Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Bern, 2. Dezember 2022

Vorentwurf zur Änderung des Bundesgesetzes vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG)

Bericht über die Ergebnisse der Vernehmlassung

Inhaltsverzeichnis

1 Ausgangslage 3

2 Gegenstand des Vernehmlassungsentwurfs 3

3 Ergebnisse der Vernehmlassung 4

3.1 Gesamtbeurteilung der Vorlage 4

3.2 Zusammenfassung der Vernehmlassungsantworten und hauptsächliche Kritikpunkte 4

3.3 Anträge und Bemerkungen zum Vorentwurf 5

3.3.1 Vorbemerkung 5

3.3.2 Anträge und Bemerkungen zu den einzelnen Bestimmungen 6

3.3.2.1 Titel 6

3.3.2.2 Artikel 1 Absatz 1 (Zweck) 6

3.3.2.3 Artikel 2 Absatz 5 (Geltungsbereich) 6

3.3.2.4 Artikel 5 Buchstaben d und e (Begriffe) 7

3.3.2.5 Artikel 73*a* Grundsatz 8

3.3.2.6 Artikel 73*b* Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen 9

3.3.2.7 Artikel 73*c* Weiterleitung von Informationen 11

3.3.2.8 Artikel 74 Unterstützung von Betreiberinnen von kritischen Infrastrukturen 12

3.3.2.9 Artikel 74*a* Meldepflicht 14

3.3.2.10 Artikel 74*b* Bereiche 15

3.3.2.11 Artikel 74*c* Ausnahmen von der Meldepflicht 18

3.3.2.12 Artikel 74*d* Zu meldende Cyberangriffe 20

3.3.2.13 Artikel 74e Inhalt der Meldung 22

3.3.2.14 Artikel 74*f* Übermittlung der Meldung 23

3.3.2.15 Artikel 74*g* Auskunftspflicht 25

3.3.2.16 Artikel 74*h* Verletzung der Melde- oder Auskunftspflicht 26

3.3.2.17 Artikel 74*i* Widerhandlungen gegen Verfügungen des NCSC 26

3.3.2.19 Artikel 76 Zusammenarbeit im Inland 29

3.3.2.20 Artikel 76*a* Unterstützung für Behörden 30

3.3.2.21 Artikel 77 Internationale Zusammenarbeit 31

3.3.2.22 Artikel 79 Abs. 1 (Datenaufbewahrung und -archivierung) 32

3.3.2.23 Änderungserlasse 33

3.4 Weitere Anträge und Anregungen zum Vorentwurf 33

3.5 Anträge und Anregungen zu Themen ausserhalb der Vorlage 34

4 Anhang 35

4.1 Kantone 35

4.2 In der Bundesversammlung vertretene politische Parteien 37

4.3 Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete 37

4.4 Gesamtschweizerische Dachverbände der Wirtschaft 37

4.5 Weitere interessierte Kreise – Stellungnahmen auf Einladung 38

4.6 Weitere interessierte Kreise – Spontane Stellungnahmen 39

1 Ausgangslage

Am 12. Januar 2022 hat der Bundesrat den Vorentwurf zur Änderung des Informationssicherheitsgesetzes vom 18. Dezember 2020 (ISG) sowie den erläuternden Bericht verabschiedet und das Eidgenössische Finanzdepartement (EFD) beauftragt, ein Vernehmlassungsverfahren durchzuführen. Die Vernehmlassung dauerte vom 12. Januar bis zum 14. April 2022. Die Liste aller Vernehmlassungsteilnehmenden mit den nachfolgend verwendeten Abkürzungen findet sich im Anhang. Es sind 99 Stellungnahmen eingegangen:

99	Total eingegangene Stellungnahmen
25	Kantonsregierungen
4	Kantonale Konferenzen
7	Parteien
1	Gesamtschweizerischer Dachverband der Gemeinden, Städte und Berggebiete
4	Gesamtschweizerische Dachverbände der Wirtschaft
19	Betroffene Unternehmen
39	Weitere interessierte Kreise

Die Stellungnahmen sind auf der Publikationsplattform des Bundesrechts «Fedlex» aufgeschaltet[1].

