPSP von Belang. Während Art. 8 Abs. 1 VPSP Personensicherheitsprüfungen (PSP) von kantonalen Angestellten normiert, welche sicherheitsempfindliche Aufgaben des Bundes ausüben (vgl. Art. 29 Abs. 1 Bst. b ISG und BBl 2017 2953 ff., S. 3070 und 3086), schafft Art. 35 E-VPSP die Möglichkeit, dass Kantone künftig Leistungen der Fachstelle PSP des VBS in Anspruch nehmen können (Art. 35 E-VPSP).
- Nach unserem Verständnis betrifft die Vorlage ansonsten die Kantone nicht. Insbesondere gehen wir mangels Anwendbarkeit auf die Kantone (es fehlt eine analoge Norm zu Art. 2 Abs. 6 E-ISV) davon aus, dass die Kantone die E-VBSV und die E-IAMV nicht umsetzen müssen.

Der Regierungsrat des Kantons Aargau nimmt mit Bedauern zur Kenntnis, dass in der E-VBSV keine Möglichkeit zum Leistungsbezug betreffend die Durchführung von Betriebssicherheitsverfahren (BSV) analog Art. 35 E-VPSP vorgesehen ist (vgl. hierzu Ziffer 4.4).

3. Beantwortung der Fragen

3.1 Ist die Umsetzung der Verordnungen für die Kantone verständlich?

Die Umsetzung der Verordnungen ist für den Regierungsrat des Kantons Aargau grundsätzlich verständlich. In Bezug auf die Bestimmungen, welche für die Kantone von Belang sind, äussern wir uns detailliert in nachfolgender Ziffer 4.

3.2 Wie gedenken die Kantone, die Verordnungen umzusetzen?

Die Umsetzung der E-ISV (das heisst Bestimmungen des 4. Abschnitts sowie der Art. 28–30 sowie Art. 34) und von Art. 8 E-VPSP erfolgen im Kanton Aargau zumindest vorläufig auf der operativen Ebene durch Anpassung der entsprechenden Vorgaben aufgrund der Anweisungen durch die für die Informatikmittel des Bundes zuständigen Verwaltungseinheiten des Bundes. Geplant ist jedoch, dass der Kanton Aargau im Jahr 2025 über neue gesetzliche Grundlagen für die Informationssicherheit sowie entsprechendes Ausführungsrecht verfügt. Im Rahmen der entsprechenden Rechtssetzungsarbeiten sollen das ISG und dessen Ausführungsrecht berücksichtigt und die Umsetzung überprüft sowie allenfalls optimiert werden.

Wie unter Ziffer 2 erwähnt, sind die E-VBSV und die Verordnung über die IAMV durch die Kantone mangels Anwendbarkeit nicht umzusetzen, weshalb sich hierzu weitere Ausführungen erübrigen.

3.3 Mit welchen finanziellen Auswirkungen rechnen die Kantone?

Der Kanton Aargau greift auf diverse Informatikmittel des Bundes zu und bearbeitet eine Vielzahl klassifizierter Informationen des Bundes. Der Regierungsrat des Kantons Aargau geht dennoch davon aus, dass die geplanten Rechtsänderungen aufgrund der heute bereits geltenden Sicherheitsmassnahmen (spezifische Vorschriften der federführenden Bundesämter, Benutzerprüfung und -verwaltung durch den Bund, kantonales Recht, etc.) für den Kanton Aargau beziehungsweise dessen

Mitarbeiterinnen und Mitarbeiter keine erheblichen Veränderungen bedeuten. Ein grösserer Mehraufwand ist ebenfalls nicht ersichtlich, soweit sich dies heute überhaupt feststellen lässt.

3.4 Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?

Kantonale Dienststelle für Fragen der Informationssicherheit ist im Kanton Aargau die Abteilung Informatik Aargau:

Departement Finanzen und Ressourcen
Informatik Aargau
Informationssicherheit
Suhrenmattstrasse 48
5035 Unterentfelden
Tel: 062 835 10 27
dominik.freitag@ag.ch

4. Zu den einzelnen Bestimmungen der Verordnungen

4.1 E-ISV

4.1.1 Art. 2 Abs. 6 E-ISV

Gemäss dieser Bestimmung gelten für die Kantone bei der Bearbeitung von klassifizierten Informationen des Bundes die Bestimmungen des 4. Abschnitts (Art. 16-26 E-ISV) und beim Zugriff auf Informatikmittel des Bundes die Art. 28-30 und 34 E-ISV. Das heisst, diese Bestimmungen gelten für diejenigen kantonalen Stellen, die Bundesapplikationen oder klassifizierte Informationen des Bundes bearbeiten. *"Die Kantone können sich allerdings von den bundesrechtlichen Vorgaben befreien, wenn sie von sich aus eine gleichwertige Informationssicherheit gewährleistet. Dies setzt voraus, dass sie eigene, an die Bundesstandards angeglichene Sicherheitsvorschriften erlassen, die sie in ihrem Zuständigkeitsbereich durchsetzen. Massgebende Bundesstandards sind die Vorschriften und technischen Anforderungen für den Grundschutz der Informatik im Bund sowie für den Schutz von klassifizierten Informationen. Die Kantone sind nicht verpflichtet, ein ISMS nach Art. 5 ff. umzusetzen. Eine «gleichwertige Informationssicherheit» liegt vor, wenn andere als in der ISV vorgesehene Sicherheitsvorkehrungen nach dem Stand der Technik gemäss Artikel 85 Absatz 1 ISG eine vergleichbare und mindestens gleich hohe beziehungsweise starke Wirkung erzielen. Die Kantone beurteilen in erster Linie in eigenem Ermessen, ob eine gleichwertige Informationssicherheit vorliegt."* (vgl. Erläuternder Bericht zum Ausführungsrecht zum ISG vom 24. August 2022, S. 12 zu Art. 2).

Diese angebliche Eigenbeurteilung erfolgt nur "in erster Linie" und kontrastiert in zweiter Linie damit, dass der Bund über den Zugang zu den Informatikmitteln des Bundes entscheidet (vgl. Erläuternder Bericht zum Ausführungsrecht zum ISG vom 24. August 2022, S. 12 zu Art. 2: *"Ob ein Zugriff besteht, entscheidet letztlich der Bund."*) und ein komplexes System der Zugangsberechtigung aufbaut, bei dem die Gleichwertigkeit schwierig nachzuweisen sein dürfte. Es ist daher aufzuzeigen, wie sich die Kantone bei einem vom Bund abgelehnten Zugriff zur Wehr setzen könnten, andernfalls bleibt diese Ausnahmebestimmung toter Buchstabe. Die Eigenverantwortung würde faktisch wohl nur beim reinen Bearbeiten von Daten gelten.

4.1.2 Art. 16 E-ISV

Art. 16 E-ISV ist verständlich, wird aber vom Kanton Aargau in der beschriebenen Form heute nicht umgesetzt. Eine Umsetzung ist möglich, wobei der Aufwand dazu für uns nicht abschätzbar ist.

4.1.3 Art. 17 E-ISV

Da die Kantone beziehungsweise deren Personen und Stellen in Art. 17 E-ISV nicht als klassifizierende Stellen aufgeführt sind und Dritte gemäss erläuterndem Bericht keine klassifizierenden Stellen sind (vgl. Erläuternder Bericht zum Ausführungsrecht zum ISG vom 24. August 2022, S. 18 zu Art. 17), ist nicht ersichtlich inwiefern diese Bestimmung für die Kantone von Belang sein sollte.

4.1.4 Art. 18-20 E-ISV

Diese Bestimmungen sind verständlich. Der Kanton Aargau verwendet derzeit die vier Klassifizierungsstufen "öffentlich", "intern", "vertraulich" und "geheim". Im Gegensatz zu Art. 18-20 E-ISV verwendet der Kanton Aargau für Informationen, die nicht explizit als "intern", "vertraulich" oder "geheim" klassifiziert sind die Klassifizierungsstufe "öffentlich". Weiter unterscheiden sich die Merkmale der Klassifizierungsstufen, das heisst, deren Definitionen. Ob und inwiefern diese Tatsache Kongruenzprobleme und mithin Schwierigkeiten bei der Umsetzung (beispielsweise erhöhte Aufwendungen) impliziert, ist für uns derzeit noch unklar.

4.1.5 Art. 21 E-ISV

Da die generell-abstrakten Weisungen gemäss Art. 21 Abs. 1 E-ISV einzig für die Stellen nach Art. 2 Abs. 1-3 E-ISV und damit nicht für die in Art. 2 Abs. 6 E-ISV aufgeführten Kantone gelten (vgl. auch Erläuternder Bericht zum Ausführungsrecht zum ISG vom 24. August 2022, S. 19 zu Art. 21), erübrigt sich eine Stellungnahme zu Art. 21 E-ISV. Es ist daher fraglich und durch den Bund darzulegen, welche Bearbeitungsvorgaben für die Kantone gelten, wer diese erlässt und allenfalls in welcher Form die Kantone vorgängig angehört werden.

4.1.6 Art. 22 und 23 E-ISV

Das Erfordernis einer Umsetzung dieser Bestimmungen ist nicht ersichtlich.

4.1.7 Art. 24 E-ISV

Art. 24 E-ISV ist verständlich und umsetzbar beziehungsweise Art. 24 E-ISV wird bereits sinngemäss für vom Kanton klassifizierte Informationen umgesetzt. Der Aufwand zur Umsetzung dürfte, wenn überhaupt ein zusätzlicher Aufwand anfällt, minim sein.

4.1.8 Art. 25 E-ISV

Da es in den Kantonen keine klassifizierenden Stellen gemäss Art. 17 E-ISV gibt, gehen wir davon aus, dass diese Bestimmung für die Kantone nicht von Belang ist.

4.1.9 Art. 26 E-ISV

Art. 26 E-ISV ist verständlich und umsetzbar. Der Aufwand hierfür ist derzeit nicht abschätzbar.

4.1.10 Art. 28 E-ISV

Art. 28 E-ISV ist verständlich und umsetzbar beziehungsweise wird in Projekten bereits sinngemäss umgesetzt. Die Umsetzung von Art. 28 E-ISV ist möglich, der Aufwand dazu jedoch derzeit nicht abschätzbar.

4.1.11 Art. 29 E-ISV

Da die generell-abstrakten Weisungen gemäss Art. 29 Abs. 1 E-ISV einzig für die Stellen nach Art. 2 Abs. 1-3 E-ISV und damit nicht für die in Art. 2 Abs. 6 E-ISV aufgeführten Kantone gelten (vgl. auch Erläuternder Bericht zum Ausführungsrecht zum ISG vom 24. August 2022, S. 21 zu Art. 29), erübrigt sich eine Stellungnahme zu Art. 29 E-ISV. Es ist daher fraglich und durch den Bund darzulegen, welche Mindestanforderungen für die jeweiligen Sicherheitsstufen für die Kantone gelten, wer diese erlässt und allenfalls in welcher Form die Kantone vorgängig angehört werden.

Sollte Art. 29 E-ISV – entgegen unserer Auffassung – für die Kantone gelten, ist er verständlich und erscheint umsetzbar, soweit dies derzeit überhaupt beurteilt werden kann, hängt doch die Umsetzung weitgehend von den uns nicht vorliegenden generell-abstrakten Weisungen über die Mindestanforderungen für die jeweiligen Sicherheitsstufen nach Art. 17 ISG ab. Für Informatikmittel des Kantons setzt der Kanton Aargau Art. 29 E-ISV sinngemäss um.

4.1.12 Art. 30 E-ISV

Art. 30 E-ISV ist verständlich und umsetzbar, der Aufwand dazu jedoch derzeit nicht abschätzbar.

4.1.13 Art. 34 E-ISV

Da die generell-abstrakten Weisungen gemäss Art. 34 Abs. 1 E-ISV einzig für die Stellen nach Art. 2 Abs. 1-3 E-ISV und damit nicht für die in Art. 2 Abs. 6 E-ISV aufgeführten Kantone gelten (vgl. auch Erläuternder Bericht zum Ausführungsrecht zum ISG vom 24. August 2022, S. 22 zu Art. 34), erübrigt sich eine Stellungnahme zu Art. 34 E-ISV. Es ist daher fraglich und durch den Bund darzulegen, welche minimal erforderlichen Massnahmen zum physischen Schutz von Informationen und Informatikmitteln für die Kantone gelten, wer diese erlässt und allenfalls in welcher Form die Kantone vorgängig angehört werden.

Sollte Art. 34 E-ISV – entgegen unserer Auffassung – für die Kantone gelten, ist er nicht verständlich. Massnahmen für den physischen Schutz von Informationen und Informatikmitteln sollten sich nach deren Schutzbedarf, das heisst nach deren Sicherheitsstufe richten – Art. 34 Abs. 2 E-ISV widerspricht diesem Grundsatz. Mit der Nennung von physischen Schutzmassnahmen in Art. 35 E-ISV würde Art. 34 E-ISV hinfällig. Ansonsten erscheint Art. 34 E-ISV umsetzbar, soweit dies derzeit überhaupt beurteilt werden kann, hängt doch die Umsetzung weitgehend von den uns nicht vorliegenden generell-abstrakten Weisungen über die minimal erforderlichen Massnahmen zum physischen Schutz von Informationen und Informatikmitteln ab.

4.2 E-IAMV

Die Kantone sind nicht vom Geltungsbereich dieser Verordnung erfasst, weshalb auf eine Stellungnahme zur E-IAMV verzichtet wird.

4.3 E-VPSP

4.3.1 Art. 8 Abs. 1 E-VPSP

Art. 8 Abs. 1 VPSP normiert PSP von kantonalen Angestellten, welche sicherheitsempfindliche Aufgaben des Bundes ausüben (vgl. Art. 29 Abs. 1 Bst. b ISG und BBl 2017 2953 ff., S. 3070 und 3086). Zunächst müssen im Kanton Aargau die Funktionen von Angestellten festgelegt werden, die einer Prüfung nach Art. 29 Abs. 1 Bst. b ISG unterstehen sollen. Im Interesse einer einheitlichen Vollzugspraxis erachten wir betreffend die Festlegung dieser Funktionen eine Klärung als angezeigt. Wünschenswert wäre, wenn hierzu der Erläuternde Bericht zum Ausführungsrecht zum ISG in geeigneter Form publiziert oder zumindest den Kantonen zur Verfügung gestellt würde. Weiter gilt es bei Inkrafttreten dieser Bestimmung den Ablauf der Antragsstellung an das VBS zu definieren. Beides dürfte mit verhältnismässig geringem Aufwand für den Kanton Aargau möglich sein.

4.3.2 Art. 35 E-VPSP

Art. 35 E-VPSP schafft die Möglichkeit, dass Kantone künftig Leistungen der Fachstelle PSP VBS in Anspruch nehmen können (Art. 35 E-VPSP). Zur Umsetzung müssten wir eine gesetzliche Grundlage gemäss Art. 35 Abs. 1 Bst. a E-VPSP schaffen, was im Rahmen der geplanten Schaffung von gesetzlichen Regelungen zur Informationssicherheit bis zirka im Jahr 2025 möglich wäre. Die Voraussetzungen gemäss den Buchstaben b und c könnten ebenfalls ohne grösseren Aufwand erfüllt werden. Insbesondere dürfte der Kanton in den geplanten neuen Rechtssätzen für die Informations-

sicherheit für durch den Kanton Aargau selber durchgeführte PSP ähnliche Beurteilungen zur Gewährleistungen der Informationssicherheit vornehmen. Die Höhe der Gebühren in Absatz 3 erachten wir als angemessen.

Ungeachtet der vorstehenden Ausführungen ist derzeit nicht vorgesehen, PSP künftig an den Bund auszulagern.

4.4 E-VBSV

Gemäss Art. 1 Abs. 2 E-VBSV gilt die Verordnung unter Vorbehalt von Art. 84 Abs. 3 ISG und Art. 2 Abs. 2-5 der ISV für die verpflichteten Behörden und Organisationen nach Art. 2 ISG. Da die Kantone in Art. 2 ISG nicht aufgeführt sind, gilt die E-VBSV für die Kantone folglich nicht. Es erübrigen sich daher Ausführungen zur Verständlichkeit und Umsetzbarkeit dieser Verordnung.

Der Regierungsrat des Kantons Aargau würde es sehr begrüssen – wenn, wie in der (17.028) Botschaft zum Informationssicherheitsgesetz vom 22. Februar 2017 zumindest angedeutet (BBl 2017 2953 ff., S. 3070 f.) – betreffend die Durchführung von BSV analog Art. 35 E-VPSP die Möglichkeit eines Leistungsbezugs der Kantone bei der Fachstelle Betriebssicherheit (BS) des Bundes geschaffen würde. Dies daher, weil es für den Kanton Aargau und wohl auch eine Vielzahl anderer Kantone aus finanziellen Gründen kaum verhältnismässig sein dürfte, ein eigenes BSV einzuführen.

Wir danken Ihnen für die Berücksichtigung unserer Vernehmlassung.

Im Namen des Regierungsrats

Alex Hürzeler
Landammann

Joana Filippi
Staatsschreiberin

Kopie
- sicherheit.vbs@qs-vbs.admin.ch

KANTON
APPENZELL INNERRHODEN

Landammann und Standeskommission

Sekretariat Ratskanzlei
Marktgasse 2
9050 Appenzell
Telefon +41 71 788 93 11
info@rk.ai.ch
www.ai.ch

Ratskanzlei, Marktgasse 2, 9050 Appenzell

Per E-Mail an
sicherheit.vbs@gs-vbs.admin.ch

Appenzell, 24. November 2022

Ausführungsrecht zum Informationssicherheitsgesetz
Stellungnahme Kanton Appenzell I.Rh.

Sehr geehrte Damen und Herren

Mit Schreiben vom 24. August 2022 haben Sie uns die Vernehmlassungsunterlagen zum Ausführungsrecht zum Informationssicherheitsgesetz zukommen lassen.

Die Standeskommission hat die Unterlagen geprüft. Sie beantwortet Ihre Fragen wie folgt:

Frage 1:

Die Umsetzung der Verordnungen ist für unseren Kanton verständlich.

Frage 2:

Einige Anforderungen hat der Kanton Appenzell I.Rh. schon im Rahmen der Netzdomänenpolicy (NSP) KOMBV-KTV umgesetzt. Insbesondere im Bereich der Cyber-Security wurde in den vergangenen Jahren sehr viel investiert und die nötigen Massnahmen umgesetzt. Es wird geprüft, ob die Rolle des Sicherheitsverantwortlichen und Informationssicherheitsbeauftragten intern oder extern vergeben wird.

Frage 3:

Finanzielle Auswirkungen ergeben sich für den Kanton Appenzell I.Rh. hinsichtlich der Schaffung einer zusätzlichen Stelle.

Frage 4:

Der Kanton Appenzell I.Rh. bezeichnet Karl Dähler, Leiter des Amts für Informatik, als kantonale Ansprechperson für die Bundesbehörden für Fragen der Informationssicherheit.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Im Auftrage von Landammann und Standeskommission
Der Ratschreiber:

Markus Dörig

Zur Kenntnis an:
- Justiz-, Polizei- und Militärdepartement Appenzell I.Rh., Marktgasse 10d, 9050 Appenzell
- Amt für Informatik, Marktgasse 2, 9050 Appenzell
- Ständerat Daniel Fässler, Weissbadstrasse 3a, 9050 Appenzell
- Nationalrat Thomas Rechsteiner (thomas.rechsteiner@parl.ch)

Appenzell Ausserrhoden

Regierungsrat

Obstmarkt 3
9102 Herisau
Tel. +41 71 353 61 11
kantonskanzlei@ar.ch
www.ar.ch

Regierungsrat, 9102 Herisau

Eidg. Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
3003 Bern

Dr. iur. Roger Nobs
Ratschreiber
Tel. +41 71 353 63 51
roger.nobs@ar.ch

Herisau, 18. November 2022 / ssc

Eidg. Vernehmlassung Ausführungsrecht zum Informationssicherheitsgesetz; Stellungnahme des Regierungsrates von Appenzell Ausserrhoden

Sehr geehrte Damen und Herren

Mit Schreiben vom 24. August 2022 wurden die Kantonsregierungen vom Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport VBS eingeladen, sich zum Ausführungsrecht des neuen Informationssicherheitsgesetzes (ISG) bis 24. November 2022 vernehmen zu lassen.

Der Regierungsrat von Appenzell Ausserrhoden nimmt dazu wie folgt Stellung:

Zur Informationssicherheitsverordnung, zur Verordnung über die Personensicherheitsprüfungen, zur Verordnung über das Betriebssicherheitsverfahren sowie zur Teilrevision der Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes hat der Regierungsrat materiell grundsätzlich keine Bemerkungen und verzichtet daher auf eine umfassende Stellungnahme.

Zu den im Begleitschreiben vom 24. August 2022 aufgeführten Fragen nimmt der Regierungsrat wie folgt Stellung:

Frage 1: Ist die Umsetzung der Verordnungen für die Kantone verständlich?

Ja, die Umsetzung der Verordnungen ist verständlich.

Frage 2: Wie gedenken die Kantone, die Verordnungen umzusetzen?

Im Moment werden die Personensicherheitsüberprüfungen durch die Kriminalpolizei gemacht. Diese Aufgabe wird in absehbarer Zeit zur Kantonalen Notrufzentrale (KNZ) wechseln. Die Auftragserteilung erfolgt über das System SIBAD bzw. in Zukunft allenfalls über ein angepasstes Informationssystem (vgl. Erläuternder Bericht / Ausführungsrecht zum Informationssicherheitsgesetz, Punkt 3.8 / Seite 11).

Der Kanton Appenzell Ausserrhoden verfügt nicht über vollständige und durchgängig anwendbare Vorschriften zur allgemeinen Informationssicherheit, die in der Summe ein gleichwertiges Niveau erreichen, wie sie das ISG vorsieht. Damit würden Teile der ISV im Kanton direkt anwendbar, soweit klassifizierte Informationen des Bundes bearbeitet werden oder auf Informatikmittel des Bundes zugegriffen wird (Art. 2 Abs. 6 E-ISV). Die konkrete Umsetzung ist daher noch vertieft zu prüfen.

Für den Regierungsrat erscheint zudem fraglich, ob die Bundesverfassung die Kantone – ausserhalb der im Rahmen des Personendaten-, also des Persönlichkeits- und Privatsphärenschutzes zu beachtenden Vorgaben zur (Personen-)Datensicherheit – zu allgemeiner Informationssicherheit verpflichtet. Gleichzeitig ist augenscheinlich, dass durch eine Erhöhung der allgemeinen Informationssicherheit auch der Personendatenschutz profitieren würde.

Frage 3: Mit welchen finanziellen Auswirkungen rechnen die Kantone?

Je nach Umsetzung ist mit erheblichen finanziellen Auswirkungen zu rechnen. Diese können aber zum heutigen Zeitpunkt aus Sicht des Regierungsrates nicht abgeschätzt werden.

Namentlich Leistungen der Fachstellen PSP zugunsten der Kantone sind in Art. 35 VPSP geregelt. Die Fachstelle PSP VBS ist für die Personensicherheitsüberprüfungen der Kantone zuständig. Für die Inanspruchnahme müssen die Kantone über eine eigene rechtliche Grundlage verfügen. Das VBS würde zudem mit dem jeweiligen Kanton eine Leistungsvereinbarung abschliessen. Im Kanton Appenzell Ausserrhoden werden Personen/Amtsträger keiner Personensicherheitsüberprüfung unterzogen. Die Fachstelle PSP wurde daher offenbar noch nie in Anspruch genommen.

Frage 4: Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?

Das Departement Inneres und Sicherheit (Departementssekretariat).

Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Im Auftrag des Regierungsrates

Dr. iur. Roger Nobs, Ratschreiber

Landeskanzlei
Rathausstrasse 2
4410 Liestal
T 061 552 50 06
landeskanzlei@bl.ch
www.bl.ch

BASEL LANDSCHAFT
REGIERUNGSRAT

Regierungsrat, Rathausstrasse 2, 4410 Liestal

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport

sicherheit.vbs@gs-vbs.admin.ch

Liestal, 22. November 2022

Vernehmlassung betreffend Ausführungsrecht zum Informationssicherheitsgesetz

Sehr geehrte Frau Bundesrätin

Besten Dank für die Möglichkeit zur Meinungsäusserung. Grundsätzlich können wir dem vorgeschlagenen Ausführungsrecht zum Informationssicherheitsgesetz zustimmen. Die Umsetzungsfrist bis am 1. April 2025 für die Klassifizierung der Systeme und bis am 1. April 2029 für die Umsetzung der technischen Sicherheitsmassnahmen erachten wir als ausreichend.