2 Gegenstand des Vernehmlassungsentwurfs

Ziel des Vorentwurfs ist es, im Informationssicherheitsgesetz (ISG), das am 18. Dezember 2020 vom Parlament verabschiedet wurde, die gesetzliche Grundlage für eine Meldepflicht für Cyberangriffe auf kritische Infrastrukturen zu schaffen.

Inhaltlich soll die Meldepflicht nur für Cyberangriffe gelten, die ein gewisses Schadenspotential aufweisen. Nicht meldepflichtig sind Cybervorfälle, die auf menschliches Fehlverhalten, also beispielsweise eine unbeabsichtigte fehlerhafte Manipulation eines Mitarbeitenden, zurückzuführen sind. Es wurde auch davon abgesehen, die Meldepflicht auf Schwachstellen in Informatikmitteln auszudehnen. Die Meldepflicht gilt für Betreiberinnen kritischer Infrastrukturen, die in kritischen Teilsektoren tätig sind. Die Funktion als zentrale Meldestelle übernimmt das NCSC, das auch freiwillige Meldungen zu Cybervorfällen und Schwachstellen in Informatikmitteln entgegennimmt.

Die gesetzlichen Grundlagen der Meldepflicht für Cyberangriffe, sollen – abgesehen von wenigen Anpassungen im 1. Kapitel – im 5. Kapitel des ISG eingefügt werden. Das 5. Kapitel wurde grundlegend überarbeitet, um darin auch die Aufgaben des NCSC – welche aktuell nur in der Cyberrisikenverordnung (CyRV)[2] definiert sind – und dessen Funktion als Meldestelle für meldepflichtige Cyberangriffe zu regeln.

Durch Einführung einer Meldepflicht können Cyberangriffe künftig frühzeitig entdeckt, ihre Angriffsmuster analysiert und andere Betreiberinnen kritischer Infrastrukturen rechtzeitig gewarnt werden. Die Meldepflicht kann dadurch einen wesentlichen Beitrag zur Erhöhung der Cybersicherheit in der Schweiz leisten.

Nicht Gegenstand dieser Vorlage ist die Einführung von verbindlichen Mindeststandards für die Cybersicherheit für Betreiberinnen kritischer Infrastrukturen sowie von Anforderungen an die Produktesicherheit von IT-Produkten.

1 www.fedlex.admin.ch > Vernehmlassungen > Abgeschlossene Vernehmlassungen > 2022 > EFD
2 SR **120.73**

3 Ergebnisse der Vernehmlassung

3.1 Gesamtbeurteilung der Vorlage

89 Vernehmlassungsteilnehmende der Vernehmlassungsteilnehmenden **begrüssen** grundsätzlich die **Zielsetzungen und Stossrichtungen des Vorentwurfs**, wobei teilweise auch Vorbehalte angebracht werden.

Positive Stellungnahmen (von insgesamt 102 Stellungnahmen)	**89**
Kantonsregierungen	25
Kantonale Konferenzen	4
Parteien	6
Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete	1
Gesamtschweizerische Dachverbände der Wirtschaft	3
Betroffene Unternehmen	17
Weitere interessierte Kreise	33

7 Vernehmlassungsteilnehmende haben sich ausdrücklich **gegen den Vorentwurf ausgesprochen**.

Negative Stellungnahmen (von insgesamt 102 Stellungnahmen)	**7**
Kantonsregierungen	-
Kantonale Konferenzen	-
Parteien	1
Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete	-
Gesamtschweizerische Dachverbände der Wirtschaft	1
Betroffene Unternehmen	2
Weitere interessierte Kreise	3

Die Bundesanwaltschaft, SwissDigital und die Piratenpartei haben inhaltliche Änderungsvorschläge gemacht, aber auf eine Bewertung der Vorlage verzichtet.
Folgende Vernehmlassungsteilnehmende haben explizit auf eine Stellungnahme verzichtet: Kanton Obwalden, Schweizerische Staatsanwälte-Konferenz, Stiftung Auffangeinrichtung BVG.

3.2 Zusammenfassung der Vernehmlassungsantworten und hauptsächliche Kritikpunkte

Alle Kantone (mit Ausnahme des Kantons Obwalden, der auf eine Stellungnahme verzichtet hat), 4 kantonale Konferenzen (KKJPD, KKPKS, RK MZF, GDK), 6 Parteien (SP, SVP, FDP, Die Mitte, die Grünen und GLP), der Schweizerische Städteverband, 3 gesamtschweizerische Dachverbände der Wirtschaft (economiesuisse, Swiss Banking, SGB), 17 Unternehmen (Abraxas, Axpo, Flughafen ZH, Flughafen GE, Helvetia Versicherungen, Migros, die Post, Raiffeisen, Romande Energie, SBB, Salt, Sunrise, Suva, Swisscom, Swissgrid, Switch, TPG), 34 interessierte Organisationen (AEROSUISSE, asut, AEIS, Verband der Auslandsbanken in der Schweiz, Centre Patronal, CH++, Digitale Gesellschaft, digitalswitzerland, eAHV, eGov-Schweiz, FER, GEM, Härting Rechtsanwälte, IG eHealth, Inter-pension, ASIP, Operation Libero, Pour Demain, privatim, santésuisse, ISSS, RAILplus, SVV, Swico, swissICT, Swissmem, Trust Valley, SVGW, UniBe, VAV, VUD, VöV, VSE, UniZH/UNIL NFP 77, UniGE) und die Gemeinde Gachnang **begrüssen die Zielsetzungen und die Stossrichtungen des Vorentwurfs.**

Die meisten Stellungnahmen zugunsten des Vorentwurfs verlangen ausdrücklich, dass die Meldepflicht **keine hohen Kosten** für die öffentliche Verwaltung oder die Privatwirtschaft (namentlich Unternehmen, die einen Cybervorfall melden) mit sich bringt, dass die Umsetzung der Meldepflicht unbürokratisch erfolgt und dass der **administrative Aufwand gering bleibt.** Alle Teilnehmenden wünschen Präzisierungen und viele äussern Vorbehalte zu gewissen Bestimmungen.

Die **Präzisierungen** betreffen insbesondere die Begriffe (Art. 5), die Liste der Bereiche, die der Meldepflicht unterstehen (Art. 74*b*), und die Ausnahmen von der Meldepflicht (Art. 74*c*), die Definition der zu meldenden Cyberangriffe (Art. 74*d*) sowie die Modalitäten für die Übermittlung der Meldung (Art. 74*f*).

Insbesondere zu den Strafen bei Verletzung der Meldepflicht (Art. 74*h* und Art. 74*i*) wurden **Vorbehalte** geäussert. 24 Institutionen, die sich an der Vernehmlassung beteiligt haben, **lehnen jegliche Möglichkeit von Sanktionen ab.** Sie begründen ihre Ablehnung hauptsächlich damit, dass Bussen grundsätzlich nicht das richtige Instrument seien, um die Einhaltung der Meldepflicht zu erwirken. Sie vertreten die Ansicht, dass die Umsetzung der Meldepflicht eher durch Anreize im Sinne von Unterstützungsleistungen gefördert werden müsste.

Diese Vernehmlassung hat ausserdem gezeigt, dass der Schutz von Informationen aus Meldungen – insbesondere von Personendaten – von grosser Bedeutung ist. Tatsächlich wurden hinsichtlich der **Weiterleitung personenbezogener Daten an die Nachrichtendienste sowie an die Strafverfolgungsbehörden** von sechs Vernehmlassungsteilnehmenden (Swico, Privatim, Piratenpartei, digitale Gesellschaft, Romande Energie, Verein Unternehmensdatenschutz) Bedenken geäussert.

Zudem wünschen sich einige Vernehmlassungsteilnehmende, dass der Vorentwurf erweitert werde. Es gehe nicht nur um die Einführung einer Meldepflicht. Das NCSC müsse zudem die Befugnis haben, den Betreiberinnen von kritischen Infrastrukturen **Mindeststandards** aufzuerlegen und die Umsetzung von Massnahmen wie die **Installation von Sicherheitsupdates** zu verlangen. In diesem Zusammenhang wird auch vorgeschlagen, dass die Betreiberinnen von kritischen Infrastrukturen den Artikeln 6 bis 10 ISG unterstellt sein sollen.