Zum vorgeschlagenen Ausführungsrecht nehmen wir anhand des im Einladungsschreiben formulierten Fragekatalogs Stellung:

1. Ist die Umsetzung der Verordnungen für die Kantone verständlich?
Der Grundsatz des Informationssicherheitsgesetzes ist verständlich, insbesondere das legitime Anliegen des Bundes, Mindestvorgaben zur Absicherung seiner Informationssysteme zu erlassen, auch für Benutzende ausserhalb der Bundesverwaltung. Auf der anderen Seite führt die jetzt vorgeschlagene Lösung, dass die Regeln des Bundes dann nicht für die Kantone anwendbar sein sollen, wenn deren Sicherheitsmassnahmen mindestens gleichwertig sind, nicht zu genügend Klarheit. Was gleichwertig wäre, ist für den Kanton Basel-Landschaft beim heutigen Stand der Vorschläge für das Ausführungsrecht nicht beurteilbar, insbesondere weil die Vorgaben sehr umfangreich sind und weil sie teilweise noch sehr allgemein gehalten und durch Weisungen des Nationalen Cyber Security Centers (NCSC) zu konkretisieren sind.

Aus kantonaler Sicht wäre eine andere Lösung erfolgversprechender: In Anlehnung an die heutigen Regelungen in der Zusammenarbeit zwischen dem Nachrichtendienst des Bundes (NDB) und den Kantonalen Nachrichtendiensten (KND) bei der Bearbeitung klassifizierter Informationen wäre viel klarer und einfacher umsetzbar, wenn die Kantone bei der Bearbeitung klassifizierter Informationen des Bundes und bei Anschlüssen an Informationssysteme und Datensammlungen des Bundes einfach die Sicherheitsvorgaben des Bundes für diese Bearbeitungen beachten und erfüllen müssten.

Vorgaben zur Informationssicherheit sind auf Grund des technischen Fortschritts und der Spannbreite der Technologien immer generisch verfasst. Diese Vorgaben müssen immer wieder interpretiert und deren Umsetzung fortlaufend überprüft werden. Es wird daher zwangsweise zu Abweichungen zwischen dem Bund und einzelnen Kantonen kommen, welche identifiziert und gegebenenfalls mit Ausnahmeregelungen behoben werden müssen.
Die Umsetzung des Informationssicherheitsgesetzes ist zurzeit nicht verständlich, weil darin Regeln, Prozesse und Referenzen fehlen, um einerseits die Ausrichtung der IT-Sicherheitsmassnahmen detaillierter vorzugeben und zweitens den Umgang mit Abweichungen zu klären.
Dafür bestehen bisher aber nur Andeutungen erstens zur Verantwortlichkeit des Nationalen Zentrums für Cybersicherheit (NCSC) für die Definition von Vorgaben und zweitens der Meldepflicht der Kantone, um dem Bund Bericht abzugeben über die Umsetzung der IT-Sicherheitsmassnahmen.
Um die bestehenden Unklarheiten zu beheben schlägt der Kanton Basel-Landschaft folgende Lösungsansätze vor:

1. Der Bund definiert einen oder mehrere international etablierte Standards im Bereich der Informationssicherheit, wovon die Kantone mindestens einen auswählen und befolgen müssen, um Zugriff auf die Informationssysteme des Bundes zu erhalten.
2. Das NCSC definiert die minimalen IT-Sicherheitsmassnahmen welche umgesetzt werden müssen, um Zugriff auf die vertraulichen IT-Systeme des Bundes zu erhalten.
3. Das NCSC erarbeitet zusammen mit der Arbeitsgruppe Cyber Security der Digitalen Verwaltung Schweiz (DVS) die folgenden Grundsätze:
   - 3a) Abwicklung der Meldepflicht über die Umsetzung der Sicherheitsmassnahmen in den Kantonen zu Handen des Bundes.
   - 3b) Mindestanforderungen und Prozess zur Anerkennung der Gleichwertigkeit der kantonalen Informationssicherheit.
   - 3b) Prozess zur Meldung und Akzeptanz und/oder Behebung von Abweichungen gegenüber den Sicherheitsvorgaben.

Ein weiterer Punkt, der im Ausführungsrecht unklar bleibt: Es gibt auch Gemeinden und möglicherweise andere Organisationen, wie öffentlich-rechtliche Anstalten und Betriebe in den Kantonen, die ebenfalls an Informationssystemen des Bundes angeschlossen sind. Das Ausführungsrecht in der heutigen Fassung stellt nicht klar, wer für die Einhaltung der Sicherheitsmassnahmen durch diese Organisationen zu sorgen hätte. Die Kantone können es für die Gemeinden jedenfalls nicht sein. Auch deshalb wäre eine Ausgestaltung im eben vorgeschlagenen Rahmen wesentlich zielführender, dass wer sich an Informationsmitteln des Bundes anschliessen will, die Vorgaben des Bundes für die jeweiligen Anschlüsse erfüllen muss und sonst nicht angeschlossen werden kann. Damit würde viel mehr Klarheit und Einfachheit geschaffen und die Sicherheitsmassnahmen könnten wirkungsvoll umgesetzt werden.

2. Wie gedenken die Kantone, die Verordnungen umzusetzen?
Die Übergangsfristen mit 1. April 2025 (Klassifizierung) und 1. April 2029 (Umsetzung) sind aus Sicht des Kantons Basel-Landschaft ausreichend, um die noch offenen Fragestellungen zu klären und die Vorgaben anschliessend angemessen umzusetzen.
Im Bereich der Informatik kann die Umsetzung des Informationssicherheitsgesetzes kombiniert werden mit der anstehenden Umsetzung der neuen Nationalen Cyberstrategie NCS 2023+.
Im Bereich der Personensicherheitsprüfung PSP geht der Kanton Basel-Landschaft davon aus, dass kein Anpassungsbedarf besteht.

3. Mit welchen finanziellen Auswirkungen rechnen die Kantone?
Nach Einschätzung des kantonalen Informationssicherheitsbeauftragten entstehen dem Kanton Basel-Landschaft für die Umsetzung des Informationssicherheitsgesetzes keine wesentlichen Zusatzkosten. Die meisten zu erwartenden Arbeiten und Aufwände können als Anforderungen in bereits geplanten Projekte mit aufgenommen und abgewickelt werden.
Betreffend den Personensicherheitsprüfungen PSP werden keine Anpassungen erwartet. Mehraufwände im Team der Informationssicherheit für Abstimmungen, Abklärungen und Prüfungen sind zu erwarten, welche aber als Erweiterung des Tagesgeschäfts beim bestehenden Sicherheitsteam betrachtet werden können.

4. Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist die Ansprechperson bei ihrem Kanton?
Ansprechperson und zuständig für die Koordination der Informationssicherheit im Kanton ist der/die kantonale Informationssicherheitsbeauftragte (KIT-SIBE). Dies entspricht auch der Nationalen Cyberstrategie NCS 2023+. Diese Person ist in der Zentralen Informatik (ZI) in der Finanz- und Kirchendirektion (FKD) eingeordnet. Der aktuelle KIT-SIBE ist dem NCSC bereits als Ansprechpartner gemeldet.

Hochachtungsvoll

K. Schweizer

Kathrin Schweizer
Regierungspräsidentin

E. Heer Dietrich

Elisabeth Heer Dietrich
Landschreiberin

Regierungsrat des Kantons Basel-Stadt

Rathaus, Marktplatz 9
CH-4001 Basel

Tel: +41 61 267 85 62
Fax: +41 61 267 85 72
E-Mail: staatskanzlei@bs.ch
www.regierungsrat.bs.ch

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Generalsekretariat VBS
Maulbeerstrasse 9
3003 Bern

Per E-Mail an:
sicherheit.vbs@gs-vbs.admin.ch

Basel, 8. November 2022

Regierungsratsbeschluss vom 8. November 2022
Vernehmlassung zum Ausführungsrecht zum Informationssicherheitsgesetz (ISG)
Stellungnahme des Kantons Basel-Stadt

Sehr geehrte Damen und Herren

Mit Schreiben vom 24. August 2022 hat Frau Bundesrätin Viola Amherd dem Regierungsrat des Kantons Basel-Stadt die Vernehmlassungsentwürfe und den erläuternden Bericht zum Ausführungsrecht zum Bundesgesetz über die Informationssicherheit beim Bund vom 18. Dezember 2020 (Informationssicherheitsgesetz, ISG) zur Vernehmlassung unterbreitet. Wir danken Ihnen für die Gelegenheit zur Stellungnahme und teilen Ihnen mit, dass wir das der Kanton Basel-Stadt das Ausführungsrecht zum ISG begrüsst.

Hinsichtlich der im Schreiben vom 24. August 2022 gestellten Fragen teilt der Kanton Basel-Stadt Folgendes mit:

1. Die Umsetzung der Verordnungen ist sichergestellt. Die Überprüfung der kantonalen Strukturen sowie entsprechende Sensibilisierungsmassnahmen befinden sich aktuell in Planung.
2. Der Kanton Basel-Stadt betreibt ein Verarbeitungssystem, welches die Anforderungen des ISG bereits abdeckt und entsprechend eine gleichwertige Informationssicherheit gewährleistet. Es wird davon ausgegangen, dass das ISG nur beschränkte Auswirkungen haben wird.
3. Unter Berücksichtigung der voraussichtlich beschränkten Auswirkungen des ISG wird nur Mehraufwand im Bereich Compliance (interne Audits, Sicherheitsüberprüfungen von Mitarbeitenden und Klassifizierungen etc.) sowie eine temporäre Bindung von personellen Ressourcen erwartet. Dieser Mehraufwand lässt sich noch nicht beziffern.
4. Für Fragen zur Informationssicherheit können mit Herrn Ferdinand Kuske, Beauftragter für Informationssicherheit (ISB), melden. Er ist elektronisch unter ferdinand.kuske@bs.ch und telefonisch unter +41 61 267 65 86 erreichbar.

Der Regierungsrat bedankt sich für die Berücksichtigung seiner Stellungnahme. Bei Fragen steht Ihnen Herr Felix Multerer (felix.multerer@jsd.bs.ch) vom Zentralen Rechtsdienst im Justiz- und Sicherheitsdepartement Basel-Stadt gerne zur Verfügung.

Mit freundlichen Grüssen
Im Namen des Regierungsrates des Kantons Basel-Stadt

Beat Jans
Regierungspräsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin

Kanton Bern
Canton de Berne

Regierungsrat

Postgasse 68
Postfach
3000 Bern 8
info.regierungsrat@be.ch
www.be.ch/rr

Staatskanzlei, Postfach, 3000 Bern 8

Per E-Mail als PDF- und Word-Dokument an:
sicherheit.vbs@gs-vbs.admin.ch

RRB Nr.:	1206/2022	23. November 2022
Direktion:	Finanzdirektion	
Klassifizierung:	Nicht klassifiziert	

Ausführungsrecht zum Informationssicherheitsgesetz.
Stellungnahme des Kantons Bern

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Der Regierungsrat dankt Ihnen für die Gelegenheit zur Stellungnahme zum titelerwähnten Geschäft.

Das Informationssicherheitsgesetz des Bundes (ISG) und damit auch sein Ausführungsrecht gilt für die Kantone nicht, wenn sie eine mindestens gleichwertige Informationssicherheit gewährleisten (Art. 3 Abs. 2 ISG). Der Kanton Bern beabsichtigt, dies durch ein eigenes Gesetz über die Informations- und Cybersicherheit (ICSG) sicherzustellen, welches sich am ISG orientieren wird. Weil die Risiken und Aufgaben des Kantons andere sind als die des Bundes, wird das ICSG voraussichtlich im Bereich der Personensicherheitsprüfung (PSP) ein einfacheres und weniger aufwändigeres Verfahren vorsehen sowie auf die Regelung des Betriebssicherheitsverfahrens verzichten.

Daher geht der Regierungsrat davon aus, dass das ISG und sein Ausführungsrecht auf Berner Behörden keine Anwendung finden werden, auch nicht in der Übergangsfrist zwischen dem Inkrafttreten des ISG (geplant Mitte 2023) und des ICSG (geplant im 1. Halbjahr 2024). Für diese beschränkte Zeit erfüllt nach der Meinung des Regierungsrates die bestehende Direktionsverordnung vom 3. Januar 2011 über Informationssicherheit und Datenschutz (ISDS DV, BSG 152.040.2) die Anforderungen von Art. 3 Abs. 2 ISG (vgl. die Ausführungen auf S. 12 des erläuternden Berichtes, wonach die Kantone dies in erster Linie in eigenem Ermessen beurteilen).

Der Regierungsrat verzichtet daher auf inhaltliche Bemerkungen zu den vorliegenden Verordnungsentwürfen. Er wird die erlassenen Verordnungen jedoch als Grundlage für das Ausführungsrecht zum ICSG berücksichtigen.

Der Regierungsrat dankt Ihnen für die Kenntnisnahme.

Freundliche Grüsse

Im Namen des Regierungsrates

Christine Häsler
Regierungspräsidentin

Christoph Auer
Staatsschreiber

Verteiler
– Finanzdirektion

ETAT DE FRIBOURG
STAAT FREIBURG

Conseil d' tat CE
Staatsrat SR

Rue des Chanoines 17, 1701 Fribourg

T +41 26 305 10 40, F +41 26 305 10 48
www.fr.ch/ce

Conseil d tat
Rue des Chanoines 17, 1701 Fribourg

PAR COURRIEL

Département fédéral de la protection de la
population et des sports DDPS
Palais fédéral est
3003 Berne

Courriel : sicherheit.vbs@gs-vbs.admin.ch

Fribourg, le 22 novembre 2022

2022-1098
Législation d'exécution de la loi sur la sécurité de l'information

Madame la Conseillère fédérale,

Par courrier du 24 août dernier, vous nous avez consultés sur l'objet cité en titre, et nous vous en remercions.

Nous relevons que la loi sur la sécurité de l'information et ses dispositions d'exécution ne s'appliquent aux cantons que lorsqu'ils traitent des informations classifiées de la Confédération ou accèdent à des moyens informatiques de la Confédération, et que les cantons peuvent par ailleurs y déroger s'ils garantissent une sécurité de l'information équivalente. Compte tenu d'une part de ce cadre très circonscrit, d'autre part du développement en cours d'un cadre légal cantonal en matière de sécurité de l'information, nous estimons que l'impact de législation mise en consultation pour le canton sera limité. Nous n'avons dès lors pas de remarques particulières à émettre et souscrivons donc sans réserve aux différents projets d'ordonnance.

S'agissant de vos questions spécifiques, nous vous confirmons comprendre la mise en œuvre de ces ordonnances. Le futur cadre légal cantonal en la matière permettra d'intégrer la mise en œuvre des ordonnances fédérales. Les conséquences financières strictement liées au cadre légal fédéral sont à ce stade difficile à estimer, mais paraissent de prime abord minimes, en raison du champ limité des informations concernées.

En outre, nous vous informons que la Direction de la sécurité, de la justice et du sport, par son secrétariat général, est appelée à prendre la responsabilité de la sécurité de l'information au sein de l'Etat de Fribourg et fonctionnera donc à ce titre comme entité interlocutrice pour ces questions.

Enfin, le Conseil d'Etat a pris bonne note que le Service de l'informatique et des télécommunications avait été consulté directement et que sa prise de position, qui est à prendre en compte, est envoyée séparément.

Nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de nos sentiments les meilleurs.

Au nom du Conseil d'Etat :

Olivier Curty, Président

Danielle Gagnaux-Morel, Chancelière d'Etat

L'original de ce document est établi en version électronique

Copie

—

à la Direction de la sécurité, de la justice et du sport ;
la Direction des finances, pour elle et le Service de l informati ue et des télécommunications ;
à la Chancellerie d'Etat.

ETAT DE FRIBOURG
STAAT FREIBURG

Service de l'informatique et des télécommunications
Case postale, 1701 Fribourg

Service de l'informatique
et des télécommunications SITel
Amt für Informatik und Telekommunikation ITA

Route André Piller 50 - Givisiez
Case postale, 1701 Fribourg

T +41 26 305 31 61
www.fr.ch/sitel

—
Réf : -
T direct : 026 305 31 61
Courriel : michel.demierre@fr.ch

Madame
Viola Amherd
Conseillère fédérale
Chef du Département fédéral de la défense, de la protection de la population et des sports
DDPS

PAR EMAIL

Givisiez, le 25 novembre 2022

Procédure de consultation : Législation d'exécution de la loi sur la sécurité de l'information

Madame la Conseillère fédérale,

Nous vous remercions de nous avoir consulté au sujet de la législation d'exécution de la loi sur la sécurité de l'information (LSI).

Vous nous avez demandé de répondre à quatre questions en lien avec la consultation.

A titre liminaire, et avant de fournir les réponses à ces questions, nous souhaitons nous déterminer sur le paysage hétéroclite de la gouvernance des systèmes d'information de la Confédération. A ce titre, nous regrettons qu'une instance unique ne puisse coordonner les questions en lien avec les systèmes d'information entre la Confédération et les cantons. Dès lors que l'administration numérique suisse (ANS) a pour ambition de devenir un organe fédérateur des systèmes d'information de la Confédération, des cantons et des villes, il nous aurait semblé pertinent de l'impliquer dans la thématique de la loi sur la sécurité de l'information.

Ensuite, les réponses aux questions sont comme suit :

1. *La mise en œuvre des ordonnances est-elle compréhensible pour les cantons ?*

Pour répondre à cette question, il s'agit avant tout pour le canton de comprendre si la LSI et sa législation d'exécution s'appliquent au canton dès lors que la législation cantonale ne permet pas de garantir une sécurité au moins équivalente de l'information (art. 3 al. 2 LSI).

A ce titre, il est en l'état impossible de se prononcer pleinement sur la question pour la simple et bonne raison que la législation d'exécution renvoi dans la plupart des cas à de futures directives et recommandations qui ne sont actuellement pas disponibles.

Le canton ne pourra pleinement répondre à cette question qu'en réalisant un travail de fonds sur ses propres systèmes afin de comparer l'état actuel de ses processus organisationnelles et techniques avec ces directives générales et abstraites. Ce travail de fonds ne pourra être effectuer qu'une fois que ces directives seront disponibles.

Nous suggérons, lors de la rédaction des directives générales et abstraites encore manquantes, que soit unifiées les contraintes techniques hétéroclites qui sont actuellement en cours au sein de la Confédération. A l'heure actuelle, et pour prendre un exemple flagrant, il y a en parallèle 3 PKI de la Confédération (armée, SJPD, etc.). Il est problématique pour le canton de comprendre le type d'exigences que la Confédération souhaite imposer si des exigences équivoques sont invoquées. Si l'ANS pouvait servir à quelque chose, ce serait avant tout à servir d'organe fédérateur en matière de systèmes d'information, et donc également en matière de sécurité de l'information. Nous souhaitons dès lors une plus grande implication de l'ANS dans les matières qui touchent les cantons et leurs systèmes d'information. Sans organe fédérateur, le paysage informationnel de l'Etat deviendra ingérable, d'autant plus pour les cantons, qui ne disposent pas de budgets similaires à celui de la Confédération.

2. *Comment les cantons envisagent-ils la mise en œuvre des ordonnances ?*

Avant toute chose, il s'agira de comprendre dans les faits, dans quelle mesure le canton sera impacté par la LSI et ses mesures d'exécution. En l'état actuel, le Canton ne dispose pas d'une liste précise des informations classifiées de la Confédération que le canton traite par ses unités administratives. Une telle liste devrait être préparée et centralisée par la Confédération. Sans une telle liste, il sera très difficile au canton de disposer de la vue d'ensemble pour garantir une bonne mise en œuvre de ses responsabilités en la matière.

En revanche, contrairement au traitement des informations classifiées, le Service de l'informatique et des télécommunications du canton de Fribourg (SITel) a mis en place des mesures afin d'inventorier les moyens informatiques de la Confédération auxquels les unités administratives du canton accèdent.

Des mesures liées à la sécurité des moyens informatiques sont constamment à l'étude au canton, sous l'égide du SITel. A défaut des directives générales et abstraites manquantes, nous ne pouvons connaitre le réel impact de la LSI pour le canton et ne pouvons dès lors envisager une mise en œuvre des ordonnances. Le canton n'a toutefois pas attendu la Confédération pour mettre en place des mesures de sécurité des moyens informatiques. Ces mesures devront être analysées sous l'angle des exigences de la Confédération. Nous attendons donc avec impatience les directives d'exécution.

Toutefois, comme il n'y a pas d'exigence pour les cantons de mettre en place un SMSI, le canton comprend qu'il n'y aura à priori pas de besoin de passer une certification ISO 27001, ce qui semble alléger un tant soit peu les éventuelles mesures supplémentaires qui avaient été craintes avec l'introduction de la LSI.

3. *A quelles conséquences financières s'attendent les cantons ?*

Pour répondre à cette question, il s'agira de comprendre plus précisément le rôle des cantons en lien avec les exigences organisationnelles et techniques mises en œuvre par la LSI et sa législation d'exécution.

A titre d'exemple, comment doivent être comprises les exigences de la Confédération envers les cantons en lien avec les moyens informatiques du canton ? Est-ce que les moyens informatiques du canton doivent répondre à des exigences similaires que pour les moyens informatiques de la Confédération? La question se pose en cas de communication entre les moyens informatiques cantonaux et les moyens informatiques de la Confédération. Notamment, qu'en serait-il des divers interfaces / API de connexion entre les deux moyens informatiques ?

De plus, est-ce que des informations classées de la Confédération qui seraient traitées par les cantons par les moyens informatiques cantonaux impliqueraient des mesures particulières pour les moyens informatiques cantonaux, notamment des obligations d'accréditation (art. 23 OSI), les règles sur les préjudices (art. 28 OSI), des mesures de sécurité (art. 29 OSI) et de sécurité de l'exploitation (art. 30 OSI) ?

Particulièrement, est-ce que la sécurité des entreprises introduite par l'OPSE s'applique aux moyens informatiques du canton ?

Nous ne pensons pas que la LSI et sa législation d'exécution aillent dans ce sens mais à défaut de mention expresse dans la législation ou dans le rapport explicatif, cette question demeure. Une clarification est dès lors souhaitée afin de dissiper les doutes.

Finalement, un renforcement des compétences cantonales sera nécessaire pour monter en compétence en matière de sécurité de l'information. Dans tous les cas, un audit sera nécessaire pour comparer les exigences de la LSI avec les mesures organisationnelles et techniques déjà en place au niveau cantonal. Cet audit ne pourra être pensé qu'une fois que les directives générale et abstraites de la Confédération seront disponibles. A ce stade, même si une augmentation des charges et coûts issus de la LSI sont à prévoir, il est difficile de chiffrer cette augmentation.

En revanche, si une uniformisation des contraintes de la Confédération envers les cantons était mise en place, au moyen par exemple de l'ANS, ces charges et coûts seraient d'autant plus réduits. Nous invitons donc la Confédération à considérer le besoin des cantons dans l'uniformisation de la communication et des contraintes qu'ils leurs sont imposées par la Confédération.

4. *Les cantons devront désigner un service faisant office d'interlocuteur pour les questions de sécurité de l'information. Quel est cet interlocuteur dans votre canton ?*

Le canton a constitué en été 2021 un groupe de travail portant sur les questions en lien avec la sécurité de l'information cantonale. Ce groupe de travail faisait suite à une réorganisation interne de l'administration cantonale en matière de sécurité informatique et de sécurité de l'information. Notamment, des règles univoques devaient être mises en place afin de préciser les responsabilités en matière de sécurité informatique d'une part, et en matière de sécurité de l'information d'autre part.

Le groupe de travail a conclu à la mise en place d'une législation cantonale prenant la forme d'un règlement : « règlement cantonal sur la sécurité de l'information (RSI) ». Le RSI est actuellement en voie de finalisation auprès de la direction cantonale concernée et fera l'objet d'une consultation générale auprès de l'administration cantonale.

En l'état actuel du RSI, l'avant-projet a décidé de créer un organe administratif particulier qui sera responsable de la sécurité de l'information au niveau cantonal. Cet organe administratif particulier sera administrativement rattaché à une Direction cantonale, et devra répondre pour le surplus à la Conférence cantonale des secrétaires généraux. Cet organe administratif aura notamment pour tâche de rédiger une politique en matière de sécurité de l'information.

Veuillez croire, Madame la Conseillère fédérale, en l'expression de nos considérations distinguées.

Michel Demierre
Directeur

RÉPUBLIQUE ET CANTON DE GENÈVE

POST TENEBRAS LUX

Genève, le 23 novembre 2022

Le Conseil d'Etat

5081-2022

Département fédéral de la défense, de la protection de la population et des sports
Madame Viola Amherd
Conseillère fédérale
Palais fédéral Est
Bundesgasse 3
3003 Berne

Concerne : consultation sur la législation d'exécution de la loi sur la sécurité de l'information

Madame la Conseillère fédérale,

Votre courrier du 24 août 2022 relatif à l'objet cité en titre nous est bien parvenu et a retenu toute notre attention.