Weiter begrüssen die Teilnehmenden die Tatsache, dass auch Schwachstellen dem NCSC gemeldet werden können, dass dieses zunächst die Hersteller der betreffenden Produkte gemäss den **«Coordinated Vulnerability Disclosure»**-Grundsätzen informiert und ihnen eine Frist setzt, um die Schwachstellen zu beheben. Es wird gewünscht, dass die Institutionen, die Schwachstellen melden, strafrechtlich nicht verfolgt werden dürfen, und dass die Hersteller, die diese Schwachstellen nicht innert der vom NCSC gesetzten Frist beheben, von öffentlichen Beschaffungen ausgeschlossen werden können.

SVP, SGV, scienceindustries, swissuniversities, Coop, Swiss Airlines und eine Einzelperson **lehnen** den Vorentwurf in seiner aktuellen Form **ab.** Die Bundesanwaltschaft (BA) hat sich nicht ausdrücklich für oder gegen den Vorentwurf geäussert.

3.3 Anträge und Bemerkungen zum Vorentwurf

3.3.1 Vorbemerkung

Im Folgenden werden die Bemerkungen, Änderungsvorschläge und Kritikpunkte zu den einzelnen Bestimmungen aufgeführt. Es werden jeweils lediglich die in einer Stellungnahme vorgebrachten Hauptargumente erwähnt. Besonders ausführliche Stellungnahmen werden nur insoweit wiedergegeben, als sie konkrete materielle Änderungen fordern. Weitere Einzelheiten können den im Internet publizierten Stellungnahmen entnommen werden.
Stillschweigende Zustimmung bzw. der Verzicht auf eine Rückmeldung zu einem Artikel wird nicht erwähnt. Dies soll die Leserschaft aber nicht darüber hinwegtäuschen, dass trotz zahlreicher kritischer Stimmen zu einzelnen Bestimmungen eine Mehrzahl der Vernehmlassungsteilnehmenden

mit weiten Teilen der vorgeschlagenen Gesetzesbestimmungen grundsätzlich einverstanden ist. Zur Gesetzessystematik sind keine Stellungnahmen eingegangen.

3.3.2 Anträge und Bemerkungen zu den einzelnen Bestimmungen

3.3.2.1 Titel

Der **Kanton Thurgau** regt an, den Titel des Erlasses anzupassen, da der aktuelle Titel «Bundesgesetz über die Informationssicherheit beim Bund» suggeriere, dass sich sein Geltungsbereich auf den Bund beschränke. Das sei mit der Einführung einer Meldepflicht nicht mehr der Fall.

3.3.2.2 Artikel 1 Absatz 1 (Zweck)

> [1] Dieses Gesetz soll:
>
> a. die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten;
>
> b. die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken erhöhen.

Zum vorliegenden Artikel sind 4 Reaktionen eingegangen, die im Wesentlichen konzeptuelle Anpassungen betrafen.

❖ **Allgemeine Bemerkungen zu Artikel 1 Absatz 1**

Migros schlägt vor, Artikel 1 mit einer Regelung zum räumlichen Geltungsbereich zu ergänzen.

Laut dem **Kanton TG** ist die Trennung in Buchstabe a und Buchstabe b in diesem Fall nicht sinnvoll.

❖ **Zustimmung zu Artikel 1 Absatz 1**

Swiss Banking begrüsst die Tatsache, dass Artikel 1 ausdrücklich die «Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken» einschliesst. Dadurch untermauere Artikel 1 die in Artikel 73*a* ff. festgelegten Aufgaben des NCSC.

❖ **Änderungsanträge und Anregungen zu Artikel 1 Absatz 1**

- **<u>Zu Buchstabe a</u>**

ISSS und Härting Rechtsanwälte verlangen, Artikel 1 wie folgt zu ergänzen: «die sichere Bearbeitung der Informationen, für die der Bund zuständig ist, sowie den sicheren Einsatz der Informatikmittel des Bundes gewährleisten, [*es sei denn eine Spezialgesetzgebung sehe eine gesonderte Zuständigkeit vor*]».

- **<u>Zu Buchstabe b</u>**

Swico verlangt, den Begriff «Cyberrisiken» durch «Bedrohungen» zu ersetzen, da der Begriff «Cyberrisiken» laut **Swico** nicht definiert werden kann.

3.3.2.3 Artikel 2 Absatz 5 (Geltungsbereich)

> [5] Für Organisationen des öffentlichen und privaten Rechts, die kritische Infrastrukturen betreiben, die aber nicht unter die Absätze 1–3 fallen, gelten die Artikel 73*a*–79. Die Spezialgesetzgebung kann weitere Teile dieses Gesetzes für anwendbar erklären.

Zum vorgeschlagenen Geltungsbereich sind 5 allgemeine Bemerkungen eingegangen.

❖ **Allgemeine Bemerkungen zu Artikel 2 Absatz 5**

Swissmem sowie UniZH/UNIL NFP 77 haben betont, dass neben den Artikeln 73*a*–79 auch Artikel 6 ISG zu berücksichtigen sei.

UniZH/UNIL NFP 77 ist der Ansicht, dass es sinnvoll wäre, die Möglichkeit vorzusehen, das NCSC beizuziehen, um festzustellen, ob eine Betreiberin dem Gesetz oder der Meldepflicht unterstellt ist, wie dies beispielsweise in der VÜPF vorgesehen ist (siehe insbesondere Art. 51 VÜPF).

Der **Kanton GE** verlangt eine Definition des Begriffs «kritisch».

❖ **Änderungsanträge und Anregungen zu Artikel 2 Absatz 5**

ISSS und Härting Rechtsanwälte bitten um eine Ergänzung von Artikel 2 Absatz 5 wie folgt: «*…* die kritische Infrastrukturen *[gemäss Artikel 74b]* betreiben, *…*»*,* um zu präzisieren, dass von kritischen Infrastrukturen im Sinne des ISG die Rede ist.

3.3.2.4 Artikel 5 Buchstaben d und e (Begriffe)

In diesem Gesetz bedeuten: d. *Cybervorfall:* Ereignis beim Betrieb von Informatikmitteln, das dazu führen kann, dass die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist; e. *Cyberangriff:* Cybervorfall, der von Unbefugten absichtlich ausgelöst wurde.

23 Vernehmlassungsteilnehmende haben sich zu den beiden Definitionen geäussert und Änderungsanträge gestellt.

❖ **Allgemeine Bemerkungen zu Artikel 5**

Economiesuisse, IG eHealth, die Post und VUD sind der Ansicht, dass die Begriffe «Cybervorfall» und «Cyberangriff», wie sie in diesem Artikel gemeint sind, genauer definiert werden müssten.

Digital Law Center UniGE verlangt, dass Cyberangriffe und Cybervorfälle so definiert werden, dass sie auch ohne Verletzung der Datensicherheit oder anderer gesetzlicher oder regulatorischer Bestimmungen entsprechend eingestuft werden können.

❖ **Änderungsanträge und Anregungen zu Artikel 5**

IG eHealth, ISSS, Härting Rechtsanwälte, der Kanton GE und die Post vertreten die Meinung, dass eine Definition der Begriffe «Schwachstelle» und «Cyberrisiko» in diesen Artikel aufzunehmen sei.

Die **Gemeinde Gachnang** erachtet es als notwendig, das Präfix «Cyber» zu definieren.

- **<u>Zu Buchstabe d</u>**

Pour Demain schlägt vor, die künstliche Intelligenz im Rahmen der Definition von «Cybervorfall» explizit zu erwähnen.

Migros, Sunrise, TPG und digitalswitzerland verlangen, dass der Satz «das dazu führen kann» geändert wird. Die letzten drei sind der Ansicht, dass er durch folgenden Satz ersetzt werden sollte**:** «das dazu führt». Migros hingegen fordert eine bessere Definition.

Santésuisse meint, dass die Definition nicht hinreichend genau sei und dass sich solche Ereignisse auch ohne Cyberangriff als Auslöser zutragen könnten, beispielsweise durch den Ausfall von IT-Komponenten oder durch Programmierfehler. Diese Ereignisse dürften nicht unter die Meldepflicht fallen.