A cet égard, nous vous prions de trouver, ci-après, les réponses aux quatre questions de cette consultation.

1. La mise en œuvre des ordonnances est-elle compréhensible pour les cantons ?

Si nous saluons la qualité globale du travail effectué, nous relevons que la mise en œuvre par les cantons nécessitera un travail conséquent qu'il est difficile de chiffrer précisément à ce stade. De plus, les détails liés à l'étendue de l'applicabilité de ces ordonnances aux cantons sont complexes à évaluer.

2. Comment les cantons envisagent-ils la mise en œuvre de ces ordonnances ?

Il s'agira pour le canton d'élaborer cas échéant des bases légales et réglementaires complémentaires. La mise en œuvre des ordonnances fédérales nécessitera des moyens financiers supplémentaires.

Par exemple, le canton ne dispose pas de réglementation formelle concernant le contrôle de sécurité des personnes, ni pour l'instant d'une liste des fonctions à risque ou nécessitant un contrôle de sécurité. A la lecture des textes, notamment l'article 35 de l'Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP), il reviendra au canton de disposer d'une base légale suffisante pour les contrôles à effectuer et établir une convention avec le Département fédéral de la défense, de la protection de la population et des sports (DDPS) pour obtenir une prestation de sa part.

3. A quelles conséquences financières s'attendent les cantons ?

Le canton s'attend à des conséquences financières importantes, notamment en termes de ressources humaines et de systèmes informatiques supplémentaires. Nous ne sommes toutefois pas à même de chiffrer ces conséquences financières à ce stade, qu'il s'agisse du domaine des systèmes d'information ou du domaine de la Police.

Nous relevons en particulier les frais des demandes de contrôles moyennant une convention avec le DDPS (entre CHF 100.- et 400.- par demande). Les cumuls de ceux-ci pourront être conséquents pour certaines entités, comme la Police ou l'Office cantonal des systèmes d'information et du numérique (OCSIN).

Dans le domaine de la Police, il y aura des mesures architectoniques nécessaires pour ses locaux, afin de respecter les normes générales et abstraites définies pour les zones de sécurité 2 notamment. A l'heure actuelle, nous n'avons pas connaissance de ces normes et ne pouvons donc pas pour l'instant estimer les éventuels coûts engendrés. Toutefois, la Police traite déjà des données classifiées et ses locaux n'ont pas fait l'objet de recommandations spécifiques concernant la sécurité de la part du Service de renseignement de la Confédérations (SRC). Par ailleurs, la Police genevoise a récemment été équipée des nouveaux matériels de communication sans restriction du SRC.

4. Les cantons devront désigner un service faisant office d'interlocuteur pour les questions de sécurité de l'information. Quel est cet interlocuteur dans votre canton ?

Il s'agit du service de la sécurité de l'information et de la protection des données, au sein de l'OCSIN. Ce service est dirigé par M. Christian Geffcken.

En complément, nous vous adressons dans une annexe des remarques sur des articles précis des quatre ordonnances.

Nous vous remercions de nous avoir consultés et vous prions de croire, Madame la Conseillère fédérale, à l'assurance de notre haute considération.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :

Michèle Righetti

Le président :

Mauro Poggia

Annexe mentionnée

Copie à : sicherheit.vbs@gs-vbs.admin.ch

Annexe : Commentaires concernant les quatre ordonnances d'exécution de la nouvelle loi sur la sécurité de l'information

Remarques concernant l'ordonnance sur la sécurité de l'information au sein de l'administration fédérale et de l'armée (OSI)

Remarque générale
De manière générale, cette ordonnance décrit très précisément le cadre de la sécurité de l'information. Pour les cantons, une telle mise en conformité représentera une tâche complexe et coûteuse.

Art. 19 et 20 Echelons de classification
Ces deux articles traitant de l'échelon de classification "confidentiel" et "secret", évoquent deux mêmes aspects, à savoir la protection de l'identité des sources (art. 19 let. c et art. 20 let. c). La principale préoccupation des services de Police est, et reste, la protection de l'identité de la source. Sans cette préoccupation constante, il serait difficile, voire impossible de recruter sur le long terme des sources si leur protection n'était pas garantie et mise en œuvre.
Le fait de classifier les identités des sources de deux manières différentes n'apporte aucune plus-value. Au contraire, elle induit des risques dans le cycle de vie de la source. En effet, cette dernière pourrait passer de l'échelon "confidentiel" à "secret" en fonction de sa capacité développée, des informations récoltées ou du milieu où elle évolue. De plus, cette classification est définie, notamment, en fonction d'un préjudice de causalité potentiellement considérable ou grave des intérêts publics de la Suisse. L'aspect des préjudices envers la source elle-même, en cas d'accès à son identité, n'est pas pris en compte ce qui est problématique et peut également porter préjudice à l'Etat. Dès lors, la protection de l'identité de la source devrait être constante et placée à l'échelon "secret" uniquement.

Art. 35 Zone de sécurité
Des données classifiées "secret" sont actuellement traitées dans les locaux de la Police. Selon les directives générales et abstraites émises par le service spécialisé de la Confédération pour la sécurité de l'information, cela pourrait donner lieu à des modifications architectoniques contraignantes impactant lesdits locaux. Ces modifications seront imposées et nécessaires pour la poursuite de l'exécution des tâches relevant de l'échelon "secret".

Remarques concernant l'ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM)

Art. 5 Systèmes IAM
L'alinéa 2 fait référence à la "licéité". Il s'agit plutôt de "légalité", voire de conformité à la loi. La licéité concerne le caractère éthiquement acceptable d'une loi. Une loi inique est "légale", mais elle n'est pas "licite".

Art. 13 Base centralisée des identités pour la distribution des données
L'alinéa 4 fait référence à "à la condition que le système concerné". S'agit-il du système source ou d'un "autre système d'information interne à l'administration fédérale" ?

Art. 18 Exigences concernant la sécurité de l'information
L'alinéa 2 fait référence aux "exigences minimales prédéfinies". Il s'agit de préciser par qui, dans quel cadre.

Art. 21 Conditions pour le raccordement de systèmes IAM externes
A sa let. c, cet article fait référence aux "systèmes IAM comprenant des collaborateurs cantonaux et communaux au sens de l'art. 9, let. a". L'art 9 let. a de l'OIAM actuelle restreint la liste "si ces personnes utilisent des systèmes d'information mis à disposition par la Confédération".
Or, le système IAM de l'Etat de Genève contient bien des personnes qui n'utilisent pas ces systèmes d'information mis à disposition de la Confédération. Cela implique-t-il qu'il faille faire un sous-ensemble restreint aux personnes y accédant, et que seul ce sous-ensemble peut être connecté ?

Annexe Catégorie de données
Concernant les données techniques (let. e, 7) "mots de passe", il s'agit de préciser que cette donnée ne saurait être stockée en clair, mais bien chiffré ou haché, selon les besoins.

Remarques concernant l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP)

Les degrés des contrôles de sécurité sont modifiés dans la présente ordonnance. A teneur des nouvelles dispositions, tous les collaborateurs des autorités d'exécution cantonales de la loi sur le renseignement (LRens) seront soumis à un contrôle de sécurité élargi. Cela se traduit par une audition supplémentaire pour chaque collaborateur à mener par le service de sécurité. Cette procédure est réalisée tous les 3 ans au plus tôt et au plus tard tous les 5 ans.
Durant la procédure de contrôle de sécurité des collaborateurs, il est aussi possible que les supérieurs hiérarchiques, anciens et actuels, fassent également l'objet d'une audition.
Cette nouvelle procédure aura un impact sur la durée entre le choix et l'affectation finale des collaborateurs au sein du Service de renseignement cantonal (SRCant) à teneur des résultats des contrôles de sécurité élargis du Département fédéral de la défense, de la protection de la population et des sports (DDPS). A noter cependant que dans le contrôle des indemnisations des postes aux cantons par le DDPS, une tolérance de 6 mois est acceptée pour un poste vacant à renouveler.
Nous ne disposons pas de base légale pour le contrôle de sécurité des personnes au niveau cantonal. Il conviendra donc de solliciter le DDPS pour les contrôles de personnes à des fonctions jugées sensibles et annoncées (art. 35). En outre, il s'agira d'évaluer si le canton dispose d'une base légale suffisante pour les contrôles effectués sur la base de cette ordonnance.

Annexe 7 Collecte et traitement des données
Nous relevons que cette ordonnance donne une base réglementaire permettant de collecter beaucoup de données, menant à une interrogation sur la proportionnalité de cette collecte, par exemple concernant les données portant sur des tiers (famille proche, cercle d'amis étroit, etc.).

Remarques concernant l'ordonnance sur la procédure de sécurité relative aux entreprises (OPSE)

Art. 17 Information de la part de l'entreprise
Concernant le changement des rapports de propriété ou des structures de l'entreprise (alinéa 1), il pourrait être utile de préciser que cela s'applique également à ses filiales.
Concernant la solvabilité et les éventuelles procédures de saisie ou de faillite, il pourrait être utile de préciser "en Suisse ou ailleurs".
Concernant les incidents dans le domaine de la sécurité (alinéa 2), il serait pertinent d'ajouter les violations de protection des données au sens de la nLPD.

kanton glarus

Telefon 055 646 68 00
E-Mail: sicherheitjustiz@gl.ch
www.gl.ch

Sicherheit und Justiz
Postgasse 29
8750 Glarus

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
3003 Bern

Glarus, 24. November 2022
Unsere Ref: 2022-198

Vernehmlassung i. S. Ausführungsrecht zum Informationssicherheitsgesetz

Hochgeachtete Frau Bundesrätin
Sehr geehrte Damen und Herren

Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport gab uns in eingangs genannter Angelegenheit die Möglichkeit zur Stellungnahme. Dafür danken wir und können mitteilen, dass die Anwendung des Informationssicherheitsgesetzes und des dazugehörigen Ausführungsrechts auf unseren Kanton beschränkt ist. Die Umsetzung erfolgt im Rahmen von Projekten oder beim Bezug von Dienstleistungen des Bundes. Der Zusatzaufwand dürfte eher gering ausfallen. Als Ansprechpartner des Bundes für Fragen der Informationssicherheit wird der IT-Sicherheitsverantwortliche der Informatikabteilung bezeichnet.

Genehmigen Sie, hochgeachtete Frau Bundesrätin, sehr geehrte Damen und Herren, den Ausdruck unserer vorzüglichen Hochachtung.

Freundliche Grüsse

Dr. Andrea Bettiga
Regierungsrat

E-Mail an (PDF- und Word-Version):
- sicherheit.vbs@gs-vbs.admin.ch

zur Kenntnis an (per CMI):
- Departement Finanzen und Gesundheit, Informatikdienst
- Kantonale Fachstelle für Datenschutz

Die Regierung
des Kantons Graubünden

La Regenza
dal chantun Grischun

Il Governo
del Cantone dei Grigioni

Sitzung vom	Mitgeteilt den	Protokoll Nr.
15. November 2022	16. November 2022	869/2022

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
sicherheit.vbs@gs-vbs.admin.ch

Vernehmlassung VBS - Ausführungsrecht zum Informationssicherheitsgesetz
Stellungnahme

Sehr geehrte Frau Amherd
Sehr geehrte Damen und Herren

Mit Email vom 25. August 2022 erhalten die Kantone die Gelegenheit, sich zu obenerwähnter Angelegenheit zu äussern.

Die Vorgaben des ISG werden in der Vorlage konsequent umgesetzt und die im revidierten Bundesgesetz über den Datenschutz (DSG; SR 235.1) aufgenommenen Neuerungen haben ebenfalls Eingang ins Ausführungsrecht gefunden. Insgesamt werden die Erwartungen an eine Verordnung erfüllt und die gesetzlichen Vorgaben zufriedenstellend umgesetzt, weshalb der Kanton Graubünden die Vorlage begrüsst.

Wir danken Ihnen für die Möglichkeit zur Stellungnahme.

GRISCHUN * GRIGIONE * GRAUBÜNDEN

Namens der Regierung

Der Präsident:
Marcus Caduff

Der Kanzleidirektor:
Daniel Spadin

JURA CH RÉPUBLIQUE ET CANTON DU JURA GOUVERNEMENT

Hôtel du Gouvernement
2, rue de l'Hôpital
CH-2800 Delémont

t +41 32 420 51 11
f +41 32 420 72 01
chancellerie@jura.ch

Hôtel du Gouvernement – 2, rue de l'Hôpital, 2800 Delémont

Département fédéral de la défense,
de la protection de la population et des sports
Madame la Conseillère fédérale Viola Amherd
Palais fédéral Est
3003 Berne

Par email : sicherheit.vbs@gs-vbs.admin.ch

Delémont, le 15 novembre 2022

Législation d'exécution de la loi sur la sécurité de l'information : ouverture de la procédure de consultation

Madame la Conseillère fédérale,

Le Gouvernement de la République et Canton du Jura accuse réception de votre lettre du 24 août 2022, par laquelle vous l'invitez à se prononcer dans le cadre de la procédure de consultation sur la législation d'exécution de la loi sur la sécurité de l'information.

Il est en mesure de répondre comme suit aux questions posées :

1. La mise en œuvre des ordonnances est-elle compréhensible pour les cantons ?

   Non, cette mise en œuvre n'est pas totalement compréhensible pour le Canton du Jura. Il est indiqué que les cantons traitent des informations classifiées et que les dispositions de la LSI et de l'OSI relatives aux informations classifiées sont applicables. Il n'est pas clair de quelles données il est question.

   S'il s'agit uniquement des données traitées dans les applications de la Confédération, ces dernières sont accessibles de façon sécurisée via l'infrastructure de la Confédération (PKI) et l'impact serait alors limité.

   Si d'autres données entrent en considération, les mesures à mettre en place ne sont pas évidentes sans une analyse détaillée.

   De plus, comme la mise en œuvre de la LSI requiert l'élaboration de trois ordonnances et la modification d'une ordonnance, la matière est très large et touche de nombreux domaines spécifiques, de telle sorte que la coordination entre les différentes entités concernées s'avère difficile à ce stade.

Il serait appréciable que pour chaque ordonnance ou chaque domaine spécifique, des précisions sur ce qui attendu précisément des cantons et/ou sur la marche à suivre soient apportées (p. ex. au moyen d'un tableau ou d'un document spécifique), car ces informations ne ressortent pas de manière suffisamment claire des documents mis en consultation.

2. Comment les cantons envisagent-ils la mise en œuvre des ordonnances ?

   Il est proposé de mettre en place ces prochains mois un groupe de travail interservices, à l'interne du canton du Jura, pour évaluer les impacts de façon globale (de ces ordonnances mais également des autres lois liées à la gestion des données) et définir les mesures (organisationnelles et techniques) à implémenter au sein du Canton du Jura. Un tel travail n'a malheureusement pas pu être réalisé durant la période de consultation, en raison d'une importante charge de travail des services concernés ces derniers mois.

3. À quelles conséquences financières s'attendent les cantons ?

   L'engagement d'un gestionnaire des données sera probablement nécessaire pour cartographier l'ensemble des données utilisées au sein de l'administration cantonale et gérer l'ensemble des processus liés à l'exploitation de ces données. La mise en œuvre de la loi et de ses ordonnances demandera dans la plupart des services de l'Etat, en tant que responsables de données, un surcroît d'activités à l'interne. Il est également certain que des adaptations des infrastructures de sécurité seront nécessaires mais ces dernières ne sont pas chiffrables sans une étude détaillée.

4. Les cantons devront désigner un service faisant office d'interlocuteur pour les questions de sécurité de l'information. Quel est cet interlocuteur dans votre canton?

   Il n'est pas possible à l'heure actuelle de désigner le service qui fera office d'interlocuteur. Le groupe de travail mentionné sous la réponse à la question n°2 sera chargé de définir ce service et de faire une proposition dans ce sens au Gouvernement qui adoptera ensuite en principe une ordonnance désignant le service cantonal compétent pour les questions de sécurité de l'information.

Tout en vous remerciant de prendre note de sa réponse, le Gouvernement de la République et Canton du Jura vous prie de croire, Madame la Conseillère fédérale, à sa haute considération.

AU NOM DU GOUVERNEMENT DE LA RÉPUBLIQUE ET CANTON DU JURA

David Eray
Président

GOUVERNEMENT DE LA RÉPUBLIQUE ET CANTON DU JURA

Jean-Baptiste Maître
Chancelier d'État

canton de vaud
LIBERTÉ ET PATRIE

CONSEIL D'ÉTAT

Château cantonal
1014 Lausanne

Madame la Conseillère fédérale
Viola Amherd
Cheffe du Département fédéral de la défense, de la protection de la population et des sports
Palais fédéral est
3003 Berne

Par courriel (en Word et PDF) :
sicherheit.vbs@gs-vbs.admin.ch

Réf. : 22_COU_6293

Lausanne, le 23 novembre 2022

Législation d'exécution de la loi sur la sécurité de l'information : procédure de consultation

Madame la Conseillère fédérale,

Le Conseil d'Etat du Canton de Vaud vous remercie d'avoir sollicité son avis dans le cadre de la procédure de consultation relative à la législation d'exécution de la loi sur la sécurité de l'information.

La sécurité de l'information est un élément fondamental, en particulier dans le cadre de la transformation numérique des organisations et de la société en général. Le Conseil d'Etat a rappelé dans sa Stratégie numérique, adoptée en 2018, l'importance du principe de sécurité dans ce contexte. Il a pris connaissance des quatre projets d'ordonnances d'application qui visent à la mise en œuvre de la loi sur la sécurité de l'information. En juillet 2014, il s'était prononcé favorablement sur ce projet de loi tout en rappelant la nécessité de prévoir des dispositions d'application en collaboration avec les cantons, étant donné les conséquences financières et humaines non négligeables qui pourraient survenir. Il regrette que les projets mis en consultation ne permettent toujours pas aux cantons d'évaluer avec précision ces conséquences.

Le Conseil d'Etat vous prie de trouver ci-après les réponses aux questions posées dans le cadre de cette consultation :

1. La mise en œuvre des ordonnances est-elle compréhensible pour les cantons ?

Le Conseil d'Etat constate l'important travail réalisé par les services de la Confédération et relève la clarté du texte des ordonnances. Toutefois, leur mise en œuvre dans les cantons nécessitera très probablement de faire évoluer la législation cantonale, des ressources humaines et financières additionnelles, et une adaptation des systèmes d'information. Le Conseil d'Etat n'est pas en mesure aujourd'hui d'évaluer ces éléments, les projets mis en consultation n'étant pas suffisamment précis à cet égard.

2. Comment les cantons envisagent-ils la mise en œuvre des ordonnances ?

Le Conseil d'Etat prévoit que la mise en œuvre des ordonnances se déroule de manière coordonnée entre les différents services de son administration, afin de créer des synergies mais également dans un souci d'efficacité, de maîtrise des coûts et d'uniformisation. La mise en œuvre devra s'appuyer sur le système de management de la sécurité de l'information (SMSI) déjà formellement en place au sein de l'administration cantonale, par la Direction générale du numérique et des systèmes d'information (DGNSI). Ce système est en préparation pour une certification à la norme ISO 27001, prévue en décembre 2022.

Le Conseil d'Etat relève également que l'adoption des ordonnances par le Conseil fédéral nécessitera vraisemblablement l'élaboration de bases légales et réglementaires cantonales complémentaires, par exemple pour procéder à des contrôles conformément à l'art. 35 de l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP).

Au vu de la complexité de la mise en œuvre sur les plans technique et juridique, le Conseil d'Etat demande que l'entrée en vigueur des ordonnances se fasse de manière échelonnée, avec une période transitoire suffisante.

3. À quelles conséquences financières s'attendent les cantons ?

Le Conseil d'Etat n'est pas en mesure à ce stade d'estimer les conséquences financières pour le Canton de Vaud : les informations nécessaires à cet égard, de même que celles portant sur les conséquences organisationnelles, ne sont en effet pas suffisamment détaillées dans le projet mis en consultation. Toutefois, le Conseil d'Etat constate que cette législation aura principalement un impact sur les systèmes d'informations qui communiquent avec les systèmes fédéraux. Le Conseil d'Etat demande que le Conseil fédéral apporte rapidement les précisions sur les systèmes et les données concernées, qui lui permettront de procéder à l'évaluation de ces conséquences.

Le Conseil d'Etat a par ailleurs pris note que des prescriptions techniques d'exécution restent à venir. Ceci induit des incertitudes sur les conséquences pour les cantons. Des questions subsistent encore également quant aux modalités d'application et aux dispositions transitoires de cette législation d'exécution, dans les cas où elle s'appliquera aux autorités cantonales.

Dans ce contexte, le Conseil d'Etat demande que les services de la Confédération communiquent les prescriptions techniques ainsi que toutes les précisions utiles dans les meilleurs délais et que le Conseil fédéral définisse qui aura la charge de vérifier le respect de la mise en œuvre.

4. *Les cantons devront désigner un service faisant office d'interlocuteur pour les questions de sécurité de l'information. Quel est cet interlocuteur dans votre canton ?*

Le Conseil d'Etat a désigné la Direction générale du numérique et des systèmes d'information (DGNSI), et en particulier son directeur de la sécurité numérique pour être l'interlocuteur pour les questions de sécurité de l'information dans le cadre de la mise en œuvre des ordonnances.

Pour le surplus, le Conseil d'Etat vous adresse en annexe de ce courrier différentes remarques et observations sur les quatre ordonnances.

En conclusion, le Conseil d'Etat peut soutenir les projets mis en consultation mais demande que le Conseil fédéral apporte dans les meilleurs délais toutes les précisions nécessaires pour diminuer les risques liés à leur mise en œuvre.

En vous souhaitant bonne réception de la présente, nous vous prions de croire, Madame la Conseillère fédérale, à l'assurance de notre considération distinguée.

AU NOM DU CONSEIL D'ETAT

LA PRESIDENTE	LE CHANCELIER
Christelle Luisier Brodard	Aurélien Buffat

Annexe

- Remarques sur les ordonnances

Copies

- Direction générale du numérique et des systèmes d'information
- Office des affaires extérieures

Annexe : remarques sur les ordonnances

Ordonnance sur la sécurité de l'information au sein de l'administration fédérale et de l'armée (OSI)

Article 18 al. 1 let. c : L'OSI prévoit que les informations susceptibles de nuire aux intérêts définis à l'art. 1, al. 2, let. a à d LSI, si elles sont portées à la connaissance d'une personne non autorisée, sont classifiées « interne » notamment si « c. des personnes subissent des lésions corporelles ». Or, la limitation à des lésions corporelles, sans spécifier s'il s'agit de lésions corporelles simples, graves ou de voies de fait, ne prend pas en compte le fait qu'une atteinte psychologique peut également entraîner de très lourdes conséquences (dépression, suicide, automutilation, perte de confiance, inefficacité au travail, etc). Ainsi, les conséquences d'une atteinte psychologique pouvant être parfois plus lourdes que celles d'une atteinte physique, la disposition légale devrait prévoir ce cas.

Articles 18 à 20 : Il n'est pas clair comment serait classifiée une fuite de données qui exposerait des données personnelles de citoyens et citoyennes à des tentatives ou des cas d'arnaques, d'escroqueries, de chantages, d'atteintes à la sécurité informatique d'entreprises ou d'individus, etc. A la lecture de ces articles, il apparait que ce sont les intérêts de la Confédération qui sont essentiellement pris en compte et non pas ceux des entreprises et des particuliers, à la protection de leur personnalité et de leurs biens juridiquement protégés en raison d'atteintes à la sécurité informatique des systèmes de la Confédération. Il conviendrait donc d'adapter ces dispositions.

Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP)

Remarque générale : Cette ordonnance aura un impact sur les entités en charge des contrôles de sécurité relatifs aux personnes dans le cadre cantonal. Il s'agit là de rappeler que la récolte importante de données prévue et les traitements de données personnelles éventuellement sensibles nécessitent un encadrement rigoureux qui soit conforme à la législation sur la protection des données.

Ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM)

Remarque générale : La révision de cette ordonnance concerne principalement des aspects d'ordre technique pour les systèmes de gestion des données d'identification. Ces derniers pourraient avoir un impact sur la gestion des identités du portail IAM du canton (Identity and Access Management), ou autres bases de données, en particulier en ce qui concerne l'obligation de gestion des accréditations et des accès aux systèmes d'information de la Confédération. Il s'agit là de prendre également en compte l'impact sur les systèmes d'information sous mandat d'exploitants « tiers », qui utilisent aussi ces systèmes d'identification.

Ordonnance sur la procédure de sécurité relative aux entreprises (OPSE)

Articles 2 et al. : Il conviendrait de préciser les relations entre l'art. 2 al. 1, fixant le champ d'application de l'ordonnance, qui énonce « La présente ordonnance s'applique aux entreprises dont le siège est en Suisse », l'art. 2 al. 2 qui stipule « La procédure s'appliquant aux entreprises dont le siège est à l'étranger est régie par un traité international conformément à l'art. 87 LSI », et l'art. 6 précisant une partie de la procédure en cas de présence d'une entreprise étrangère.