UniZH/UNIL NFP 77 sind der Ansicht, dass die vorliegende Definition von «Cybervorfall» und die in Artikel 3 Buchstabe b CyRV vorgesehene Definition aufeinander abzustimmen seien. Zudem erachten **UniZH/UNIL NFP 77** den Ausdruck «beim Betrieb von Informatikmitteln» als nicht optimal, da er jegliches passives Verhalten ausschliesst und so als zu restriktiv empfunden werden könne.

- **<u>Zu Buchstabe e</u>**

Swissgrid fragt, ob die Definition von «Unbefugten» nur externe oder auch interne Personen umfasse.

3.3.2.5 Artikel 73*a* Grundsatz

Zum Schutz der Schweiz vor Cyberrisiken nimmt das nationale Zentrum für Cybersicherheit (NCSC) insbesondere folgende Aufgaben wahr: a. Sensibilisierung der Öffentlichkeit auf Cyberrisiken; b. Warnung vor Cyberrisiken und Schwachstellen von Informatikmitteln; c. Veröffentlichung von Informationen zur Cybersicherheit sowie von Anleitungen für präventive und reaktive Massnahmen gegen Cyberrisiken; d. technische Analysen zur Bewertung und Abwehr von Cyberrisiken; e. Entgegennahme und Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen von Informatikmitteln; f. Unterstützung von Betreiberinnen von kritischen Infrastrukturen.

16 Vernehmlassungsteilnehmende haben sich zum Teil sehr ausführlich zu den vorgeschlagenen Grundsätzen geäussert. 2 Teilnehmende sind mit dem aktuellen Wortlaut von Artikel 73*a* einverstanden, 5 verlangen, dass zur obigen Liste eine Aufgabe hinzugefügt wird, und 9 weitere haben Bemerkungen gemacht und andere Änderungen beantragt.

- ❖ **Allgemeine Bemerkungen zu Artikel 73*a***

CH++ begrüsst den Artikel, ist aber der Meinung, dass als Aufgabe des NCSC die «aktive Erkennung von Schwachstellen und Bedrohungen» zum vorliegenden Artikel hinzugefügt werden müsste.

Die **Gemeinde Gachnang** begrüsst den Artikel, spricht sich aber dafür aus, im Artikel 73*a* die Aufgaben um ein «regelmässiges Reporting zwecks Qualitätssicherung und Erfolgskontrolle» zu ergänzen.

Migros verlangt eine nicht abschliessende Liste von Beispielen, um die Absicht von Artikel 73*a* zu untermauern.

Der **Kanton BE** verlangt die Ergänzung von Artikel 73*a* um einen zweiten Absatz: «Das NCSC arbeitet bei der Erfüllung dieser Aufgaben mit den Polizeibehörden der Kantone zusammen».

Swisscom begrüsst diesen Artikel, hält es aber für notwendig, dass für das NCSC neben den bereits erwähnten Aufgaben und Kompetenzen im Gesetz festgehalten wird, dass es nicht nur den Bund, sondern auch die Wirtschaft und die Bevölkerung unterstützt.

- ❖ **Zustimmung zu Artikel 73*a***

Swico, SuisseDigita und swissICT loben die Schaffung rechtlicher Grundlagen für die Aufgaben des NCSC explizit.

- ❖ **Änderungsanträge und Anregungen zu Artikel 73*a***

- **<u>Zu Buchstabe b</u>**

Pour Demain ist der Ansicht, dass die mit der KI verbundenen Risiken zu den oben erwähnten Aufgaben des NCSC hinzugefügt werden müssten.

- **Zu Buchstabe c**

Swiss Banking und Raiffeisen begrüssen den Artikel, erachten aber die «Anleitungen für präventive und reaktive Massnahmen gegen Cyberrisiken» nur als sinnvoll, wenn sie nicht verpflichtend sind.

- **Zu Buchstabe f**

Die Grünen fordern, dass die «Unterstützung von Betreiberinnen von kritischen Infrastrukturen» (Art. 73*a* Bst. f) breiter gedacht wird, als die Definitionen das bisher vorsehen.

3.3.2.6 Artikel 73*b* Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen

[1] Werden dem NCSC Cybervorfälle oder Schwachstellen von Informatikmitteln gemeldet, so analysiert es diese auf ihre Bedeutung für den Schutz der Schweiz vor Cyberrisiken. Es gibt auf Wunsch der meldenden Person eine Empfehlung zum weiteren Vorgehen ab, sofern dafür keine weiteren Analysen und Abklärungen erforderlich sind.
[2] Das NCSC kann Informationen zu Cybervorfällen veröffentlichen oder an interessierte Behörden und Organisationen weiterleiten, sofern dies dazu dient, Cyberangriffe zu verhindern oder zu bekämpfen. Diese Informationen dürfen Personendaten und Daten juristischer Personen enthalten, sofern es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt und die betroffene Person einwilligt.
[3] Werden dem NCSC Schwachstellen gemeldet, so informiert es umgehend den Hersteller und setzt ihm zur Behebung der Schwachstelle eine angemessene Frist. Behebt der Hersteller die Schwachstelle nicht innert dieser Frist, so veröffentlicht das NCSC die Schwachstelle unter Angabe der betroffenen Soft- oder Hardware, sofern dies zum Schutz vor Cyberrisiken beiträgt.

21 Teilnehmende haben sich dazu geäussert. Im Allgemeinen hat Absatz 3 am meisten Reaktionen hervorgerufen.

❖ **Allgemeine Bemerkungen zu Artikel 73*b***

Scienceindustries ist der Meinung, dass die Umsetzung der Meldepflicht bedinge, dass sie einen Mehrwert für die betroffenen Unternehmen darstelle, einen verhältnismässigen und subsidiären Ansatz verfolge, keine Mehrkosten für die Schweizer Wirtschaft auslöse und auf einer kooperativen Grundlage beruhe.

Die Grünen, die Digitale Gesellschaft und die Piratenpartei begrüssen Artikel 73*b,* vertreten aber die Ansicht, dass das NCSC bestimmte Mindestanforderungen erfüllen müsse, um seine Verpflichtungen in Bezug auf diesen Artikel einhalten zu können: Es müsse über umfassendere Kompetenzen verfügen bei schweren Vorfällen und ein Responsible-Disclosure-Verfahren für die kritischen Infrastrukturen einrichten.

Die Grünen und CH++ verlangen, dass das NCSC gegenüber Herstellern und Betreiberinnen Leitlinien sowie verbindliche Standardfristen erlassen kann, die sie verpflichten, Schwachstellen rasch zu beheben und Schäden zu begrenzen.

Der Kanton VD verlangt, den Artikel 73*b* mit der Medizinprodukteverordnung (MepV) abzustimmen.

❖ **Änderungsanträge und Anregungen**

- **Zu Absatz 1**

Laut **UniZH/UNIL NFP 77** ist die Formulierung «sofern dafür keine weiteren Analysen und Abklärungen erforderlich sind» nicht klar. Sie sei zu ersetzen durch «wenn Cybervorfälle oder Schwachstellen dem NCSC gemeldet werden», damit keine Beschränkung auf eine Meldung vorliegt, die mit der Meldung von Cyberangriffen durch die betreffende Person verwechselt werden könnte.

- **Zu Absatz 2**

Den Grünen und CH++ zufolge müsste das NCSC, ausser bei gerechtfertigten Ausnahmen eine Verpflichtung zur Veröffentlichung von Cybervorfällen einführen. **ISSS, Härting Rechtsanwälte, VSE, VöV, Swissgrid, der Kanton GE und RAILplus** bestehen hingegen darauf, dass Personendaten sowie Daten von juristischen Personen nur mit ausdrücklicher und vorgängiger Einwilligung veröffentlicht werden dürfen und dass die Umstände, unter denen der Cybervorfall veröffentlicht werden muss, sowie die bereitzustellenden Informationen aus Gründen des Datenschutzes und der Geheimhaltung vertraulicher Daten genauer zu regeln sind.

UniZH/UNIL NFP 77 sind der Ansicht, dass die Einwilligung von der Person stammen müsste, die die Daten teilt, und nicht von den betroffenen Personen. Denn das Einholen der Einwilligung sämtlicher betroffener Personen könne unverhältnismässig aufwendig sein.