Article 14 : Cet article prévoit un plan de sécurité et un examen lors de la procédure d'adjudication, mais il n'est pas prévu que ce plan soit vérifié en cours de mandat alors que la technologie et les risques évoluent rapidement. Il conviendrait d'adapter la disposition pour prendre en compte les évolutions techniques.

KANTON LUZERN

Finanzdepartement
Bahnhofstrasse 19
6002 Luzern
Telefon 041 228 55 47
info.fd@lu.ch
www.lu.ch

Öffnungszeiten:
Montag - Freitag
08:00 - 11:45 und 13:30 - 17:00

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
per E-Mail an (Word- und PDF-Datei):
sicherheit.vbs@gs-vbs.admin.ch

Luzern, 15. November 2022

Protokoll-Nr.: 1338

Vernehmlassung Ausführungsrecht zum Informationssicherheitsgesetz

Sehr geehrte Damen und Herren

Mit Schreiben vom 24. August 2022 haben Sie die Kantonsregierungen in eingangs erwähnter Angelegenheit zur Stellungnahme eingeladen.

Im Namen und Auftrag des Regierungsrates teile ich Ihnen mit, dass der Kanton Luzern das Ausführungsrecht zum Informationssicherheitsgesetz begrüsst und als sinnvoll erachtet. Ihre Fragen beantworten wir gerne wie folgt:

1. Ist die Umsetzung der Verordnungen für die Kantone verständlich?

   Die Umsetzung der Verordnungen ist verständlich. Bei der Informationssicherheitsverordnung sehen wir folgenden Änderungs- und Ergänzungsbedarf:

   Art. 8 Abs. 1 lit. d ISV:
   "*Sie weisen die ~~die~~ Akzeptanz der Restrisiken nach.*"

   Art. 9 Abs. 2 ISV:
   "*Die Fachstelle des Bundes für Informationssicherheit und die Departemente können die Bewilligung von Ausnahmen delegieren.*"
   Die Verordnung legt nicht fest, an wen delegiert werden kann. Eine Präzisierung wäre sinnvoll.

   Art. 9 Abs. 4 lit. b ISV:
   "*Die Verwaltungseinheiten, die Departemente und die Fachstelle des Bundes für Informationssicherheit führen je ein Verzeichnis der Ausnahmebewilligungen, die:*"
   Es stellt sich die Frage, ob die Verwaltungseinheiten, die Departemente und die Fachstelle des Bundes in jedem Fall informiert werden, wenn die Bewilligung von Ausnahmen delegiert wurde, damit sie diese Ausnahmebewilligungen auch in ihrem Verzeichnis auf-

führen können. Um den Informationsfluss zu sichern, wäre eine Mitteilungs- und Informationspflicht derjenigen Stelle empfehlenswert, an welche eine Bewilligung von Ausnahmen delegiert wurde.

Art. 12 Abs. 7 lit. a ISV:
"*Sie kann in Fällen nach Absatz 5 nach Rücksprache mit der betroffenen Verwaltungseinheit und dem betroffenen Departement die Federführung für die Bewältigung eines Sicherheitsvorfalls oder die Behandlung einer Sicherheitslücke übernehmen. Dabei hat sie folgende Aufgaben und Kompetenzen: (lit. a): Sie kann die betroffenen Verwaltungseinheiten, Leistungserbringer und Dritten verpflichten, ihr alle nötigen Informationen mitzuteilen.*"
Hier sollte präzisiert werden, welche Informationen mitgeteilt werden müssen. Ansonsten kann dies vor allem aus datenschutzrechtlicher Sicht problematisch sein.

Zu den anderen drei Verordnungen der Vorlage haben wir keine Bemerkungen.

2. Wie gedenken die Kantone, die Verordnungen umzusetzen?

   Der Kanton Luzern hat sich entschieden, ein Information Security Management System (ISMS) aufzubauen. Damit ist er in der Lage, eine gleichwertige Informationssicherheit wie die in der Verordnung beschriebene zu gewährleisten. Entsprechend beurteilen wir die bundesrechtlichen Vorgaben aus der Verordnung über die Informationssicherheit bei der Bundesverwaltung und der Armee für den Kanton Luzern als nicht verpflichtend.

3. Mit welchen finanziellen Auswirkungen rechnen die Kantone?

   Das ISMS ist aktuell in der Planung. Der Kanton Luzern rechnet mit einem jährlichen tiefen einstelligen Millionenbetrag.

4. Die Kantone sollen für die Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?

   Martin Achermann
   Chief Information Security Officer (CISO)
   Kanton Luzern
   Dienststelle Informatik (DIIN)
   Postfach 3439
   6002 Luzern
   martin.achermann@lu.ch

Ich danke Ihnen für die Möglichkeit zur Stellungnahme.

Freundliche Grüsse

Reto Wyss
Regierungsrat

LE CONSEIL D'ÉTAT
DE LA RÉPUBLIQUE ET
CANTON DE NEUCHÂTEL

Département fédéral de la défense, de la
protection de la population et des sports DDPS
Maulbeerstrasse 9
3003 Berne

Législation d'exécution de la loi sur la sécurité de l'information

Madame la conseillère fédérale,

Nous vous prions de bien vouloir trouver ci-dessous les observations de la République et Canton de Neuchâtel concernant la législation d'exécution de la loi sur la sécurité de l'information.

D'un point de vue général, il apparaît que ces prescriptions, prises dans leur globalité, répondent bien aux nouvelles réalités de la société de l'information et aux objectifs sécuritaires de la politique de sécurité de l'information.

S'agissant des questions posées, nous sommes en mesure de vous répondre comme suit :

1. La mise en œuvre des ordonnances est-elle compréhensible pour les cantons ?

Oui, d'un point de vue technique, les prescriptions permettent d'appréhender les mesures générales à mettre en œuvre, basées sur une gestion des risques en fonction des éléments à protéger. Ceci dit, il manque à notre avis les recommandations techniques précises qui permettront aux cantons de s'aligner sur les pratiques exigées par la Confédération. Celles-ci seront nécessaires pour affiner les modalités de mises en œuvre ainsi que les conséquences en personnel et financières. Nous nous permettons donc à cette fin de solliciter la communication de ces recommandations techniques.

Les éléments suivants soulèvent toutefois des interrogations :

- Art. 6 OSI : les cantons doivent-ils également consulter le service spécialisé lorsqu'ils établissent leurs propres bases légales nécessaires à atteindre le niveau de sécurité équivalent ou pour la mise en œuvre les recommandations techniques par exemple ?

- Art. 26, 27, 26 OCSP : quelle est la durée de validité des évaluations résultant d'un contrôle de sécurité de personnes ? En cas de répétition du contrôle en raison de l'apparition de nouveaux risques, la nouvelle évaluation remplace-t-elle ou complète-t-elle la précédente ?

- Art. 35 OCSP : lorsque les cantons recourent aux prestations du service spécialisé pour leur propre sécurité de l'information, les motifs de sécurité invocables sont-ils ceux de l'OSCP ou ceux définis par les bases légales cantonales ?

2. Comment les cantons envisagent-ils la mise en œuvre des ordonnances ?

Dans un premier temps, le canton devra définir un plan de mise en œuvre. À cette fin, il aura besoin de ressources supplémentaires afin, notamment, de procéder à l'identification des actifs informationnels, la classification, la définition des flux et des responsabilités. Il n'est pas exclu que davantage de ressources soient nécessaires pour renforcer le système de contrôle interne qui est également à prévoir. À noter aussi que la nature des recommandations techniques attendues (point 1) pourra encore avoir une incidence sur ce besoin en ressources.

3. À quelles conséquences financières s'attendent les cantons ?

D'après notre première estimation, la mise en place des mesures nécessaires à l'établissement d'un SMSI et au renforcement de la sécurité engendrera un coût très important pour le Canton de Neuchâtel. À ce stade, les ressources supplémentaires en personnel sont estimées à 3 EPT ; ce qui implique en termes financiers des charges de l'ordre de 500'000 francs par an, sans compter d'éventuels suppléments découlant des adaptations techniques et recommandations attendues (point 1) pouvant s'élever à plusieurs millions.

4. Quel service cantonal fera office d'interlocuteur pour les questions de sécurité de l'information ?

À ce stade, l'interlocuteur cantonal pour les questions de sécurité de l'information n'est pas encore désigné. Nous ne manquerons pas de vous communiquer l'information dès que ce sera chose faite.

En vous remerciant de nous avoir associés à cette procédure de consultation et de l'attention que vous porterez à nos observations, nous vous prions de croire, Madame la conseillère fédérale, à l'assurance de notre haute considération.

Neuchâtel, le 23 novembre 2022

Au nom du Conseil d'État :

Le président,
L. KURTH

La chancelière,
S. DESPLAND

RÉPUBLIQUE ET CANTON DE NEUCHÂTEL * CONSEIL D'ÉTAT *

KANTON NIDWALDEN
LANDAMMANN UND REGIERUNGSRAT
Dorfplatz 2, Postfach 1246, 6371 Stans
Telefon 041 618 79 02, www.nw.ch

CH-6371 Stans, Dorfplatz 2, Postfach 1246, STK

PER E-MAIL
Eidg. Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Frau Bundesrätin Viola Amherd
Bundeshaus Ost
3003 Bern

Telefon 041 618 79 02
staatskanzlei@nw.ch
Stans, 22. November 2022

Ausführungsrecht zum Informationssicherheitsgesetz. Stellungnahme

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 24. August eröffnete das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) bei den Kantonen das Vernehmlassungsverfahren zum Ausführungsrecht zum Informationssicherheitsgesetz.

Wir danken Ihnen für diese Möglichkeit und lassen uns wie folgt vernehmen.

1 Vorbemerkung

Der Regierungsrat Nidwalden nimmt zur Kenntnis, dass sowohl das Informationssicherheitsgesetz (ISG) als auch die dazugehörigen Verordnungen die Kantone meist nur indirekt betreffen, wenn sie auf Daten des Bundes zugreifen oder diese bearbeiten. Zudem muss festgehalten werden, dass zum heutigen Zeitpunkt einige Bestimmungen nicht abschliessend geregelt sind, die für die Kantone wichtig sein werden. Dies betrifft v.a. die Revision des ISG samt Verordnung bezüglich der Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen (Kapitel 5 des ISG). Die generellen Anpassungen werden jedoch unterstützt und gehen mit der Berücksichtigung des vernetzten, digitalisierten Umfelds mit dem vermehrten Datenaustausch nach dem "Once-Only-Prinzip" in die richtige Richtung. Die Informationssicherheit als Verbundsaufgabe mit vernetzter Verantwortung, die gemeinsame Ziele definiert und ein koordiniertes Vorgehen unter Beachtung von Minimalstandards verfolgt, wird als wichtig erachtet.

2 Beantwortung der Fragen

Zu den konkreten Fragen des VBS wird wie folgt Stellung genommen:

1. Ist die Umsetzung der Verordnungen für die Kantone verständlich?
Die zugestellten Unterlagen sind mehrheitlich verständlich. Es bestehen im Detail Unklarheiten, ob die Kantone nicht grundsätzlich als "Dritte" zu bezeichnen sind. Zudem wird der Begriff "Kantone" im Ausführungsrecht zum ISG neu definiert und umfasst auch öffentlich-rechtliche Körperschaften, Anstalten oder Stiftungen. Eine kohärente Begrifflichkeit – welche im Einklang mit der Definition gemäss Art. 3 der Bundesverfassung steht – würden wir begrüssen. In einem weiteren Schritt wären auch die weiteren Körperschaften etc. separat zu erwähnen.

2. *Wie gedenken die Kantone, die Verordnungen umzusetzen?*
Die Zuständigkeit zum Erlass der entsprechenden Regelungen liegt bei den einzelnen Kantonen. Jeder Kanton regelt dies eigenständig. Im Kanton Nidwalden wird (gestützt auf die bundesrechtlichen Vorgaben und die weiteren Bestimmungen im kantonalen Recht) zu klären sein, ob die erforderlichen Bestimmungen in einem formellen Gesetz oder auf Verordnungsstufe erlassen werden müssen bzw. können.

3. *Mit welchen finanziellen Auswirkungen rechnen die Kantone?*
Dies ist zum aktuellen Zeitpunkt schwierig abzuschätzen, da noch nicht alle Rahmenbedingungen abschliessend definiert sind. Es ist aber davon auszugehen, dass erweiterte Definitionen, Klassifizierungen der Systeme und Risikoabschätzungen mit allen Beteiligten vorgenommen und diese kontinuierlich überprüft werden müssen. Bei einer zentralen Organisation der Koordinationsaufgaben für beide Kantone mit allen Gemeinden gehen wir aktuell von jährlichen Mehrkosten von ca. CHF 100'000.- aus.

4. *Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörde bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?*
Das Informatikleistungszentrum der Kantone Obwalden und Nidwalden (ILZ) hat seit mehreren Jahren ein entsprechendes Knowhow aufgebaut und kennt die Voraussetzungen für die Umsetzung eines Informationssicherheits-Managementsystem (ISMS). Zudem ist in der neuen Informatik-Vereinbarung der Kantone Obwalden und Nidwalden explizit vorgesehen, dass das ILZ für die Umsetzung der Informationssicherheit zuständig sein soll. Es ist somit in Zukunft eine gesetzliche Grundlage vorhanden, um das ILZ als Ansprechpartner für die Bundesbehörde zu bezeichnen. Das ILZ führt diesbezüglich bereits einen aktiven Informationsaustausch mit den Bundesbehörden (Sicherheitsverbund Schweiz, NCSC).

Der Regierungsrat Nidwalden bedankt sich für die Möglichkeit zur Stellungnahme, bittet um Kenntnisnahme der Antworten sowie die Berücksichtigung der vorgebrachten ergänzenden Anliegen.

Freundliche Grüsse
NAMENS DES REGIERUNGSRATES

Joe Christen
Landammann

REGIERUNGSRAT · KANTON NIDWALDEN ·

lic. iur. Armin Eberli
Landschreiber

Geht an:
- sicherheit.vbs@gs-vbs.admin.ch

Kanton Obwalden

Der Vorsteher des Sicherheits- und Sozialdepartements SSD

CH-6060 Sarnen, Enetriederstrasse 1, SSD

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

per Mail an:
sicherheit.vbs@gs-vbs.admin.ch

Referenz/Aktenzeichen: OWSTK.4455
Unser Zeichen: ks

Sarnen, 17. November 2022

Ausführungsrecht zum Informationssicherheitsgesetz; Stellungnahme.

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Für die Einladung zur Vernehmlassung zum Ausführungsrecht zum Informationssicherheitsgesetz danken wir Ihnen.

Sowohl das Informationssicherheitsgesetz (ISG) als auch die vorliegenden dazugehörigen Verordnungen betreffen die Kantone, wenn auch teilweise nur indirekt, namentlich wenn sie auf Daten des Bundes zugreifen oder diese bearbeiten. Die vorgeschlagenen Anpassungen unterstützen wir. Sie gehen mit der Berücksichtigung des vernetzten, digitalisierten Umfelds mit dem vermehrten Datenaustausch nach dem "once-only-Prinzip" in die richtige Richtung. Die Informationssicherheit als Verbundsaufgabe mit vernetzter Verantwortung, die gemeinsame Ziele definiert und ein koordiniertes Vorgehen unter Beachtung von Minimalstandards verfolgt, erachten wir ebenfalls als korrekt und wichtig.

Gerne nehmen wir zu den im Einladungsschreiben zur Stellungnahme aufgeführten vier konkreten Fragen wie folgt Stellung:

1. Ist die Umsetzung für die Kantone verständlich?
Wir erachten die uns zugestellten Unterlagen mehrheitlich als verständlich. Unklar ist für uns die Frage, ob die Kantone nicht grundsätzlich als "Dritte" zu bezeichnen sind. Der Begriff "Kantone" wird im Ausführungsrecht zum ISG so definiert, dass er auch öffentlich-rechtliche Körperschaften, Anstalten oder Stiftungen umfasst. Eine einheitliche Bezeichnung gemäss Art. 3 der Bundesverfassung

Sicherheits- und Sozialdepartement SSD
Enetriederstrasse 1, 6060 Sarnen
Tel. +41 41 666 62 19
ssd@ow.ch
www.ow.ch

würden wir begrüssen und damit einhergehend eine genaue Definition der Zuteilung der Kantone und deren weiteren Körperschaften.

2. Wie gedenken die Kantone, die Verordnungen umzusetzen?
Zu dieser Frage sind unserer Ansicht nach noch weitere Abklärungen nötig und sie kann deshalb zum jetzigen Zeitpunkt noch nicht abschliessend beantwortet werden. Bezüglich der Verordnung über die Personensicherheitsprüfung gehen wir davon aus, dass noch weitere Personen in der kantonalen Verwaltung (insbesondere der Kantonspolizei) einer Sicherheitsprüfung unterstellt werden könnten, begründet mit dem jeweiligen Schutzgrad der bearbeiteten Daten.

3. Mit welchen finanziellen Auswirkungen rechnen die Kantone?
Die finanziellen Auswirkungen sind zum aktuellen Zeitpunkt noch schwierig abzuschätzen, da noch nicht alle Rahmenbedingungen abschliessend definiert sind. Es ist jedoch davon auszugehen, dass erweiterte Definitionen, Klassifizierungen der Systeme und Risikoabschätzungen vorgenommen und diese kontinuierlich überprüft werden müssen. Für den Kanton Obwalden schätzen wir jährliche Kosten von rund Fr. 50 000.–.

4. Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörde bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?
Im Kanton Obwalden ist das InformatikLeistungsZentrum Obwalden – Nidwalden (ILZ), Güterstrasse 3, 6060 Sarnen 2, info@ilz.info, Tel. 041 666 60 00 zuständig.

Wir danken Ihnen, sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren, für die Berücksichtigung unserer Ausführungen.

Freundliche Grüsse

Christoph Amstad
Landammann

Kopie an:
- Kantonale Mitglieder der Bundesversammlung
- Kantonspolizei
- Staatsanwaltschaft
- Datenschutzbeauftragter Schwyz Obwalden Nidwalden
- InformatikLeistungsZentrum Obwalden – Nidwalden
- Staatskanzlei (Kommunikation)

Kanton Schaffhausen
Departement des Innern
Mühlentalstrasse 105
CH-8200 Schaffhausen
www.sh.ch

Telefon 052 632 74 61
sekretariat.di@sh.ch

Departement des Innern

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz
und Sport VBS

per E-Mail an:
sicherheit.vbs@gs-vbs.admin.ch

Schaffhausen, 21. November 2022

Ausführungsrecht zum Informationssicherheitsgesetz

Sehr geehrte Damen und Herren

Mit Schreiben vom 24. August 2022 haben Sie die Kantonsregierungen zur Vernehmlassung in eingangs erwähnter Angelegenheit eingeladen und die Kantone gebeten, vier Fragen zu beantworten, um die Praxistauglichkeit der neuen Bestimmungen sowie die Kostenfolgen zu beurteilen. Ihre Einladung wurde zuständigkeitshalber an das Departement des Innern weitergeleitet. Wir bedanken uns für die Möglichkeit zur Stellungnahme und lassen uns wie folgt vernehmen:

Wir begrüssen die unterbreiteten Vorlagen grundsätzlich. Insbesondere ist der Umstand positiv zu werten, dass in der neuen Verordnung über die Personensicherheitsprüfungen, wie mit dem Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) angestrebt, dem Grundsatz der Erforderlichkeit bzw. der Datensparsamkeit gebührend Rechnung getragen wird.

Die von Ihnen gestellten Fragen können wir wie folgt beantworten:

1. Ist die Umsetzung der Verordnungen für die Kantone verständlich?

Ja. Indes begrüssen wir, dass die Fachstelle PSP als Ansprechstelle eine Erleichterung für die Umsetzung der Bundesvorgaben sein wird. Die Möglichkeit des Beizugs der Bundesstelle gewährleistet eine möglichst einheitliche Umsetzung bei den Kantonen.

2. Wie gedenken die Kantone, die Verordnungen umzusetzen?

Mit der Verordnung betreffend Informatiksicherheit vom 2. Dezember 2014 (Informatiksicherheitsverordnung, ISV; SHR 174.102) besteht im Kanton Schaffhausen bereits eine Informationssicherheitsgesetzgebung. Der Kanton wird eine Revision der ISV prüfen, um die eidgenössischen Vorgaben und die technischen Anforderungen umzusetzen. Insbesondere wird zu prüfen sein, ob die bestehenden Sicherheitsbestimmungen des Kantons Schaffhausen mit den bundesrechtlichen Vorgaben gleichwertig sind. Eine «gleichwertige Informationssicherheit» liegt vor, wenn andere als in der ISV vorgesehene Sicherheitsvorkehrungen nach dem Stand der Technik eine vergleichbare und mindestens gleich hohe beziehungsweise starke Wirkung erzielen (Art. 85 Abs. 1 ISG). Die Beurteilung, ob eine gleichwertige Informationssicherheit vorliegt, soll im Ermessen des Kantons liegen.

Seit 2015 verfügt der Kanton Schaffhausen über einen Informatiksicherheitsbeauftragten (ISB). Darüber hinaus ist eine Stelle für einen kantonalen Chief Information Security Officer (CISO) unmittelbar geplant. Gemäss § 4 Abs. 5 ISV ist der ISB der KSD (Informatikunternehmen von Kanton und Stadt Schaffhausen) verantwortlich für den Aufbau, die Implementierung, die Umsetzung und die Anpassung der gesamten Sicherheitsgrundsätze für den Informatik- und Telekommunikationsbetrieb der KSD als zentrale IT-Servicedienstleisterin und gegenüber allen dieser Verordnung unterstehenden Organisationseinheiten. Dies sind gemäss § 2 der ISV die kantonale Verwaltung, die Justizbehörden und die öffentlich-rechtlichen Anstalten, sowie die Gemeinden und alle öffentlich-rechtlichen Körperschaften im Kanton Schaffhausen, soweit sie gemeinsam mit der kantonalen Verwaltung Informatiksysteme und -anwendungen betreiben, Daten oder Informationen austauschen oder eigene Anwendungen bei der KSD betreiben lassen. Für die Beratung der Informatiksicherheitsstelle besteht ein Security-Board (§ 5 Abs. 6 ISV). Dieses ist zudem Kontrollorgan über die Tätigkeiten des Informatiksicherheitsbeauftragten und Eskalationsstelle. Im Übrigen verfügt der Kanton Schaffhausen bereits über ein zertifiziertes Informationssicherheits-Managementsystem (ISMS) gemäss ISO 27001.

Für strategische Belange ist ein neues kantonales Fachgremium geplant, in welchem der CISO, der ISB der KSD und die weiteren kantonalen ISB vertreten sein werden.

3. Mit welchen finanziellen Auswirkungen rechnen die Kantone?

Gemäss erläuternden Bericht (Kapitel 5.2) ist die Anwendung des ISG und der Verordnungen auf die Kantone beschränkt. Die Umsetzungskosten sollen vorwiegend im Rahmen von Projekten oder beim Bezug von Dienstleistungen des Bundes anfallen. Der Bund hat diese Kosten noch nicht näher beziffert (vgl. Erläuternder Bericht, S. 46). Eine indirekte Folge der neuen Bundesgesetzgebung dürfte zudem sein, dass entsprechende Sicherheitsstandards in Analogie zum Bund fortan auch verstärkt auf kantonaler Ebene gefordert werden. Darüber hinaus sind

zusätzlicher Aufwand für die Revision der kantonalen Gesetzgebung sowie zusätzliche Kosten für IT-Ressourcen zu erwarten. Weitere Kosten sind nicht abschätzbar.

4. *Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?*

Gerne stehen Ihnen der kantonale Informatiksicherheitsbeauftragte, Michael Bachmann (michael.bachmann@ksd.ch), sowie der kantonale Chief Information Security Officer, Daniel Messerli (daniel.messerli@ksd.ch), für Fragen zur Verfügung.

Für die Kenntnisnahme und die Berücksichtigung unserer Stellungnahme danken wir Ihnen.

Freundliche Grüsse
Der Departementssekretär

Christoph Aeschbacher

Regierungsrat des Kantons Schwyz

VERSENDET AM 02. NOV. 2022

kantonschwyz

6431 Schwyz, Postfach 1260

per E-Mail
VBS
3003 Bern

sicherheit.vbs@gs-vbs.admin.ch

Schwyz, 25. Oktober 2022

Ausführungsrecht des Informationssicherheitsgesetzes
Vernehmlassung des Kantons Schwyz

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 24. August 2022 haben Sie die Kantonsregierungen eingeladen, zur oben erwähnten Vernehmlassungsvorlage bis 24. November 2022 Stellung zu nehmen.

Der Kanton Schwyz beschränkt sich in seiner Vernehmlassung auf die in der Einladung aufgeworfenen Fragen und nimmt dazu gerne wie folgt Stellung:

1. Ist die Umsetzung der Verordnungen für die Kantone verständlich?

Die Umsetzung der Verordnungen ist verständlich. Die konkreten Rahmenbedingungen des Bundes zur Wahrung der Informationssicherheit werden pro Anwendungsfall und nach Vorgabe der involvierten Bundesstelle zu beachten sein.

2. Wie gedenken die Kantone die Verordnungen umzusetzen?

a) Personensicherheitsprüfungen werden in Teilbereichen der Kantonsverwaltung bereits vorgenommen. Mit der neuen Verordnung werden diese tendenziell ausgeweitet.
b) Die Erarbeitung eines Information Security Management Systems (ISMS) ist gemäss Verordnung für die Kantone nicht obligatorisch. Die Einführung eines ISMS wird derzeit evaluiert.
c) Mittels einer anstehenden Überarbeitung der entsprechenden kantonalen Verordnung wird eine Ausweitung von IT-Sicherheitsfunktionen in den Departementen/Ämtern angestrebt. Diese existieren heute formell noch nicht, wobei die vorliegende Vernehmlassung den entsprechenden Bedarf klar aufzeigt.

3. Mit welchen finanziellen Auswirkungen rechnen die Kantone?

Die finanziellen Auswirkungen für den Kanton Schwyz sind derzeit schwierig abzuschätzen. Es ist von einem unteren fünfstelligen Betrag auszugehen.

4. Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?

Als Kontaktstelle im Kanton Schwyz wurde die Stabstelle «IT-Sicherheit» im Amt für Informatik bestimmt. Ansprechsperson ist Jan Gerlach, IT-Sicherheitsbeauftragter, jan.gerlach@sz.ch, 041 819 24 74.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und versichern Sie, Frau Bundesrätin, unserer vorzüglichen Hochachtung.

Im Namen des Regierungsrates:

André Rüegsegger
Landammann

Regierungsrat Kanton Schwyz

Dr. Mathias E. Brun
Staatsschreiber

KANTON solothurn

Finanzdepartement

Rathaus
Barfüssergasse 24
4509 Solothurn
Telefon 032 627 20 57
finanzdepartement@fd.so.ch
so.ch

Peter Hodel
Regierungsrat

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz
und Sport
Frau Bundesrätin Viola Amherd
Bundeshaus Ost
3003 Bern

17. November 2022

Ausführungsrecht zum Informationssicherheitsgesetz

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 24. August 2022 haben Sie uns das Ausführungsrecht zum Informationssicherheitsgesetz zur Vernehmlassung unterbreitet. Für die Gelegenheit zur Stellungnahme bedanken wir uns.

Wir begrüssen die Umsetzung der Verordnung in den Kantonen. Sie ist eine wichtige Grundlage bei der heutigen und der zukünftigen Bedrohungslage. Im Kanton Solothurn ist im Amt für Informatik und Organisation (AIO) bereits ein Information Security Management System (ISMS) nach der Norm ISO/IEC 27001 eingeführt. Dieses wird laufend betrieben und aktuell gehalten. Als nächsten Schritt und Ziel wird es sein, dieses zu zertifizieren, wodurch auch die kontinuierliche Überprüfung von externer Seite her gewährleistet wird.

Des Weiteren wurden sowohl eine Leitlinie Informationssicherheit, als auch ein Konzept Informationssicherheit erstellt und von der Regierung beschlossen und freigegeben. Darin geregelt sind neben den Aufgaben auch organisatorische Bestimmungen, Ziele und Verantwortlichkeiten für den Bereich Informationssicherheit. Dese gelten über alle Dienststellen der kantonalen Verwaltung.

Die Umsetzung der Verordnungen werden für den Kanton Solothurn namentlich in personeller Hinsicht Auswirkungen nach sich ziehen. Neben 300 Stellenprozenten im AIO, wird mit zusätzlichen 425 Stellenprozenten für die weiteren Dienststellen der kantonalen Verwaltung gerechnet. Weiter fallen Investitionen in ISMS- und Sicherheitssysteme an, welche ebenfalls indirekt mit der Umsetzung der beschriebenen Verordnungen zu tun haben.

Die zusätzlichen finanziellen Aufwände, welche im Zusammenhang mit dem neuen ISG entstehen, sind nur schwer zu beziffern. Gemäss einer groben Schätzung für das erste Jahr gehen wir für die kantonale Verwaltung von ca. 300'000 Franken aus (Personal und Investitionen).

Als Ansprechpartner für die Bundesbehörden für Themen der Informationssicherheit in der kantonalen Verwaltung ist die Abteilung «Informationssicherheit / Qualitätssicherung QS» im AIO des Kanton Solothurn zuständig. Toni Widmer, Leiter Informationssicherheit / Qualitätssicherung steht Ihnen gerne zur Verfügung.

Folgende Abgrenzungen gilt es spezifisch zu beachten:

- Das AIO betreibt das ISMS für seine Aufgaben und Prozesse als Betreiber der kantonalen Informatikumgebung, mit Schnittstellen zu Informatik-Projekten. Der Geltungsbereich des ISMS ist somit auf das AIO reduziert und umfasst nicht die gesamte kantonale Verwaltung.
- Die Zertifizierung ISO 27001 umfasst alleine den Geltungsbereich des AIO. Die Zertifizierung beinhaltet somit nicht die gesamte kantonale Verwaltung.
- Die Solothurner Spitäler AG, die Fachhochschule Nordwestschweiz, die öffentlich-rechtlichen Anstalten des Kantons, die Gemeinden des Kantons Solothurn und der Informatik-Einsatz in den kantonalen Schulen für Unterrichtszwecke unterstehen nicht dem Zuständigkeitsbereich des AIO. Das AIO hat diesbezüglich auch keine Weisungsbefugnisse.

Freundliche Grüsse

Peter Hodel
Regierungsrat

Regierung des Kantons St.Gallen

EINGANG
GS - VBS
16. NOV. 2022
251.2-35/1/6/14/2

Regierung des Kantons St.Gallen, Regierungsgebäude, 9001 St.Gallen

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport
Bundeshaus Ost
3003 Bern

Regierung des Kantons St.Gallen
Regierungsgebäude
9001 St.Gallen
T +41 58 229 74 44
info.sk@sg.ch

St.Gallen, 15. November 2022

Ausführungsrecht zum Informationssicherheitsgesetz; Vernehmlassungsantwort

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 24. August 2022 laden Sie uns zur Vernehmlassung zum Ausführungsrecht zum Informationssicherheitsgesetz (ISG) ein.

Wir danken für diese Gelegenheit und können Ihnen mitteilen, dass wir mit dem vorgeschlagenen Vorentwurf gemäss Vorlage einverstanden sind.

Die von Ihnen gestellten Fragen, können wir wie folgt beantworten:

1. Die Umsetzung der Verordnungen ist verständlich.
2. Da einige Teile des ISG für die Kantone verbindlich umzusetzen sind, werden die Sicherheitsanforderungen im Kanton möglichst synchron auf die Grundschutzanforderungen des Bundes ausgerichtet. Ein entsprechender Abgleich des kantonalen Informationssicherheits-Managementsystems ist bereits in Arbeit. Eine Impactanalyse wird zeigen, welche konkreten Massnahmen in der Folge in Projekten umzusetzen sind. Die Zugriffrechte sollen im Einklang mit den Vorgaben des Bundes an diejenigen Rollenträger in den jeweiligen Ämtern erteilt werden, die sie für die Erfüllung ihrer gesetzlichen Aufgaben benötigen.
3. Eine konkrete Aussage zu den unmittelbaren finanziellen Auswirkungen kann zum heutigen Zeitpunkt nicht gemacht werden.
4. Ansprechperson im Kanton St.Gallen ist der Dienst für Informatikplanung im Finanzdepartement, konkret Peter Müntener, Abteilungsleiter Informations- und Cybersicherheit (Unterstrasse 22, 9001 St.Gallen, peter.muentener@sg.ch, 058 229 14 55).

Wir danken Ihnen für die Kenntnisnahme.

Im Namen der Regierung

Marc Mächler
Vizepräsident

Dr. Benedikt van Spyk
Staatssekretär

KANTON ST. GALLEN
REGIERUNG

Zustellung auch per E-Mail (pdf- und Word-Version) an:
sicherheit.vbs@gs-vbs.admin.ch

Numero			Bellinzona
5736	fr	0	23 novembre 2022

Consiglio di Stato
Piazza Governo 6
Casella postale 2170
6501 Bellinzona
telefono +41 91 814 41 11
fax +41 91 814 44 35
e-mail can@ti.ch
web www.ti.ch

Repubblica e Cantone
Ticino

Il Consiglio di Stato

Dipartimento federale della difesa, della protezione della popolazione e dello sport
DDPS

Invio per posta elettronica (Word e pdf): sicherheit.vbs@gs-vbs.admin.ch

Procedura di consultazione concernente il diritto di esecuzione della legge sulla sicurezza delle informazioni

Gentili signore, egregi signori,

abbiamo ricevuto la vostra lettera del 24 agosto 2022 in merito alla summenzionata procedura di consultazione. Le modifiche delle ordinanze, unitamente al relativo rapporto esplicativo, sono stati da noi esaminati in collaborazione con il Centro sistemi informativi e i servizi di polizia interessati.

Ringraziando per l'opportunità che ci viene offerta di esprimere il nostro giudizio, rispondiamo come segue alle vostre domande.

1. L'attuazione delle ordinanze è comprensibile per i Cantoni?

L'attuazione delle ordinanze è comprensibile per quanto riguarda gli scopi e le fasi d'implementazione. Per quanto attiene alle misure tecniche per la salvaguardia delle informazioni si intravvede una competenza maggiorata per il Centro sistemi informativi dell'Amministrazione cantonale ticinese (di seguito: CSI).
Per quanto concerne invece le verifiche di sicurezza, non appare del tutto chiaro in quale misura i funzionari delle unità amministrative e giudiziarie dell'Amministrazione cantonale, subordinatamente altre entità esterne che espletano compiti secondo le normative federali, dovranno essere sottoposti a tali verifiche. Sebbene la linea evidenziata dal rapporto esplicativo determini una riduzione di funzioni per le quali sarà richiesto un controllo di sicurezza, l'impossibilità di consultare l'elenco completo ed esaustivo delle funzioni sottoposto alla verifica di sicurezza pone degli interrogativi sul piano dell'applicazione pratica. Nello specifico, per la Polizia cantonale si rileva oggi un unico servizio sottoposto a verifiche di sicurezza delle persone e misure tecniche atte a salvaguardare la sicurezza delle informazioni; il Servizio Informazioni Federali (di seguito: SIF) è subordinato per questi aspetti al Servizio delle attività informative della Confederazione (di seguito: SIC).

2. In che modo i Cantoni intendono attuare le ordinanze?

Il nodo principale risiede nella mappatura dei processi che coinvolgono le Autorità cantonali, al fine di verificarne l'allineamento degli standard di sicurezza imposti dalle normative. La metodica d'implementazione dipenderà dalla quantità di discrepanze e quindi di adattamenti necessari.
Da una prima analisi, risulta che le norme cantonali in ambito di sicurezza delle informazioni, si limitano alla Legge sulla protezione dei dati personali del 9 marzo 1987 (LPDP; RL 163.100) che si applica tuttavia all'elaborazione di dati personali, allo scopo di proteggere la personalità e la sfera privata delle persone i cui dati vengono elaborati da organi pubblici. Si tratta dunque di norme che sono a tutela dei dati personali e non delle informazioni che potrebbero danneggiare lo Stato.
Parimenti, vi sono delle misure sussidiarie per la sicurezza delle informazioni in generale si fondano su normative generali che regolamentano l'obbligo al segreto d'ufficio così come al segreto istruttorio, fiscale, ecc. Queste norme di fondo mirano alla salvaguardia delle informazioni in termini preventivi generalizzati e non specificatamente per rapporto ai rischi potenziali.

Per quanto riguarda la categorizzazione delle informazioni, occorre tener conto che a livello cantonale non esiste un sistema di classificazione, pertanto è determinante la categorizzazione dei servizi della Confederazione per i quali i diversi servizi del Cantone svolgono le attività. L'allineamento alle norme in consultazione deve pertanto limitarsi ai servizi che trattano informazioni classificate secondo gli standard della Confederazione. Per la Polizia cantonale, il trattamento di informazioni "Segrete" e "Confidenziali" è concentrato presso il SIF che opera sotto l'egida della LAIn su mandato del SIC, per quanto attiene l'ambito della protezione dello Stato. Il medesimo servizio tratta inoltre informazioni classificate relative alle misure di sicurezza emanate dal Servizio Federale di Sicurezza (Fedpol). Per quest'ultimo ambito, occorre tenere conto di altri servizi che sono subordinatamente coinvolti nell'attuazione delle misure, rispettivamente sono parte integrante degli Stati maggiori cantonali, quali ad esempio la Sezione Pianificazione Impiego (sotto lo Stato maggiore operativo), il Reparto Interventi Speciali (appartenente allo Stato maggiore) e il Reparto Giudiziario 4 (sotto la Polizia giudiziaria). Trattandosi di un elenco non esaustivo, al fine di determinare quali servizi della Polizia cantonale saranno influenzati dalle norme in consultazione occorrerà procedere con un "censimento" dei servizi che trattano informazioni classificate.

3. Quali ripercussioni finanziarie prevedono i Cantoni?

Anche per questo punto è necessario procedere a un esame della situazione determinando l'entità degli interventi da attuare. In un primo momento l'onere economico sarà determinato dalle risorse umane impiegate per la verifica dell'infrastruttura e la mappatura dei diversi processi. L'esito di questa prima fase potrà generare ulteriori oneri finanziari, ad esempio per l'esecuzione di controlli di sicurezza necessari (funzionari, personale ditte fornitrici, ecc.) come pure oneri relativi all'adeguamento di infrastrutture risultate non conformi alle normative in oggetto. Ai costi relativi alla verifica e all'attuazione di eventuali misure sanatorie, potrebbero poi aggiungersi gli oneri derivanti dalla formazione del personale e dall'unità amministrativa del servizio designato quale *Single Point Of Contact* (SPOC, ossia interlocutore) in materia di sicurezza delle informazioni.

Le misure minime di sicurezza (cfr. TIC) sono applicate per quanto riguarda l'accesso a piattaforme della Confederazione (vale per Polizia), in ossequio alla OCiber. È prevista una categorizzazione ulteriore di mezzi informatici, che andrà verosimilmente a toccare ambiti specifici di competenza esclusiva della Confederazione, caratterizzati da eccezioni puntuali quali il SIC che demanda parte dei compiti al SIF. Per quanto concerne il SIF, è necessario ricordare che le informazioni della Confederazione trattate non possono essere gestite dai cantoni (cfr. art. 46 della legge federale sulle attività informative del 25 settembre 2015; LAIn, RS 121) e di conseguenza la Confederazione fornisce, assumendosi i costi, l'infrastruttura necessaria per adempiere al compito in pieno rispetto di tutti i parametri e legali e di sicurezza. Diversamente per gli altri servizi di Polizia dove, in linea generale, occorrerà identificare le misure di sicurezza non ancora implementate e l'applicazione di un *Information Security Management System* (di seguito: SGSI) ex-novo o l'adattamento di un eventuale SGSI già in vigore per l'Amministrazione cantonale. Un ulteriore onere finanziario potrebbe essere generato dai controlli di sicurezza richiesti per i funzionari che detengono i diritti d'accesso a sistemi informatici per il trattamento di dati personali degni di particolare protezione o informazioni classificate, come pure per gli addetti, interni o esterni all'Amministrazione cantonale incaricati della manutenzione e dell'infrastruttura.

4. **Per le questioni concernenti la sicurezza delle informazioni i Cantoni dovranno inoltre designare un servizio che fungerà da interlocutore per le autorità federali. Chi è la persona di contatto nel vostro Cantone?**

La sicurezza delle informazioni riguarda più Sezioni in due Dipartimenti diversi, ossia il Dipartimento delle finanze e dell'economia (DFE) per logistica e infrastruttura informatica e il Dipartimento delle Istituzioni per la Polizia, la Sezione del militare e della protezione della popolazione (SMPP) e la Sezione della popolazione (SPOP).
A nostro avviso quale interlocutore per le autorità federali dovrebbe essere identificato una persona che possa fungere da coordinatore per le diverse aree cantonali che sottostanno alle normative in oggetto e in particolare al SGSI. A tal proposito segnaliamo l'intenzione di formalizzare per l'anno prossimo una posizione di *Chief Security Officier* (CSO) con una competenza specifica per la sicurezza.

Vogliate gradire, gentili signore, egregi signori, i sensi della nostra massima stima.

PER IL CONSIGLIO DI STATO

Il Presidente
Claudio Zali

Il Cancelliere
Arnoldo Coduri

Copia a:
- Dipartimento delle istituzioni (di-dir@ti.ch)
- Segreteria generale del Dipartimento delle istituzioni (di-sg.ap@ti.ch)
- Comando della Polizia cantonale (polizia-segr@polca.ti.ch; servizio.giuridico@polca.ti.ch)
- Divisione della giustizia (di-dg@ti.ch)
- Deputazione ticinese alle Camere federali (can-relazioniesterne@ti.ch)
- Pubblicazione in Internet

Der Regierungsrat des Kantons Thurgau

Thurgau

Staatskanzlei, Regierungsgebäude, 8510 Frauenfeld

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
(VBS)
Frau Viola Amherd
Bundesrätin
Bundeshaus Ost
3003 Bern

Frauenfeld, 8. November 2022
653

Ausführungsrecht zum Informationssicherheitsgesetz

Vernehmlassung

Sehr geehrte Frau Bundesrätin

Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum Entwurf für drei neue Verordnungen und eine Verordnungsänderung im Zusammenhang mit der Umsetzung des Informationssicherheitsgesetzes (ISG; SR 128) und teilen Ihnen mit, dass wir mit den Vorlagen grundsätzlich einverstanden sind. Zu zwei Verordnungsentwürfen gestatten wir uns die nachfolgenden Bemerkungen und bitten Sie, diese bei den weiteren Rechtsetzungsarbeiten zu berücksichtigen.

1. Art. 16 der Verordnung über die Informationssicherheit bei der Bundesverwaltung und bei der Armee (Informationssicherheitsverordnung, ISV)

Bezüglich Art. 16 Abs. 1 ISV besteht nach unserer Auffassung die Unklarheit, ob wirklich das Öffentlichkeitsgesetz des Bundes für kantonale Belange zur Anwendung kommt oder ob allenfalls das kantonale Öffentlichkeitsgesetz gelten soll. Art. 3 Abs. 2 ISG hält fest, dass die Bestimmungen des neuen Rechtes nur subsidiär anwendbar sind. Dieser Vorbehalt wird auch in Art. 2 Abs. 6 ISV wiederholt, indem explizit auf Art. 3 Abs. 2 ISG verwiesen wird. Dennoch ist nicht ganz klar, gestützt auf welche Rechtsgrundlage und durch welche Stelle Einsichtsgesuche zu erledigen wären. Da auf die Informatikmittel des Bundes zugegriffen wird oder weil Daten des Bundes bearbeitet werden, gehen wir davon aus, dass die kantonalen Öffentlichkeitsgesetze nicht zur Anwendung gelangen und entsprechende Gesuche an den Bund zu richten sind. Dies sollte in Art. 16 Abs. 3 ISV klarer erwähnt werden, indem ausdrücklich darauf hingewiesen wird, dass die kantonalen Öffentlichkeitsgesetze nicht gelten.

2. Anhang 7 zur Verordnung über die Personensicherheitsprüfungen (VPSP)

Es ist für uns nicht ersichtlich, weshalb bei der Grundsicherheitsprüfung nach Art. 34 ISG über den Weg von Art. 19 VPSP und Anhang 7 zur VPSP festgelegt werden darf, dass Angaben zu religiösen Tätigkeiten, weltanschaulichen Ansichten sowie über politische und gewerkschaftliche Tätigkeiten umfassend einverlangt und bearbeitet werden dürfen, wenn doch Art. 75 ISG solche Datenbearbeitungen nur erlaubt, soweit konkrete Bedrohungen und Gefahren bestehen. Die VPSP geht hier klar zu weit. Ebenso findet sich keine Rechtsgrundlage für Datenerhebungen zur Intimsphäre und Sexualität, zum Familienverhältnis, zur Identität der Eltern und zum Freundeskreis.

Mit freundlichen Grüssen

Die Präsidentin des Regierungsrates

Der Staatsschreiber

DER REGIERUNGSRAT · DES KANTONS THURGAU ·

Landammann und Regierungsrat des Kantons Uri

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz und Sport (VBS)
Papiermühlestrasse 20
3003 Bern

Ausführungsrecht zum Informationssicherheitsgesetz; Vernehmlassung

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Schreiben vom 24. August 2022 laden Sie den Regierungsrat des Kantons Uri ein, zum Ausführungsrecht des Informationssicherheitsgesetzes (ISG) sowie zu vier Fragen Stellung zu nehmen. Gerne äussern wir uns wie folgt:

I. Rückmeldung im Allgemeinen

Das Ausführungsrecht zum ISG dient in erster Linie der Informationssicherheit des Bundes. Dementsprechend finden die Erlasse hauptsächlich in der Bundesverwaltung Anwendung und haben lediglich eine begrenzte Auswirkung auf die Kantone.

Mangels Relevanz für die Kantone erübrigen sich Rückmeldungen zur Verordnung über Identitätsverwaltungssysteme und Verzeichnisdienste des Bundes (IAMV) sowie zur Verordnung über das Betriebssicherheitsverfahren (VBSV).

Die Informationssicherheitsverordnung (ISV) betrifft den Kanton Uri in Bezug auf die Bearbeitung von klassifizierte Informationen des Bundes und beim Zugriff auf die Informatikmittel des Bundes. Ein ausreichender Schutz der Informationen wird begrüsst und die diesbezüglichen Regelungen in der ISV werden als sinnvoll erachtet.

Die Verordnung über die Personensicherheitsprüfungen (VPSP) konkretisiert unter anderem die Datenerhebung bei Personensicherheitsprüfungen. Diese ist im ISG in Artikel 34 geregelt und unterscheidet zwischen einer Grundsicherheitsprüfung und einer erweiterten Personensicherheitsprüfung. Die VPSP wiederum sieht in Anhang 7 eine sehr umfassende Datenerhebung für alle Prüfstufen - folglich auch für die Grundsicherheitsprüfung - vor, welche teilweise im Widerspruch zum Gesetz zu stehen scheint und deutlich weitergeht als die Bestimmungen im heutigen Recht. Beispielsweise stellt sich die Frage, inwiefern sich religiöse oder weltanschauliche Ansichten, politische Tätigkeiten oder Angaben zu Intimsphäre und Sexualität (vgl. Anhang 7 VPSP) bei einer Grundsicherheitsprüfung ohne Befragung aus den gemäss Artikel 34 Absatz 1 ISG aufgeführten Datenquellen ableiten beziehungsweise erheben lassen. Auch hält Artikel 27 Absatz 3 ISG fest, dass Daten über die Ausübung verfassungsmässiger Rechte nur unter bestimmten Voraussetzungen erhoben werden dürfen. Demgegenüber lässt die VPSP eine uneingeschränkte Datenerhebung zu, beispielsweise betreffend Vereinstätigkeit, religiöse Tätigkeiten oder politische Aktivitäten. Entsprechend geht die in der VPSP vorgesehene Datenerhebung über die gesetzlich vorgesehene Datenerhebung hinaus.

II. Beantwortung der Fragen

1. Ist die Umsetzung der Verordnungen für die Kantone verständlich?

Diese Frage kann im Grundsatz bejaht werden, wobei in erster Linie die Informationssicherheitsverordnung und eher marginal die Verordnung über die Personensicherheitsprüfungen Auswirkungen auf die Kantone haben können. Da sich bestimmte Hilfsmittel seitens des Bundes erst in Ausarbeitung befinden und die Fachstelle des Bundes für Informationssicherheit noch aufgebaut werden muss, besteht in einigen Punkten Konkretisierungsbedarf. Insbesondere sollte der Bund die Anwendungen und Informationen benennen, an die erhöhte Anforderungen an die Informationssicherheit gestellt werden.

2. Wie gedenken die Kantone, die Verordnungen umzusetzen?

a) Informationssicherheitsverordnung (ISV)

Die Bestimmungen der ISV betreffend klassifizierte Informationen und betreffend Sicherheit im Einsatz von Informatikmitteln gelten für die Kantone nur, wenn sie nicht mindestens eine gleichwertige Informationssicherheit gewährleisten, wie sie das ISG verlangt. Gemäss dem erläuternden Bericht vom 24. August 2022 zum Informationssicherheitsgesetz (nachfolgend «Bericht ISG») liegt eine «gleichwertige Informationssicherheit» vor, wenn andere als in der ISV vorgesehene Sicherheitsvorkehrungen nach dem Stand der Technik gemäss Artikel 85 Absatz 1 ISG eine vergleichbare und mindestens gleich hohe beziehungsweise starke Wirkung erzielen, wobei die Kantone in erster Linie in eigenem Ermessen beurteilen, ob eine gleichwertige Informationssicherheit vorliegt (vgl. Seite 12). Sobald die Standardanforderungen und -massnahmen nach Artikel 85 ISG verfügbar sind, können kantonsintern entsprechende Überprüfungen der Sicherheitsvorkehrungen erfolgen. Der Bericht ISG hält auf Seite 7 weiter fest, dass die Kriterien zur Klassifizierung von Informationen und zur Sicherheitseinstufung von Informatikmitteln von Natur aus schwammig seien und ausgelegt werden müssten. Für die Umsetzung würden Hilfsmittel erstellt. Detaillierte Vorgaben betreffend konkrete Mass-

nahmen zum Schutz von klassifizierten Informationen und zur Gewährleistung der Informatiksicherheit würden voraussichtlich bis Ende 2023 erarbeitet. Demzufolge ist gegenwärtig keine exakte Aussage zur kantonsinternen Umsetzung der ISV möglich. Abschliessend kann indes festgehalten werden, dass die wichtigen Sicherheitsvorkehrungen im Kanton Uri grundsätzlich dem sogenannten «State of the Art» entsprechen.

b) Verordnung über Identitätsverwaltungssysteme und Verzeichnisdienste des Bundes (IAMV)

Artikel 2 regelt den Geltungsbereich, der keine Anwendung auf die Kantone vorsieht.

c) Verordnung über die Personensicherheitsprüfungen (VPSP)

Nach Artikel 29 Absatz 1 Buchstabe b ISG kann bei Angestellten eines Kantons, die eine sicherheitsempfindliche Tätigkeit ausüben, eine Personensicherheitsprüfung durchgeführt werden. Um Personensicherheitsprüfungen für bestimmte Angestellte einzuleiten, muss ein Kanton über eine ausreichende gesetzliche Grundlage verfügen, zur Gewährleistung der Informationssicherheit ähnliche Beurteilungen wie der Bund vornehmen wollen und mit dem VBS eine Leistungsvereinbarung abgeschlossen haben.

Auf Antrag eines Kantons entscheidet das VBS, für welche Funktionen der kantonalen Angestellten eine Personensicherheitsprüfung durchgeführt wird. Dabei konsultiert es vorgängig eine noch aufzubauende Fachstelle des Bundes für Informationssicherheit. Selbst wenn ein Kanton zukünftig eine bestimmte Kategorie von Angestellten nach dem ISG prüfen lassen möchte, kann zum heutigen Zeitpunkt aufgrund der noch ausstehenden Beurteilung durch die noch aufzubauende Fachstelle keine verbindliche Aussage bezüglich Umsetzung der VPSP getroffen werden. Einzelheiten würden im Übrigen in der Leistungsvereinbarung mit dem VBS geregelt werden.

d) Verordnung über das Betriebssicherheitsverfahren (VBSV)

Gemäss Artikel 3 ISG gelten für die Kantone nur die Bestimmungen (i) über klassifizierte Informationen, soweit sie klassifizierte Informationen des Bundes bearbeiten, und (ii) über die Sicherheit beim Einsatz von Informatikmitteln, soweit sie auf Informatikmittel des Bundes zugreifen. Diese Bestimmungen gelten nicht, wenn die Kantone eine mindestens gleichwertige Informationssicherheit gewährleisten.

Das Betriebssicherheitsverfahren betrifft die Wahrung der Informationssicherheit bei der Vergabe von sicherheitsempfindlichen Aufträgen der Bundesbehörden an Betriebe, die nicht ihrer unmittelbaren Aufsicht unterstehen. Entsprechend ist keine Umsetzung der VBSV durch die Kantone erforderlich.

3. Mit welchen finanziellen Auswirkungen rechnen die Kantone?

Der Bericht ISG erwähnt, die Anwendung des ISG und der Verordnungen auf die Kantone sei beschränkt und die Umsetzungskosten würden vorwiegend im Rahmen von Projekten oder beim Bezug von Dienstleistungen des Bundes anfallen, weshalb sie in diesem Kontext beurteilt werden müssten

(vgl. Seite 46). Eine Bezifferung der finanziellen Auswirkungen ist für den Kanton Uri unter anderem davon abhängig, ob für den Zugriff auf Informatikmittel des Bundes zusätzliche Sicherheitsvorkehrungen notwendig sind. Für diese Beurteilung fehlen zum heutigen Zeitpunkt - wie oben in der Antwort auf Frage 2 aufgezeigt - detaillierte Vorgaben beziehungsweise konkrete Beurteilungskriterien.

4. *Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist Ansprechperson in Ihrem Kanton?*

Das Amt für Informatik, das sämtliche Informatik-Dienstleistungen für alle kantonalen Verwaltungseinheiten erbringt.

Sehr geehrte Frau Bundesrätin, sehr geehrte Damen und Herren, wir bedanken uns für die Möglichkeit zur Stellungnahme und grüssen Sie freundlich.

Altdorf, 22. November 2022

Im Namen des Regierungsrats

Der Landammann Der Kanzleidirektor

REGIERUNGSRAT DES KANTONS URI

Urs Janett Roman Balli

Conseil d'Etat
Staatsrat
CP 670, 1951 Sion

CANTON DU VALAIS
KANTON WALLIS

2022.04962

P.P. CH-1951 Sion A Poste CH SA

Département fédéral de la défense, de la protection de la population et des sports
Madame Viola Amherd
Conseillère fédérale
Palais fédéral est
3003 Berne

Date 23 novembre 2022

Procédure de consultation sur la législation d'exécution de la Loi sur la sécurité de l'information

Madame la Conseillère fédérale,

Le Conseil d'État du canton du Valais vous remercie de le consulter sur les ordonnances d'exécution de la loi sur la sécurité de l'information (LSI).

Nous saluons tout particulièrement le choix d'impliquer les cantons dans le cadre du processus d'élaboration, notamment au travers des ateliers qui ont permis aux cantons de faire part de leur première analyse avant consultation.

Ordonnance sur la sécurité de l'information (OSI)
L'ordonnance sur la sécurité de l'information (OSI) s'applique aux cantons uniquement lors de traitements d'informations classifiées de la Confédération ou d'accès aux systèmes informatiques fédéraux. Nous relevons avec satisfaction que les cantons peuvent s'affranchir de ces dispositions légales s'ils mettent en œuvre une sécurité de l'information équivalente à celle proposée au travers de cette ordonnance.

Ordonnance sur les contrôles de sécurité relatif aux personnes (OCSP)
Les fonctions au sein du canton nécessitant un contrôle de sécurité personnel sont connues et les contrôles déjà réalisés depuis plusieurs années. Nous notons toutefois que selon l'explication de l'art. 8, al. 1, du rapport explicatif, le DDPS a reçu pour mandat d'homogénéiser les pratiques. Cela pourrait potentiellement impliquer l'élargissement des contrôles au sein de notre canton avec des coûts financiers liés non négligeables.

Ordonnance sur la procédure de sécurité relative aux entreprises (OPSE)
Nous n'avons rien de particulier à relever au sujet de cette ordonnance.

Ordonnance sur les systèmes de gestions des données d'identification et les services d'annuaires de la Confédération (OIAM)
Nous notons avec intérêt que l'interconnexion avec un IAM cantonal est dorénavant autorisée par cette nouvelle version de l'ordonnance et évaluerons, le cas échéant, la mise en place de cette nouvelle possibilité.

En complément à ces commentaires globaux, veuillez trouver ci-dessous les réponses aux questions posées :

1. **La mise en œuvre des ordonnances est-elle compréhensible pour les cantons ?**
   Les ordonnances sont compréhensibles, mais néanmoins complexes à interpréter sans le rapport explicatif qui contient de nombreuses précisions.

La notion de ce que référence un canton est par exemple à géométrie variable au vu du fonctionnement hétérogène des cantons suisses.

2. **Comment les cantons envisagent-ils la mise en œuvre des ordonnances ?**
Le canton du Valais dispose d'une politique de sécurité de l'information et de directives cadres qui fixent les objectifs, les principes généraux et l'organisation de la sécurité de l'information. Ces dernières s'appliquent à l'ensemble des autorités cantonales.

   Les communes et institutions cantonales ne sont par contre pas couvertes par les directives existantes. Toutefois, tous les accès vers la Confédération transitant par notre canton sont gérés et sécurisés par l'Administration cantonale.

   Le canton propose cependant aux communes qui le désire un soutien subsidiaire dans le domaine de la cybersécurité et proposera dès 2023 la solution eCyAd de sensibilisation, en cours de finalisation par la Confédération dans le cadre de la 2e stratégie de protection de la suisse contre les cyberrisques (SNPCv2).

3. **À quelles conséquences financières s'attendent les cantons ?**
Globalement le canton du Valais ne s'attend pas à des conséquences financières particulières en lien avec la mise en place de ces nouvelles ordonnances d'exécution. Toutefois une attention particulière sera portée sur les éventuels changements en lien avec les fonctions nécessitant un contrôle de sécurité personnel qui pourraient avoir une incidence financière quant au nombre de contrôles à effectuer.

4. **Les cantons devront désigner un Service faisant office d'interlocuteur pour les questions de sécurité de l'information. Quel est cet interlocuteur dans votre canton ?**
C'est le Service cantonal de l'informatique par sa cellule sécurité de l'information et son Responsable de la sécurité des systèmes d'information, M. Patrick Siggen, qui officiera comme interlocuteur pour le canton du Valais.

Concernant la mise en œuvre, l'élaboration de nombreuses prescriptions seront encore effectuées avant l'entrée en vigueur de la LSI et de ses ordonnances en 2023, nous sommes vivement intéressés par ces prescriptions dès leur disponibilité, en particulier celles liées à la classification des informations et des systèmes.

Nous vous remercions de nous avoir consultés et vous prions d'agréer, Madame la Conseillère fédérale, l'expression de notre considération distinguée.

Au nom du Conseil d'Etat

Le président

Roberto Schmidt

CANTON DU VALAIS
CONSEIL D'ETAT

Le chancelier

Philipp Spörri

Copie à sicherheit.vbs@gs-vbs.admin.ch

Regierungsrat, Postfach, 6301 Zug

Nur per E-Mail
Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Frau Bundesrätin Viola Amherd
Bundeshaus Ost
3003 Bern

Zug, 15. November 2022 sa

Ausführungsrecht zum Informationssicherheitsgesetz (ISG)
Stellungnahme des Kantons Zug

Sehr geehrte Frau Bundesrätin Amherd
Sehr geehrte Damen und Herren

Mit Schreiben vom 24. August 2022 hat uns das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport eingeladen, zum Ausführungsrecht betreffend das Informationssicherheitsgesetz (ISG) bis 24. November 2022 Stellung zu nehmen. Zum Ausführungsrecht äussern wir uns wie folgt:

1. Allgemeines

Das Ausführungsrecht zum ISG umfasst insgesamt drei neue Verordnungen:
- Informationssicherheitsverordnung (ISV),
- Verordnung über Personensicherheitsprüfungen (VPSP),
- Verordnung über das Betriebssicherheitsverfahren (VBSV)

und eine Änderung einer bestehenden Verordnung:
- Verordnung über Identitätsverwaltungs-Systeme (IAMV).

Ziel dieser Ausführungserlasse ist es, für alle Behörden und Organisationen des Bundes ein möglichst einheitliches Sicherheitsniveau zu erreichen, wobei die Kantone für eine gleichwertige Informationssicherheit sorgen müssen, wenn sie klassifizierte Informationen des Bundes bearbeiten oder auf seine Informatikmittel zugreifen. Das Inkrafttreten des ISG und seiner Verordnungen ist auf Mitte 2023 geplant. Für einen erfolgreichen Übergang ins neue Recht sehen sowohl das ISG (vgl. Art. 90) als auch die zugehörigen Ausführungsverordnungen (Art. 48 ISV, Art. 38 VPSP und Art. 25 VBSV) Übergangsfristen vor.

Der Regierungsrat des Kantons Zug unterstützt das vorerwähnte Ausführungsrecht, wobei nur im Bereich der ISV, die VPSP und und die IAMV Umsetzungsbedarf für den Kanton Zug besteht, weil die VBSV die Wahrung der Informationssicherheit bei der Vergabe von Aufträgen der Bundesbehörden an Dritte (Betriebe) regelt und daher nur für Bundesbehörden gilt.

2. Fragen

Zu den vier im Rahmen der Vernehmlassung gestellten Fragen äussern wir uns wie folgt:

2.1. Ist die Umsetzung der Verordnungen für die Kantone verständlich?

Die Vorgaben sind zwar verständlich, gehen aber zu wenig ausführlich auf die Pflichten der Kantone ein. Zudem macht der verfolgte föderalistische Ansatz, wonach die Vorgaben des Bundes nur dann gelten, wenn die kantonalen Regelungen den Sicherheitsanforderungen des Bundes nicht genügen, das Ganze kompliziert.

2.2. Wie gedenken die Kantone die Verordnung umzusetzen?

Die Hauptverantwortung für die Sicherheit bei der Bearbeitung von klassifizierten Informationen des Bundes liegt bei den kantonalen Organen, die diese Daten bearbeiten bzw. die auf die Informatikmittel des Bundes zugreifen (namentlich Amt für Zivilschutz und Militär, Notorganisation, Zuger Polizei, Verein für Arbeitsmarktmassnahmen). Diese Organe haben die erforderlichen Prozesse, Zuständigkeiten und Massnahmen festzulegen, um das vom Bund verlangte Sicherheitsniveau sicherstellen zu können. Dabei kommen die Vorschriften des Bundes nur dann zur Anwendung, wenn die Vorschriften und Massnahmen der Kantone den Sicherheitsanforderungen des Bundes nicht genügen.

Die Mitarbeitenden der Organe sind für die Einhaltung der Vorgaben beim Umgang mit den klassifizierten Informationen und den Informatikmitteln verantwortlich. Der richtige Umgang mit den klassifizierten Informationen und den Informatikmittel setzt voraus, dass die Bundesbehörden den Organen entsprechende Vorgaben machen.

Auf Basis dieser Vorgaben wird der Chief Information Security Officer (CISO) des Amtes für Informatik und Organisation des Kantons Zug (AIO) eine auf die entsprechenden Organe angepasste Schulung erarbeiten und durchführen. Das AIO ist zudem dafür verantwortlich, die nötigen Informatikmittel anzubieten und deren Sicherheit im Betrieb zu gewährleisten.

Die Organe sind verpflichtet, die Wirksamkeit der getroffenen Schutzmassnahmen periodisch zentral durch das AIO überprüfen zu lassen. Der CISO des AIO stellt sicher, dass die Fachstellen des Bundes für Informationssicherheit periodisch über die Ergebnisse der Überprüfungen orientiert wird.

2.2.1. ISV

Aktuell verfügt nur das AIO für Dienste, die es selber zur Verfügung stellt, über ein ISMS (Informationssicherheitsmanagementsystem) nach ISO27001. Die Bereitstellung des vom Bund geforderten ISMS Light führt zu beachtlichen Aufwendungen für Organe, die klassifizierte Informationen des Bundes auf ihren eigenen IT-Anwendungen bearbeiten oder auf Informatikmittel

des Bundes zugreifen. Dies ist beispielsweise der Fall bei der Zuger Polizei, die noch nicht wie das AIO über ein ISMS verfügt.

2.2.2. VPSP

Der Kanton verfügt mit den §§ 2bis und 2 ^{quater} des Gesetzes über das Arbeitsverhältnis des Staatspersonals (Personalgesetz; PG) vom 1. September 1994 (BGS 154.21) über eine allgemeine Grundlage für die Vornahme von Eignungsprüfungen, wobei gemäss § 2 Abs. 1 PG abweichende spezialgesetzliche Bestimmungen ausdrücklich vorbehalten sind.

Im Bereich Personensicherheitsüberprüfungen können die Kantone gar keine gleichwertige Sicherheit gewährleisten wie der Bund, weshalb schon aus diesem Grund hier die Vorschriften des Bundes gelten. Die Kantone haben nämlich keine direkte Möglichkeit, Daten über ihre Angestellten beim Nachrichtendienst des Bundes oder bei anderen Sicherheitsbehörden des Bundes zu erheben. Deshalb wird gemäss Artikel 29 Absatz 1 Buchstabe b des Informationssicherheitsgesetzes (ISG) eine Personensicherheitsprüfung des Bundes bei Angestellten der Kantone durchgeführt, die eine sicherheitsempfindliche Tätigkeit ausüben. Der Bund trägt gemäss Artikel 36 Absatz 3 ISG die Kosten dieser Prüfungen. Die Kantone müssen nach Artikel 31 Absatz 1 ISG dem Bund die zuständigen Stellen melden für:

- die Einleitung der Personensicherheitsprüfungen (einleitende Stellen);
- den Entscheid über die Ausübung der sicherheitsempfindlichen Tätigkeit (entscheidende Stellen).

Der Bund wird nach erfolgter Vernehmlassung Kontakt mit den Kantonen aufnehmen, um die entsprechenden Listen der Funktionen zu liefern, welche der Personensicherheitsprüfung unterstellt werden müssen.

2.2.3. IAMV

Mit der Verordnung über die elektronische Übermittlung im Verwaltungsverfahren vom 1. September 2015 (BGS 162.13) verfügt der Kanton Zug über Vorgaben an ein Identitätsverwaltungssystem (ZUGLOGIN). Mit dem Bund wird derzeit die Föderation ZUGLOGIN zum CH-Login bereits realisiert. Über das interne kantonale IAM-System stehen Admin-PKI-Zugänge bei erhöhtem Schutzbedarf auf Bundesanwendungen zur Verfügung.

2.3. Mit welchen finanziellen Auswirkungen rechnen die Kantone

Für die Schulung, die Sicherstellung der Sicherheit des Informatikbetriebs, die Einleitung der Personensicherheitsprüfungen und die Überprüfung der Informatiksicherheit bei den Organen wird beim AIO eine zusätzliche Vollzeitstelle (Informationssicherheits-Spezialist) benötigt.

Zu den finanziellen Auswirkungen, insbesondere zu einem allfälligen personellen Mehraufwand bei den Organen, die klassifizierte Informationen des Bundes bearbeiten oder auf seine

Informatikmittel zugreifen, können derzeit keine Aussagen gemacht werden. Die konkreten Auswirkungen werden sich erst bei bzw. nach der Umsetzung der Verordnungen zeigen

2.4. Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?

Ansprechperson ist der CISO des AIO.

Zug, 15. November 2022

Freundliche Grüsse
Regierungsrat des Kantons Zug

Martin Pfister
Landammann

Tobias Moser
Landschreiber

Versand per E-Mail an:
- sicherheit.vbs@gs-vbs.admin.ch (Word- und PDF-Format)
- Zuger Mitglieder der Bundesversammlung
- Staatskanzlei (info.staatskanzlei@zg.ch, Geschäftskontrolle)
- Datenschutzstelle (datenschutz.zug@zg.ch)
- Sicherheitsdirektion (info.sd@zg.ch)
- Volkswirtschaftsdirektion (info.vds@zg.ch)
- Finanzdirektion (info.fd@zg.ch)
- Amt für Informatik und Organisation (info.aio@zg.ch)
- Personalamt (info.pa@zg.ch)

Kanton Zürich
Regierungsrat

Eidgenössisches Departement
für Verteidigung, Bevölkerungsschutz
und Sport
3003 Bern

9. November 2022 (RRB Nr. 1462/2022)
Ausführungsrecht zum Informationssicherheitsgesetz (Vernehmlassung)

Sehr geehrte Frau Bundesrätin

Mit Schreiben vom 24. August 2022 haben Sie uns eingeladen, zum Ausführungsrecht zum Informationssicherheitsgesetz Stellung zu nehmen und vier konkrete Fragen zu beantworten. Wir danken für diese Gelegenheit und äussern uns wie folgt:

Die Bestrebungen des Bundes im Bereich der Informationssicherheit begrüssen wir. Zu den Verordnungsentwürfen schlagen wir keine Änderungen vor. Ihre Fragen beantworten wir gerne wie folgt:

1. Ist die Umsetzung der Verordnungen für die Kantone verständlich?

Die Verordnungsentwürfe betrachten wir grundsätzlich als verständlich. Sie lassen allerdings noch wesentliche Punkte offen, beispielsweise zur Frage, unter welchen Voraussetzungen die Informationssicherheit bei einem Kanton als «gleichwertig» im Sinne von Art. 3 Abs. 2 des Bundesgesetzes vom 18. Dezember 2020 über die Informationssicherheit beim Bund (ISG) zu betrachten ist. Unklar ist ferner, ob und inwieweit von den Kantonen gemäss Art. 16 Abs. 3 der Verordnung über die Informationssicherheit bei der Bundesverwaltung und bei der Armee (ISV) erwartet wird, nach Bundesrecht Gesuche um Zugang zu Informationen des Bundes zu behandeln.
Eine abschliessende Beurteilung ist deshalb erst möglich, wenn die weiteren Vorgaben gemäss Kapitel 3.8 des erläuternden Berichts vorliegen. Diese sollten wirksam, zweckmässig und wirtschaftlich sein.

2. Wie gedenken die Kantone, die Verordnungen umzusetzen?

Die Umsetzung im Kanton Zürich muss sinnvollerweise darauf ausgerichtet sein, eine mindestens gleichwertige Informationssicherheit im Sinne von Art. 3 Abs. 2 ISG zu gewährleisten. Sie erfolgt nach den Vorgaben von § 7 des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007 (LS 170.4), §§ 12 ff. der Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019 (LS 170.8) und der Allgemeinen Informationssicherheitsrichtlinie des Regierungsrates für die kantonale Verwaltung vom 3. September 2019 (RRB Nr. 795/2019) sowie der gestützt darauf erlassenen Besonderen Informationssicherheitsrichtlinien.
Die Sicherheit beim Betrieb gemäss Art. 30 E-ISV kann das Amt für Informatik schon heute mit dem Cyber Defence Center (CDC) gemäss der kantonalen Cybersicherheitsstrategie vom 4. Mai 2022 (RRB Nr. 676/2022) gewährleisten. Das CDC überprüft die Infrastruktur auch regelmässig auf Schwachstellen und Lücken. Die Sicherheitsakkreditierung von Informatikmitteln gemäss Art. 23 E-ISV erfolgt mit einer Kombination aus Schwachstellenmanagement, Pentesting, Bug-Bounty und einem konzeptionellen Review der Lösung. Bei der Umsetzung der physischen Schutzmassnahmen gemäss Art. 34 E-ISV ist im Kanton Zürich das Immobilienamt federführend. Im Bereich der Personensicherheitsprüfungen wird eine Präzisierung der Rechtsgrundlagen zu prüfen sein.
Die Umsetzung durch die Kantone kann jedoch erst dann abschliessend festgelegt werden, wenn die weiteren Vorgaben gemäss Kapitel 3.8 des erläuternden Berichts vorliegen.

3. Mit welchen finanziellen Auswirkungen rechnen die Kantone?

Grundsätzlich gehen wir davon aus, dass dem Kanton Zürich durch das neue Informationssicherheitsrecht des Bundes Zusatzkosten entstehen. Dies gilt beispielsweise für die Sicherheitsakkreditierung von Informatikmitteln gemäss Art. 23 E-ISV. Die Kosten dafür belaufen sich – abhängig vom Umfang und der Komplexität einer Lösung – jeweils auf ungefähr Fr. 10 000 bis 50 000. Weiter entstehen in diesem Zusammenhang auch Zusatzkosten für die regelmässige Prüfung der Sicherheit während des Lebenszyklus.
Aufgrund der noch offenen Fragen zur Umsetzung des neuen Informationssicherheitsrechts (vgl. Antwort auf Frage 2) können dessen finanzielle Auswirkungen aber noch nicht abschliessend abgeschätzt werden.

4. Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?

Die Bezeichnung einer zentralen Ansprechstelle für Fragen der Informationssicherheit in jedem Kanton erachten wir grundsätzlich als sinnvoll. In der kantonalen Verwaltung Zürich steht den Bundesbehörden dafür grundsätzlich die oder der Informationssicherheitsbeauftragte des Kantons Zürich zur Verfügung. Je nach dem Gegenstand der Anfrage erfordern Auskünfte indessen eine Rücksprache mit den betroffenen kantonalen Organisationseinheiten. Für die tägliche Arbeit ist ausserdem der direkte Austausch zwischen

den «Peer»-Abteilungen von Bund und Kantonen notwendig, da die Themen in den verschiedenen Organisationseinheiten sehr unterschiedlich sind und ein spezifisches Detailwissen erfordern.

Genehmigen Sie, sehr geehrte Frau Bundesrätin,
die Versicherung unserer ausgezeichneten Hochachtung.

Im Namen des Regierungsrates

Der Präsident:

Ernst Stocker

Die Staatsschreiberin:

Dr. Kathrin Arioli

Sozialdemokratische Partei der Schweiz

Zentralsekretariat
Theaterplatz 4
3011 Berne

Tel. 031 329 69 69
Fax 031 329 69 70

info@spschweiz.ch
www.spschweiz.ch

Generalsekretariat VBS
Bundeshaus Ost
3003 Bern
Per Mail an:
sicherheit.vbs@gs-vbs.admin.ch

Bern, 24. November 2022

Stellungnahme zum Ausführungsrecht zum Informationssicherheitsgesetz

Sehr geehrte Frau Bundesrätin Amherd,
sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit zur Stellungnahme, die wir gerne nutzen.

Übersicht und grundsätzliche SP-Haltung

Das Informationssicherheitsgesetz schafft für alle Bundesbehörden einen einheitlichen, formell-gesetzlichen Rahmen für die Informationssicherheit und regelt dabei die wichtigsten Massnahmen zum Schutz ihrer Informationen und Informatikmittel. Gleichzeitig werden die bestehenden rechtlichen und organisatorischen Lücken behoben. Im Hinblick auf die Inkraftsetzung Mitte 2023 hat der Bundesrat die Ausführungsbestimmungen auf Verordnungsstufe erarbeitet und für vier Verordnungen die Vernehmlassung eröffnet

Das Ausführungsrecht zum Informationssicherheitsgesetz (ISG) umfasst drei neue Verordnungen (Informationssicherheitsverordnung, Verordnung über die Personensicherheitsprüfungen, Verordnung über das Betriebssicherheitsverfahren) und die teilrevidierte Verordnung über die Identitätsverwaltungssysteme und Verzeichnisdienste des Bundes.

Die SP Schweiz ist mit den Ausführungsbestimmungen zum Informationssicherheitsgesetz grundsätzlich einverstanden. Die Datenerhebung für die Personensicherheitsüberprüfung geht jedoch viel zu weit und wird von der SP abgelehnt. Insbesondere ist es für die SP inakzeptabel, dass Daten über die Intimsphäre und Sexualität, die religiösen, politischen, gewerkschaftlichen und weltanschaulichen Ansichten oder Tätigkeiten erhoben und bearbeitet werden dürfen.

Personensicherheitsprüfung geht zu weit: Keine ausreichende gesetzliche Grundlage für ausufernde Prüfungskompetenzen

Die Personensicherheitsprüfung dient zur Beurteilung, ob ein Risiko für die Informationssicherheit bestehen könnte, wenn eine Person im Rahmen ihrer Funktion

oder eines Auftrags eine sicherheitsempfindliche Tätigkeit ausübt (Art. 27 Abs. 1 ISG). Zu diesem Zweck werden sicherheitsrelevante Daten über die Lebensführung der zu prüfenden Person, insbesondere über ihre engen persönlichen Beziehungen und familiären Verhältnisse, ihre finanzielle Lage und ihre Beziehung zum Ausland, bearbeitet (Art. 27 Abs. 2 ISG).

Diese Bestimmungen sollen als gesetzliche Grundlage für Art. 19 Abs. 1 der Verordnung über die Personensicherheitsprüfungen (VPSP) sowie deren Anhang 7 dienen. Art. 19 Abs. 1 VPSP hält fest: «Die Fachstellen PSP können die Daten nach Anhang 7 erheben und bearbeiten.» Anhang 7 der VPSP führt aus, welche Daten konkret gemeint sind (kursive Hervorhebungen hinzugefügt):

«1. Daten, die bei allen Prüfstufen bearbeitet werden können:

a. (…)

b. Daten über die Lebensführung der zu prüfenden Person, *insbesondere*:
   1. beruflicher Werdegang
   2. schulischer Werdegang
   3. Werdegang innerhalb der Armee, des Zivilschutzes oder des Zivildienstes
   4. Ausbildungen
   5. Hobbies
   6. Projekte
   7. Angehörigkeit zu Vereinen
   8. ehrenamtliche Tätigkeiten
   9. religiöse Ansichten oder Tätigkeiten
   10. weltanschauliche Ansichten
   11. politische Ansichten oder Tätigkeiten
   12. gewerkschaftliche Ansichten oder Tätigkeiten

c. Daten über enge persönliche Beziehungen und familiäre Verhältnisse der zu prüfenden Person, *insbesondere*:
   1. Zivilstand
   2. Intimsphäre und Sexualität
   3. Verhältnis zur Familie
   4. Identität der Eltern
   5. Freundeskreis

d. Daten über die Beziehung zum Ausland der zu prüfenden Person, *insbesondere*:
   1. Ferien
   2. Sprachaufenthalte

Sozialdemokratische Partei der Schweiz
Theaterplatz 4
Case postale · 3001 Berne
Tel. 031 329 69 69
Fax 031 329 69 70
info@spschweiz.ch
www.spschweiz.ch

3. Geschäftsreisen
4. personelle Beziehungen im Ausland und internationale Kontakte
5. finanzielle Interessen im Ausland

e. Daten über die Gesundheit der zu prüfenden Person, *insbesondere*:
   1. physische und psychische Krankheiten
   2. physische und psychische Behinderungen
   3. Konsum von Betäubungsmittel und Alkohol
   4. Süchte und Abhängigkeiten

f. Finanzdaten der zu prüfenden Person, *insbesondere*:
   1. Bankauszüge
   2. Finanzanlagen
   3. Löhne
   4. Hypotheken
   5. Kredite
   6. Vermögen
   7. Steuern
   8. Schulden
   9. Investitionen

Das geht viel zu weit. Genauso gut hätte man in Anhang 7 der VPSP schreiben können: «Jegliche Daten über die Identität der zu prüfenden Person darf erhoben und bearbeitet werden.» Das ist weder für das Ziel der Gesetzesbestimmung notwendig, noch besteht dafür eine ausreichende gesetzliche Grundlage. Deshalb fordert die SP:

SP-Forderung:
Anhang 7 ist hier aus Platzgründen nicht in voller Länge reproduziert. Zusätzlich zur äusserst ausführlichen Aufzählung, ist das Wort «insbesondere» am Anfang jeder Aufzählung zu beachten. Es soll sich dabei also nicht um eine abschliessende Liste handeln, sondern lediglich um Beispiele. Die SP fordert, dass das Wort «insbesondere» in Anhang 7 VPSP überall ersatzlos gestrichen wird (bei 1a; 1b; 1c; 1d; 1e; 1f; 1g; 1h; 1i; 1j). Bei solch heiklen persönlichen Daten muss die staatliche Kompetenz explizit erwähnt und glasklar definiert sein. Eine nicht abschliessende Liste lehnt die SP ab.

SP-Forderung
Zudem ist es für die SP inakzeptabel, dass Daten über die Intimsphäre und Sexualität, die religiösen, politischen, gewerkschaftlichen und weltanschaulichen Ansichten oder Tätigkeiten erhoben und bearbeitet werden dürfen. Art. 27 ISG stellt zwar

Sozialdemokratische Partei der Schweiz
Theaterplatz 4
Case postale · 3001 Berne
Tel. 031 329 69 69
Fax 031 329 69 70
info@spschweiz.ch
www.spschweiz.ch

tatsächlich eine weitgehende gesetzliche Grundlage dar, kann aber nicht so interpretiert werden, dass schlicht alles über eine zu prüfende Person in Erfahrung gebracht werden kann. Hätte der Gesetzgeber dies gewollt, so wäre das ISG und insbesondere Art. 27 ISG anders formuliert. Er hätte es sich dann nämlich einfacher machen können und schlicht ins Gesetz schreiben können, dass jegliche Information über zu prüfende Personen erhoben und bearbeitet werden könne. Die SP fordert deshalb eine Streichung der Bestimmungen in Anhang 7 VPSP, Abs. 1, lit. b, Ziff. 9, 10, 11, 12 sowie von Anhang 7 VPSP, Abs. 1, lit. c, Ziff. 2.

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

Sozialdemokratische Partei der Schweiz

Mattea Meyer
Co-Präsidentin

Cédric Wermuth
Co-Präsident

Severin Meier
Politischer Fachsekretär

Sozialdemokratische Partei der Schweiz
Theaterplatz 4
Case postale · 3001 Berne
Tel. 031 329 69 69
Fax 031 329 69 70
info@spschweiz.ch
www.spschweiz.ch

Schweizerische Volkspartei
Union Démocratique du Centre
Unione Democratica di Centro
Partida Populara Svizra

Generalsekretariat / Secrétariat général
Postfach, CH-3001 Bern
Tel. +41(0)31 300 58 58, Fax + 41(0)31 300 58 59
gs@svp.ch, www.svp.ch, PC-Kto: 30-8828-5

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz und Sport (VBS)
Bundesrätin Viola Amherd

Elektronisch an:
sicherheit.vbs@gs-vbs.admin.ch

Bern, 11. November 2022

Ausführungsrecht zum Informationssicherheitsgesetz

Vernehmlassungsantwort der Schweizerischen Volkspartei (SVP)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir danken Ihnen für die Einladung, im Rahmen der oben genannten Vernehmlassung Stellung zu nehmen. Wir äussern uns dazu wie folgt:

Aus Sicht der SVP ist das vorliegende Ausführungsrecht zum Informationssicherheitsgesetz grundsätzlich zu begrüssen. Die Kosten für die Umsetzung der Massnahmen und die zusätzlichen Stellenprozente müssen jedoch sofort transparent ausgewiesen werden. Personendaten der höchsten Klassifizierung müssen zwingend in der Schweiz aufbewahrt werden, ebenso ist für den Austausch der Daten der offizielle Dienstweg vorzusehen. Die SVP fordert, dass durch die Massnahmen Kosteneinsparungen und eine Verbesserung des Datenschutzes erzielt werden.

Bei der Beratung des Informationssicherheitsgesetzes im Nationalrat war die SVP-Fraktion hinsichtlich des nicht klar definierten Kostenrahmens sehr kritisch eingestellt und lehnte das neue Gesetz ab. Angesichts dieser erheblichen Unsicherheiten bei den Kosten für Personal und Material bestehen bei der SVP nach wie vor grosse Fragezeichen. Eine transparente Budgetierung für die Umsetzung der vorgesehenen Massnahmen muss schnellstmöglich erstellt und veröffentlicht werden. Der effizienten und reibungslosen Umsetzung der Vorhaben ist angesichts der angespannten Finanzlage des Bundes höchste Priorität einzuräumen.

Im erläuternden Bericht ist von einem «moderaten, einmaligen Initialaufwand von etwa 0.5 Vollzeitstellen im Schnitt» für das «ISMS light» die Rede. Zudem ist für den minimalen Betrieb in den Ämtern ein Zusatzaufwand von 0.2 Vollzeitstellen vorgesehen. Der Aufwand für die Akkreditierung der Informatikmittel kann noch nicht beziffert werden. Weiter kommt auf die Informationssicherheitsbeauftragten aller Departemente ein erhöhter Aufwand von 0.2 Vollzeitstellen zu. Detaillierte Angaben zum Aufwand für die Personensicherheitsprüfung liegen erst nach der Vernehmlassung vor. Ebenfalls sind die Kosten für die Kantone bei der Umsetzung noch nicht bekannt. Diese Aufstellungen sind unbefriedigend.

Die Vereinheitlichung des Informationssicherheits-Managementsystems bei allen Verwaltungseinheiten im Rahmen der neuen Informationssicherheitsverordnung ist zu begrüssen. Die SVP erhofft sich durch dieses Zentralisierung Kosteneinsparungen und einen effizienten Betrieb und Unterhalt. In allen Ämtern ist deshalb möglichst schnell das gleiche ISMS-System einzuführen.

Bei der Verordnung über die Personensicherheitsprüfungen ist die Reduktion der Prüffälle von Mindestens 30 Prozent positiv hervorzuheben. Ebenfalls nachzuvollziehen ist die damit verbundene Ersetzung älterer Verordnungen, die aufgrund des raschen technologischen Wandels überholt sind.

Die Verordnung über das Betriebssicherheitsverfahren ist absolut nötig. Es ist richtig, dass Betriebe, welche sicherheitsempfindliche Aufträge für den Bund ausführen, zuvor auf ihre Vertrauenswürdigkeit überprüft werden. Die SVP verspricht sich damit eine Erhöhung des Datenschutzes bei sicherheitsempfindlichen Informationen. Die Ersetzung der Geheimschutzverordnung von 1990 ist überfällig.

Die Verordnung über Identitätsverwaltungs-Systeme und die damit Verbundene Ausdehnung des Geltungsbereiches auf die Verwaltungseinheiten der dezentralen Bundesverwaltung ist hinsichtlich einer effektiveren Personenprüfung zu begrüssen. Die Auswirkungen auf den Datenschutz, insbesondere durch die erweiterte Bearbeitung biometrischer Daten, sind kritisch zu begleiten.

Der mit dem neuen Informationssicherheitsgesetz stark verbesserte Rechtsvergleich mit anderen Ländern ist für eine bessere internationale Zusammenarbeit im Bereich der Informationssicherheit zu begrüssen. Die von der Schweizerischen Eidgenossenschaft aufgenommenen und gespeicherten Personendaten müssen jedoch mindestens in der Kategorie der höchsten Klassifizierung zwingend in der Schweiz gelagert werden. Schliesslich ist für den Austausch der Daten zwingend der offizielle Dienstweg vorzusehen.

Wir danken Ihnen für die Berücksichtigung unserer Stellungnahme.

Freundliche Grüsse

SCHWEIZERISCHE VOLKSPARTEI

Der Parteipräsident	Der Generalsekretär
	
Marco Chiesa	Peter Keller
Ständerat	Nationalrat

Bundesrätin Viola Amherd
Eidg. Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundeshaus Ost
CH-3003 Bern

Einreichung per Mail an:
sicherheit.vbs@gs-vbs.admin.ch

Bern, 24. November 2022

Stellungnahme zum Ausführungsrecht zum neuen Informationssicherheitsgesetz (ISG)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Wir nehmen Bezug auf die am 24. August 2022 eröffnete Vernehmlassung zu der teilrevidierten sowie den drei neuen Verordnungen zum Informationssicherheitsgesetz (ISG) und übermitteln Ihnen fristgerecht die Einschätzung des Schweizerischen Verbandes der Telekommunikation (asut).

Die Telekommunikations-Branche begrüsst einen robusten regulatorischen Rahmen für die Informationssicherheit, der dem aktuellen Stand der Technologie und damit zusammenhängenden Risikoszenarien entspricht. Die Verordnungen beinhalten das richtige Mass an Flexibilität und Genauigkeit, um auch bei neuen technologischen Entwicklungen die Verantwortlichkeiten aller Beteiligten klar auszuweisen. Ebenso begrüssen wir den Ansatz der Bundesverwaltung künftig weniger zu klassifizieren und somit, wo möglich, zu entbürokratisieren.

Aus dem erläuternden Bericht «Ausführungsrecht zum Informationssicherheitsgesetz» geht hervor, dass vor dem Inkrafttreten des ISG und den Verordnungen Mitte 2023 noch eine Reihe von Vorgaben erarbeitet oder aktualisiert werden müssen. Im gleichen Bericht wird ferner angekündigt, dass «die detaillierten Vorgaben, einschliesslich der derzeit fehlenden technischen Anforderungen an die elektronische Bearbeitung von klassifizierten Informationen […] voraussichtlich bis Ende 2023 erarbeitet» werden. Dies stellt eine Überschneidung mit dem geplanten Inkrafttreten des ISG dar.

Aus unserer Sicht kann diese zeitliche Überschneidung dazu führen, dass Vorgaben und Anforderungen erst kurz vor oder sogar deutlich nach Inkrafttreten veröffentlicht werden. Obwohl es Übergangsfristen geben wird, ist es für die betroffenen Firmen wichtig, dass solche essenziellen Informationen so früh wie möglich bekannt gegeben werden, da es uns ein wichtiges Anliegen ist, die Informationssicherheit jederzeit vollumfänglich zu gewährleisten. Weiter führt das ISG für die betroffenen Firmen zu Mehraufwand. Entsprechend ist es entscheidend, dass die noch auszuarbeitenden Vorgaben und Anforderungen möglichst praxisnah und unbürokratisch umsetzbar sind.

asut
Schweizerischer Verband der Telekommunikation
Hirschengraben 8
3011 Bern

+41 (0)31 560 66 66
info@asut.ch
www.asut.ch

@asut_ch

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse
asut – Schweizerischer Verband der Telekommunikation

Peter Grütter, Präsident

Bundesanwaltschaft
Ministère public de la Confédération
Ministero pubblico della Confederazione
Procura publica federala

CH-3003 Bern, BA

Per E-Mail an
sicherheit.vbs@gs-vbs.admin.ch

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Frau Bundesrätin Viola Amherd
Bundeshaus Ost
3a003 Bern

Referenz: RD.22.0034
Bern, 24. November 2022

Ausführungsrecht zum Informationssicherheitsgesetz; Vernehmlassung 2022/49 Vernehmlassung der Bundesanwaltschaft (BA)

Sehr geehrte Frau Bundesrätin
Sehr geehrte Damen und Herren

Mit Bezugnahme auf Ihre Einladung zur Vernehmlassung vom 24. August 2022 nimmt die BA als fachlich und organisatorisch von Bundesrat und Bundesverwaltung unabhängige Behörde Stellung zu Aspekten der Vorlage, welche sie betreffen.

Zu den folgenden Bestimmungen der Vorlage äussert sich die BA wie folgt:

4. Abschnitt: Prüfstufen

Art. 10 und Art. 11 VPSP

Die BA ist die Strafverfolgungsbehörde des Bundes. Zu ihrer Aufgabenerfüllung gehören namentlich die Führung von Strafverfahren im Bereich des repressiven Staatsschutzes (z.B. verbotener Nachrichtendienst), die Verfolgung komplexer internationaler Schwerstkriminalität (z.B. kriminelle Organisationen und Terrorismus) und die Führung von Rechtshilfeverfahren. Aufgrund ihrer sicherheitsempfindlichen Tätigkeiten ist es für die BA daher essentiell, dass sie ihre Mitarbeitenden einer stufengerechten und wirksa-

Bundesanwaltschaft
Nicole Vontobel
Guisanplatz 1
3003 Bern
www.bundesanwaltschaft.ch

men Personensicherheitsprüfung unterziehen lassen kann, wozu nebst einer Grundsicherheitsprüfung auch die Möglichkeit einer erweiterten Personensicherheitsprüfung gehört.

Vor diesem Hintergrund ist es notwendig, ausdrückliche Grundlagen in der VPSP vorzusehen, gestützt auf welche die BA als verpflichtete Behörde stufengerechte Personensicherheitsprüfungen anordnen kann (Art. 30 ISG).

Im Vernehmlassungsentwurf zu den Art. 10 und 11 VE-VPSP fehlen solche ausdrücklichen Grundlagen. Um Unklarheiten oder gar Lücken in der Rechtsanwendung zu vermeiden, schlagen wir nachfolgende Ergänzungen in Art. 11 VE-VPSP vor:

Art. 11 Prüfung der Vertrauenswürdigkeit nach dem BPG

1 Einer Grundsicherheitsprüfung sind folgende Tätigkeiten nach Artikel 20*b* BPG zugeordnet:

a. hoheitliche Tätigkeiten von im Ausland eingesetzten Angestellten des Bundes und von versetzungspflichtigen Angestellten des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA);
b. Tätigkeiten nach Artikel 20*b* Absatz 1 Buchstabe b BPG, bei deren ungetreuer Ausführung ein Schaden von fünfzig Millionen bis fünfhundert Millionen Franken entstehen kann;
c. Tätigkeiten im Rahmen von Strafverfolgungs- oder polizeilichen Aufgaben:
   1. in Bezug auf die operativen Mittel und Methoden zur Bekämpfung von Verbrechen oder Vergehen,
   2. in Bezug auf die Identität exponierter Personen,
   3. von Personal des Bundesamts für Polizei (fedpol) und des Bundesamts für Justiz,
   4. von internem und externem Personal der Bundesanwaltschaft;
d. Tätigkeiten, die von Personen ausgeübt werden, die einer Departementsvorsteherin oder einem Departementsvorsteher oder der Bundeskanzlerin oder dem Bundeskanzler direkt unterstellt sind oder die zu ihrem oder seinem engsten Stab gehören.

2 Einer erweiterten Personensicherheitsprüfung sind folgende Tätigkeiten nach Artikel 20*b* BPG zugeordnet:

a. Tätigkeiten von Funktionen, für die nach Artikel 2 Absatz 1 der Bundespersonalverordnung vom 3. Juli 2001[12] (BPV) der Bundesrat für die Begründung, Änderung und Beendigung des Arbeitsverhältnisses zuständig ist;
b. Tätigkeiten im Rahmen von Arbeitsverhältnissen, für deren Begründung, Änderung und Beendigung nach Artikel 2 Absatz 1[bis] BPV die Departementsvorsteherin oder der Departementsvorsteher oder der Bundeskanzlerin oder dem Bundeskanzler zuständig ist;
c. Tätigkeiten von Leiterinnen und Leitern von dezentralisierten Verwaltungseinheiten nach Artikel 2 Absatz 1 Buchstabe e BPG;
d. Tätigkeiten nach Artikel 20*b* Absatz 1 Buchstabe b BPG, bei deren ungetreuen Ausführung ein Schaden von über fünfhundert Millionen Schweizer Franken entstehen kann;
e. Tätigkeiten der Angestellten der Fachstellen PSP.
f. Tätigkeiten von Angestellten der Bundesanwaltschaft, bei deren vorschriftswidriger oder unsachgemässer Ausübung die Interessen des Bundes schwerwiegend beeinträchtigt werden können.

Die vorgeschlagene Ergänzung der neuen Ziff. 4 in Art. 11 Abs. 1 Bst. c erfolgt in Nachachtung von Art. 30 Bst. a ISG und Art. 20b Abs. 1 lit. c E-BPG (Risiko einer *erheblichen* Beeinträchtigung resp. Gefährdung).

Die vorgeschlagene Ergänzung eines neuen Bst. f in Art. 11 Abs. 2 erfolgt in Umsetzung von Art. 30 Bst. b ISG (Risiko einer *schwerwiegenden* Beeinträchtigung).

Die BA bedankt sich für die Berücksichtigung der vorliegenden Vernehmlassung. Weiter danken wir Ihnen, dass die BA bei allfälligen weiteren Ämterkonsultationen im vorliegenden Rechtssetzungsprojekt berücksichtigt wird.

Freundliche Grüsse

Bundesanwaltschaft BA

Jacques Rayroud
Stv. Bundesanwalt

Eidgenössisches Departement für
Verteidigung, Bevölkerungsschutz und Sport (VBS)
Frau Bundesrätin Viola Amherd
Bundeshaus Ost
3003 Bern

Bern, 2. Dezember 2022

Stellungnahme im Vernehmlassungsverfahren:
Ausführungsrecht zum Informationsgesetz

Sehr geehrter Frau Bundesrätin Amherd
Sehr geehrte Damen und Herren

Im Namen der unterzeichnenden Gewerkschaften und Berufsverbände erlauben wir uns, trotz der bereits verstrichenen Vernehmlassungsfrist, in einer Frage nachträglich noch Stellung zu beziehen. Wir wären Ihnen verbunden, wenn Sie unsere Anmerkungen trotzdem noch berücksichtigen würden.

Gewerkschaftlich und für das Personal relevante Fragen finden sich insbesondere in der Verordnung über die Personensicherheitsprüfungen (VPSP) unter Art. 19 Datenerhebung, welcher auf den neuen Anhang 7 verweist. Dazu mangelte es in der Vernehmlassung etwas an Transparenz, denn dieser neue Anhang wurde in den Erläuterungen zum entsprechenden Artikel nicht erwähnt.

Während in der alten Version der Verordnung über die Personensicherheitsprüfungen (VPSP) der Art. 19 Abs. 2 Datenerhebung keine klar definierten zu prüfenden Daten festlegt, schreibt der Abs. 1 im revidierten VPSP über den dort aufgeführten neuen Anhang 7 sehr klar definierte, zu prüfende Daten explizit fest (ohne – was noch dazu kommt –, dass es sich bei dieser ausführlichen Liste um eine abschliessende Liste handeln würde). Darunter wurden unter anderem folgende Datenpunkte aufgenommen:

- weltanschauliche Ansichten
- politische Ansichten oder Tätigkeiten
- gewerkschaftliche Ansichten oder Tätigkeiten
- Intimsphäre und Sexualität

Auch wenn diese sowie viele weitere Datenpunkte gemäss erläuternden Ausführungen bereits heute – ohne explizite Erwähnung im Ausführungsrecht – abgefragt werden können und situationsbezogen auch werden, ist die neue, sehr ausführliche Liste sehr befremdlich. Es werden dabei Kriterien erwähnt, welche äusserst stark in die Privat- und Intimsphäre der betroffenen Personen fallen und entsprechendes Missbrauchs- und Diskriminierungspotenzial bergen. Als Personalverbände und Gewerkschaften sehen wir zum Beispiel nicht ein, wie sich eine gewerkschaftliche Mitgliedschaft auf das Sicherheitsrisiko auswirken könnte, wie dies sicher auch für andere Datenpunkte gilt. Wir

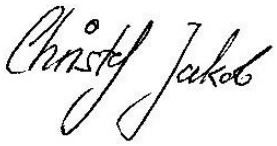
möchten Sie daher bitten, diese Liste, beziehungsweise den ihr zugrunde liegenden Ansatz der Personensicherheitsüberprüfungen grundsätzlich zu überarbeiten und das Ausführungsrecht entsprechend anzupassen, respektive die Anwendung und den Umgang mit den stark auf die Privat- und Intimsphäre zielenden Datenpunkte, nur bei Funktionen mit entsprechend sehr hohem Risiko im Umgang mit sensiblen Daten, einzuschränken.

Für die Berücksichtigung unserer Stellungnahme danken wir Ihnen im Voraus.

Freundliche Grüsse

IG Bundespersonal

Jérôme Hayoz
Generalsekretär PVB



Christof Jakob,
Gewerkschaftssekretär VPOD

Heidi Rebsamen
Zentralsekretärin Garanto

Matthias Humbel
Leiter öffentliche
Verwaltung transfair

Beat Grossrieder
Zentralsekretär swisspersona

Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Per Email
sicherheit.vbs@gs-vbs.admin.ch

Bern, 24. November 2022 sgv-Sc

Vernehmlassungsantwort
Ausführungsrecht zum Informationssicherheitsgesetz

Sehr geehrte Damen und Herren

Als grösste Dachorganisation der Schweizer Wirtschaft vertritt der Schweizerische Gewerbeverband sgv über 230 Verbände und gegen 600 000 KMU, was einem Anteil von 99,8 Prozent aller Unternehmen in unserem Land entspricht. Im Interesse der Schweizer KMU setzt sich der grösste Dachverband der Schweizer Wirtschaft für optimale wirtschaftliche und politische Rahmenbedingungen sowie für ein unternehmensfreundliches Umfeld ein.

Der sgv lehnt die gesamte Vorlage ab. Sie geht weit über die gesetzliche Grundlage hinaus und unterlässt, die von ihr generierten Kosten zu quantifizieren. Man könnte sogar den Eindruck erhalten, die Vorlage verzichte bewusst auf die Quantifizierung der Kosten, um ihre weitgehenden und granularen Regulierungsanliegen durchzusetzen. Ohne die klaren und transparenten Angaben der Kosten ist eine Bewertung des vorliegenden Entwurfs unmöglich. Entsprechend lehnt der grösste Dachverband der Schweizer Wirtschaft diese eklatant-mangelhaft aufbereitete Vorlage ab.

Zwei Elemente zeigen, wie einerseits lückenhaft die Vorlage aufbereitet wurde und andererseits, wie granular-intrusiv sie ausfällt und damit die gesetzliche Grundlage verletzt:

Erstens: Mit dem Betriebssicherheitsverfahren wird ein Sonderbeschaffungsrecht begründet. Schon seine Einführung mit dem ISG lehnte der sgv ab; seine Umsetzung über den Verordnungsweg fällt indes noch regulierungsintensiver aus als im Gesetz vorgesehen. Die erläuternden Materialien machen indes keine Angaben zu den damit verbundenen Regulierungskosten. Auch die Zusatzkosten für die Kantone, welche sich aus der Umsetzung des gesamten Ausführungsrechts ergeben, werden nicht quantifiziert.

Zweitens: Die Verordnung über die Personensicherheitsüberprüfungen geht entschieden zu weit. Es ist nicht ersichtlich, weshalb bei der Grundsicherheitsprüfung festgelegt werden darf, dass Angaben zu religiösen Tätigkeiten, weltanschaulichen Ansichten sowie über politische und gewerkschaftliche Tätigkeiten umfassend einverlangt und bearbeitet werden dürfen. Ebenso finde sich keine Rechtsgrundlage für Datenerhebungen zur Intimsphäre und Sexualität, zum Familienverhältnis, zur Identität der Eltern und zum Freundeskreis.

Freundliche Grüsse

Schweizerischer Gewerbeverband sgv

Hans-Ulrich Bigler
Direktor

Henrique Schneider
stellvertretender Direktor

swissgrid

Swissgrid AG
Bleichemattstrasse 31
Postfach
5001 Aarau
Schweiz

T +41 58 580 21 11
info@swissgrid.ch
www.swissgrid.ch

Ihr Kontakt
Michael Rudolf
T direkt +41 58 580 35 15
michael.rudolf@swissgrid.ch

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Per E-Mail an: sicherheit.vbs@gs-vbs.admin.ch

9. November 2022

Swissgrid Stellungnahme zum Ausführungsrecht Informationssicherheitsgesetz - Personensicherheitsprüfungen

Sehr geehrte Damen und Herren

Wir danken Ihnen für die Möglichkeit zur Stellungnahme zum Ausführungsrecht Informationssicherheit. Als nationale Netzgesellschaft ist Swissgrid direkt von der «Verordnung über die Personensicherheitsprüfungen (VPSP)» betroffen. Gerne äussern wir uns nachfolgend zu den Inhalten des Verordnungsentwurfs. Diesbezüglich danken wir Ihnen für den bisherigen Einbezug von Swissgrid.

Art. 2 Geltungsbereich

Antrag:

> Diese Verordnung gilt unter Vorbehalt von Artikel 84 Absatz 3 ISG und Artikel 2 Absätze 2–5 der Informationssicherheitsverordnung vom …[9] für die verpflichteten Behörden und Organisationen nach Artikel 2 ISG **sowie Art. 20a StromVG**.

Begründung: Die im Bundesgesetz über die Informationssicherheit (ISG) vorgesehene Fremdänderung im Art. 20a StromVG stellt eine eigenständige gesetzliche Grundlage dar, auf welche sich die VPSP nebst anderem stützt. Der hierin vorgesehene Geltungsbereich ist formal in Art. 2 VPSP abzubilden.

Art. 3 Zuordnung

Antrag:

> 3 Für Funktionen nach Artikel 20a Absatz 1 StromVG gilt die Funktionenliste nach Anhang 6. **Anstelle des Departements ist die Elektrizitätskommission nach Art 21 StromVG zuständige Behörde für Anträge gemäss Artikel 4, Aktualitätsprüfungen gemäss Artikel 6 und Anträge auf ausserordentliche Prüfungen gemäss Artikel 7.**

Begründung: Gemäss Entwurf der Verordnung haben Änderungen, Ergänzungen und Aktualitätsprüfungen von Funktionenlisten sowie ausserordentliche Prüfungen über das zuständige Departement zu erfolgen (Art. 4, Art. 6 und Art. 7 VPSP). Darunter fällt gemäss dem Verordnungsentwurf auch die Funktionenliste der nationalen Netzgesellschaft bzw. der Anhang 6. Aus Sicht Swissgrid ist jedoch nicht eindeutig, welches Departement für Swissgrid zuständig wäre. Swissgrid ist im Sinne von Art. 2 Abs. 5 ISG als «*Organisation des öffentlichen und privaten Rechts, die kritische Infrastrukturen betreiben*» zu betrachten. Sie ist weder Teil der zentralen noch dezentralen Bundesverwaltung.

Aus «thematischer» Sicht wäre allenfalls das UVEK zuständiges Departement. Das UVEK hat nach Gesetz jedoch keine umfassende Aufsichtsfunktion über die Swissgrid. Swissgrid ist eine privatrechtliche Aktiengesellschaft und hinsichtlich der Erfüllung ihres Auftrages nach StromVG der Aufsicht der ElCom unterstellt. Die ElCom ist als die unabhängige staatliche Regulierungsbehörde im Elektrizitätsbereich zuständig für die Überwachung der Einhaltung des Stromversorgungsgesetzes (somit inkl. der Prüfungen der Vertrauenswürdigkeit nach Art. 20a StromVG). Swissgrid beantragt deshalb eine Anpassung der VPSP, wonach für die nationale Netzgesellschaft die ElCom für die gemäss Art. 4, Art. 6 und Art. 7 vorgesehenen Aufgaben zuständige Behörde ist.

Art. 5 Veröffentlichung, Aufbewahrung und Bekanntgabe

Die Funktionenliste von Swissgrid ist ein vertrauliches Dokument. Anhand der Funktionenliste könnten mit geringem Aufwand Personen in kritischen Funktionen identifiziert werden. Swissgrid begrüsst es, dass die Funktionenliste gemäss Art. 5 Abs. 1 nicht in der Amtlichen Sammlung publiziert wird. Zum Schutz von Swissgrid und ihrer Mitarbeitenden ist der Zugriff auf die Funktionenliste strikt auf das notwendige Mindestmass zu reduzieren.

Art. 14 Prüfungen der Vertrauenswürdigkeit nach dem StromVG

Swissgrid ist mit dem Wortlaut von Art. 14 Abs. 1 und 2 einverstanden. Wir danken Ihnen für die Berücksichtigung der entsprechenden Eingaben seitens Swissgrid.

Art. 15 Einleitende und entscheidende Stelle

Swissgrid begrüsst die in Abs. 4 enthaltene Bestimmung, wonach für Prüfungen der Vertrauenswürdigkeit nach Artikel 20a StromVG die nationale Netzgesellschaft einleitende und entscheidende Stelle ist.

Art. 19 Datenerhebung

Antrag:

2 Eine Befragung nach Artikel 34 Absatz 2 Buchstaben d ISG wird durchgeführt, wenn:

c. die zu prüfende Person bei einer der folgenden Stellen eine Funktion ausübt oder dafür vorgesehen ist:

8. die nationale Netzgesellschaft

Begründung: Als nationale Netzgesellschaft verantwortet Swissgrid den Betrieb des Übertragungsnetzes als wesentliche Grundlage für die sichere Versorgung der Schweiz (Art. 20 StromVG). Das Übertragungsnetz bzw. die Stromversorgung ist die kritischste Infrastruktur der Schweiz[1]. Der Schutz dieser Infrastruktur inklusive dem Schutz vor möglichen Innentätern ist von essenzieller Bedeutung.

Die Erfahrungen von Swissgrid mit Personensicherheitsprüfungen auf privatrechtlicher Basis zeigen, dass die Befragungen zu Erkenntnissen führen können, welche über das «Aktenstudium» alleine nicht zu erreichen sind (bspw. zu psychischen Belastungen). Swissgrid beantragt, dass als Teil einer erweiterten Personensicherheitsprüfung gemäss Art. 14 Abs. 2 VPSP eine Befragung nach Art. 34 Abs. 2 ISG durchgeführt wird.

Art. 38 Übergangsbestimmungen

Antrag:

4 Sicherheitsprüfungen, die die nationale Netzgesellschaft vor **und bis ein Jahr nach** Inkrafttreten dieser Verordnung ~~und vor Ablauf der Frist nach Absatz 5 auf privatrechtlicher~~

[1] Vgl. u.a. Bericht des Bundesamtes für Bevölkerungsschutz BABS (2020) «Katastrophen und Notlagen Schweiz 2020, Bericht zur nationalen Risikoanalyse».

~~Basis~~ erhalten hat, bleiben im Rahmen der Wiederholungsfristen nach den Artikeln 26 und 27 wie folgt verwendbar:

a. Sicherheitsprüfungen für kritische Funktionen: als Grundsicherheitsprüfung nach dieser Verordnung;

b. Sicherheitsprüfungen für höchst kritische Funktionen: als erweiterte Personensicherheitsprüfung nach dieser Verordnung.

~~5 Die nationale Netzgesellschaft ist berechtigt, bis ein Jahr nach Inkrafttreten dieser Verordnung Prüfungen der Vertrauenswürdigkeit nach Artikel 20a StromVG auf privatrechtlicher Basis durchführen zu lassen.~~

Begründung: Die Auslegung von Art. 38 Abs. 5 ist aus unserer Sicht nicht eindeutig. Nach unserem Verständnis bringt die Formulierung in Abs. 5 zum Ausdruck, dass Prüfungen, welche auf privatrechtlicher Basis bis ein Jahr nach Inkrafttreten der Verordnung durchgeführt wurden, im Hinblick auf die Wiederholungsfristen verwendbar sind (vgl. Absatz 4).

Nicht gemeint (aus dem Wortlaut aber interpretierbar) ist, dass es der Swissgrid nach Ablauf der Übergangsfrist rechtlich untersagt wäre, Prüfungen auf privatrechtlicher Basis durchzuführen. Ein solches Verbot wäre aus unserer Sicht weder erforderlich noch zielführend. Der Swissgrid steht es offen, in entsprechenden Situationen ggf. eigene Abklärungen durchzuführen (bspw., wenn der Prüfstelle keine hinreichende Datenbasis verfügbar ist, oder als Teil einer Vor-Selektion von Bewerbenden). Wir beantragen deshalb eine Anpassung von Abs. 4 und Streichung von Abs. 5.

Anhang 6

Swissgrid ist mit dem Aufbau von Anhang 6 einverstanden. Wir weisen darauf hin, dass Funktionen bei Swissgrid (sowohl von Angestellten als auch von Dienstleistern) nicht primär anhand ihrer Zugangsberechtigungen zu Informationen, Applikationen und Infrastrukturen festgelegt werden. Zudem können die Anforderungen an Zugangsberechtigungen teilweise rasch ändern. Die Funktionen bei Swissgrid sind deshalb bewusst relativ breit formuliert.

Ein «System Engineer» als Beispiel ist zuständig für das Konzipieren, das Engineering und für den zuverlässigen, sicheren Betrieb der IT-Infrastruktur in seinem / ihrem Tätigkeitsumfeld. Die Beurteilung der erforderlichen Prüfstufe erfolgt auf Basis einer Einzelfallbetrachtung der konkreten Verantwortlichkeiten, bzw. der IT-Infrastruktur, für welche die Person zuständig ist. Für das Befüllen von Anhang 6 schlagen wir deshalb eine weitergehende Differenzierung vor, bspw.:

- System Engineer, Typ 1 – Keine Prüfung
- System Engineer, Typ 2 – Grundsicherheitsprüfung gemäss Art. 14 Abs. 1

- System Engineer, Typ 3 – Erweiterte Personensicherheitsprüfung gemäss Art. 14 Abs. 2

Von den weiteren Verordnungen ist Swissgrid nicht direkt betroffen, weshalb wir auf eine Stellungnahme verzichten.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und stehen Ihnen bei Fragen gerne zur Verfügung.

Freundliche Grüsse
Swissgrid AG

Yves Zumwald
CEO

Michael Schmid
Head of Legal, Regulatory & Compliance

Xavier Dufour MLaw
Adresse professionnelle
Institut de droit pénal et de criminologie
Université de Berne
Schanzeneckstrasse 1
3001 Berne

Département fédéral de la défense,
de la protection de la population et des sports
Secrétariat général
c/o Christophe Perron
Palais fédéral Est
3003 Berne

Berne, le 24 novembre 2022

Procédure de consultation du droit d'exécution de la loi sur la sécurité de l'information

Madame la Conseillère fédérale Amherd

Je me permets de vous communiquer les remarques suivantes relatives au projet de droit d'exécution de la loi fédérale sur la sécurité de l'information actuellement en consultation.

Remarques générales

L'actuelle prise de position se limite à l'ordonnance sur la sécurité de l'information au sein de l'administration fédérale et de l'armée (OSI) et l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP).

Au niveau de la légistique, les quatre ordonnances sont rédigées de manière très détaillée. Ce niveau de détail représente une entrave à la bonne connaissance et la bonne compréhension de toutes les ordonnances pour le personnel de la Confédération, en particulier pour les collaborateurs sans formation juridique. Ce risque de mécompréhension peut entraver l'action de l'État, voir, dans certains cas, avoir pour conséquence pour des autorités administratives d'agir de manière inappropriée. Il est questionnable si certains articles pourraient être simplifiés pour la version finale des ordonnances.

Différents éléments proposés dans la future OCSP ne semblent pas disposer des prérogatives nécessaires dans la LSI[1]. Comme, selon l'art. 36 al. 1 Cst[2] les restrictions graves aux droits fondamentaux doivent être prévues par **une loi,** certains éléments proposés de l'annexe 7 OCSP ne disposent pas des bases légales suffisantes pour être intégrés dans une ordonnance.

---

[1] Loi fédérale sur la sécurité de l'information au sein de la Confédération (LSI), du 18 décembre 2020, RS 128.
[2] Constitution fédérale de la Confédération suisse (Cst), du 18 avril 1999, RS 101.

Ordonnance sur la sécurité de l'information au sein de l'administration fédérale et de l'armée (OSI)

Art. 22 al. 1 OSI

Le chef du Renseignement militaire (RM) et du Service pour la protection préventive de l'armée (SPPA) a été omis dans la liste des personnes autorisées à « fixer des directives spécifiques à l'engagement ou à l'opération visant à simplifier le traitement ». Il convient d'ajouter le chef RM & SPPA à cette liste, car il est responsable pour de très nombreuses informations classifiées, parfois non-autorisées d'accès au chef de l'armée ou au chef du commandement des Opérations. De plus, il convient de laisser au RM et au SPPA suffisamment de marge de manœuvre pour le traitement et l'échange d'informations dans le cadre d'engagements ou d'opérations.

Proposition : modifier l'art. 22 al. 1 OSI comme suit :

e. le chef RM & SPPA ;
f. le directeur de l'Office fédéral de la douane et[3] de la sécurité des frontières.

Art. 35 OSI

Comme proposé actuellement, les zones de sécurité se limitent uniquement aux locaux et espaces dans lesquels des informations classifiées sont fréquemment traitées. Cette conception ne prend pas suffisamment en considération les possibilités d'espionnage offertes par le niveau technologique actuel. Il est par exemple possible d'utiliser des lasers comme microphones. Le rayon laser pouvant mesurer de manière suffisamment précise les vibrations sur une vitre pour écouter la conversation se déroulant dans la salle. Les « IMSI-catcher » permettent d'écouter les conversations téléphoniques par antennes-relais dans un périmètre de plusieurs centaines de mètres. Des boxes WiFi modifiées (p. ex. « WiFi Pineapple ») permettent de créer un faux réseau WiFi, lequel se fait passer pour le réseau officiel dans un périmètre d'une centaine de mètres. Les ordinateurs se connectant automatiquement au réseau normal créent une connexion automatique sur le faux réseau sans que l'utilisateur ne puisse s'en rendre compte. Ceci permet d'obtenir les informations traitées sur ce faux réseau, voire d'y pirater les ordinateurs connectés. Il en va de même avec les capacités de prise de vue et d'images disponibles à moindre prix sur internet, etc. Face à ces nouvelles technologies, lesquelles permettent à une personne malintentionnée d'obtenir des informations classifiées à plusieurs centaines de mètres de distance, les zones avoisinant la zone de sécurité doivent être inclues dans le dispositif de sécurité. Pour ce faire, il faut offrir aux unités administratives responsables (respectivement aux organes de police) la possibilité d'effectuer des contrôles d'objets et de personnes dans un rayon suffisamment large, en particulier lorsque les zones de sécurité sont en lien avec des objets militaires.

Proposition : Inclure un nouvel article 36 OSI en lien avec le périmètre des zones de sécurité. Il est probable que les bases légales actuelles (lois) ne permettent pas encore d'inclure totalement de possibles fouilles et contrôle d'objets et de personnes dans l'OSI. Si tel devait être le cas, un projet de modification de la loi en ce sens conviendrait d'être initié. Au niveau de l'ordonnance, il est aujourd'hui possible, sans bases légales supplémentaires, de préciser dans ce nouvel article 36 OSI que les autorités compétentes peuvent effectuer des contrôles accrus de l'utilisation malveillante des ondes électro-magnétiques aux alentours des zones de sécurité. Cette inclusion permettra, après adoption de la base légale souhaitée, de préciser les mesures et contre-mesures applicables aux alentours des zones de sécurité en gardant l'unité de structure de la nouvelle OSI.

---

[3] Le « et » a été oublié dans le projet d'ordonnance.

Art. 44 OSI

Il semble que la loi ne prévoit pas de manière suffisamment explicite cet échange de données. Il convient de s'assurer que le Parlement a délégué de manière suffisamment claire la compétence de réglementer cet échange au niveau de l'ordonnance. Les organes autorisés à effectuer ces échanges entre eux disposent de cadres légaux en matière de traitement des informations pouvant fortement varier. Dans tous les cas, si cet échange devait être légitimé au niveau de l'ordonnance, il est absolument nécessaire de préciser l'article pour indiquer que les organes mentionnés ne peuvent seulement recevoir et traiter des informations qu'ils sont habilités à traiter au niveau de leur contenu. Par exemple, les organes de l'armée ne doivent pas pouvoir recevoir des informations en lien avec les activités religieuses, philosophiques, politiques, syndicales (cf. art. 10 LSIA[4]), car l'interdiction de la LSIA est absolue[5]. Dans certains cas, d'autres organes de la Confédération (SRC, fedpol) sont sur le principe autorisés à traiter de tels informations en lien avec des activités protégées constitutionnellement du moment qu'elles sont en lien direct avec l'incident.

Proposition : Démontrer qu'une loi autorise le Conseil fédéral à prévoir cet échange au niveau de l'ordonnance. Si c'est le cas préciser l'article comme indiqué.

Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP)

Cette ordonnance est extrêmement problématique au regard des droits fondamentaux et des droits constitutionnels, elle ne peut pas être publiée en l'état. Il convient de revoir totalement différents aspects de l'ordonnance et d'assurer la légalité de son contenu en mandatant un spécialiste du droit public, en particulier des droits fondamentaux.

Art. 19 OCSP

Cet article est beaucoup trop long, effroyablement mal formulé et insipide au regard de son lien avec « l'annexe 7 ». En terme de légistique, un tel article n'est pas digne de la qualité rédactionnelle des lois et ordonnances du droit suisse. Il convient de couper cet article en 5-6 articles plus petits et d'assurer la légalité des données collectées selon l'annexe 7.

Art. 30 OCSP

Il est possible d'augmenter cet article en précisant qu'un octroi d'office est réalisé pour différentes fonction du SRC, du RM et de l'AS-Rens, ceci pour amoindrir la charge administrative en terme de nombre de demandes de certificat.

Annexe 7 OCSP

L'annexe 7 ne peut en aucun cas être publiée en l'état. Les bases légales actuelles ne permettent pas de récolter de telles information (opinions ou activités religieuses, philosophiques, politiques, syndicales, sphère privée et sexualité informations médicales etc.) sans une base légale suffisament explicite **au niveau de la loi.** Il s'agit d'atteintes très graves à la sphère privée, droit fondamental réalisé dans l'article 13 de la Constitution fédérale. De telles atteintes nécessitent selon l'art. 36 Cst **une base légale dans une loi.** De plus, ces informations ne permettent pas d'effectuer directement un contrôle de risque.

---

[4] Loi fédérale sur les systèmes d'information de l'armée (LSIA), du 3 octobre 2008, RS 510.91.
[5] Sauf pour le Renseignement militaire (RM) à qui ne s'applique explicitement pas la LSIA.

À la lettre « j », l'autorité chargée du contrôle de sécurité souhaite s'octroyer la possibilité d'avoir accès aux données des systèmes d'information du Renseignement militaire (RM). Cette proposition doit être tracée. Les informations traitées dans ces systèmes n'ont aucuns liens avec les activités du service spécialisé et doivent être communiquées au cercle le plus restreint possible.

La différenciation entre les différents niveaux de contrôle pour le traitement des données n'est pas suffisamment précise.

Proposition : Revoir totalement l'annexe 7 et l'article 19 OCSP. Consulter des juristes externes au DDPS, voir à l'administration fédérale, pour assurer la légalité des éléments mentionnés dans cette partie de l'OCSP. Effectuer une nouvelle procédure de consultation pour le texte nouvellement écrit.

Cette prise de position a été réalisée à titre personnel et non au nom de l'Université de Berne ou de l'Institut de droit pénal et de criminologie.

En espérant que mes remarques vous seront utiles pour assurer la légalité et la proportionnalité des activités du DDPS.

Recevez, Madame la Conseillère fédérale, l'assurance de mes meilleures salutations,

Xavier Dufour, MLaw