- **Zu Absatz 3**

Die Piratenpartei begrüsst, dass in Artikel 73*b* Absatz 3 die Sicherheitslücken unverzüglich mit den Betreiberinnen kritischer Infrastrukturen geteilt werden, und bittet darum, hinzuzufügen, dass diese sie nicht für offensive Cyberspiele gemäss NDG missbrauchen dürfen. Ebenso müssten Hacker im Rahmen von Responsible Disclosure automatisch Straffreiheit erhalten.

CH++ schlägt vor, dass Hersteller, welche nicht auf Schwachstellenmeldungen reagieren, von öffentlichen Beschaffungen ausgeschlossen werden können sollen.

UniZH/UNIL NFP 77 vertreten die Meinung, dass es sinnvoll wäre, Absatz 3 neben der Veröffentlichung mit einer Sanktionsmöglichkeit auszustatten, während **die Post** hingegen erklärt, dass sich Sanktionen negativ auf die Anzahl Meldungen auswirken könnten.
Der **Kanton GE** beantragt, «Hersteller» durch «Hersteller und/oder Herausgeber» zu ersetzen.

Nach Ansicht **der Digitalen Gesellschaft** muss das NCSC, wenn es Kenntnis über eine Sicherheitslücke betreffend ein Drittprodukt hat, bei der nicht davon auszugehen ist, dass sie dem Hersteller bereits bekannt ist, diese Sicherheitslücke dem betreffenden Hersteller im Rahmen eines Responsible-Disclosure-Verfahrens unverzüglich melden. Zudem müssten dem NCSC der **Digitalen Gesellschaft** zufolge Mittel zur Verfügung gestellt werden, die es ihm erlauben, bei den Organisationen, die eine Sicherheitslücke melden, auf deren Behebung zu bestehen.

Laut **ISSS und Härting Rechtsanwälte** müssen Meldungen von Schwachstellen, die das NCSC den Herstellern zukommen lässt, vom Öffentlichkeitsprinzip ausgeschlossen sein.

Pour Demain und Operation Libero sind der Ansicht, dass die Fristen auch für die Betreiberinnen festgelegt werden müssten, um die effektive Durchführung von Sicherheitsupdates zu gewährleisten.

SSV und VUD äussern Bedenken, dass eine vorzeitige Veröffentlichung der Schwachstelle mit Angabe der betroffenen Software oder des betreffenden Materials für die meldende Stelle zu einem zusätzlichen Risiko führen könnte. Daher schlägt **VUD** vor, dass sämtliche Informationen und Kommunikationsmassnahmen des NCSC dem Gesetzesvorbehalt unterstellt werden müssen, dass sie Cyberangriffe nicht fördern oder erleichtern.

3.3.2.7 Artikel 73*c* Weiterleitung von Informationen

[1] Ergeben sich aus der Meldung eines Cybervorfalls oder dessen Analyse Informationen, die für das frühzeitige Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit, für die Beurteilung der Bedrohungslage oder für die nachrichtendienstliche Frühwarnung zum Schutz von kritischen Infrastrukturen nach Artikel 6 Absätze 1 Buchstabe a, 2 und 5 des Nachrichtendienstgesetzes vom 25. September 2015 (NDG) relevant sind, so leitet das NCSC diese Informationen an den NDB weiter.
[2] Für Mitarbeitende des NCSC entfällt die Anzeigepflicht gemäss Artikel 22a des Bundespersonalgesetzes vom 24. März 2000, wenn sie im Zusammenhang mit der Meldung eines Cybervorfalls oder dessen Analyse Hinweise auf eine mögliche Straftat erhalten. Die Leiterin oder der Leiter des NCSC kann Anzeige erstatten, sofern dies aufgrund der Schwere der möglichen Straftat geboten scheint.
[3] Informationen, die von einer Person im Rahmen einer Meldung dem NCSC bekanntgegeben wurden, dürfen in einem Strafverfahren gegen diese Person nur mit deren Einverständnis verwendet werden.
[4] Informationen, die strafrechtlich geschützte Geheimnisse offenbaren, darf das NCSC nur nach den Vorgaben von Artikel 320 StGB weiterleiten.

25 Teilnehmende haben sich zu diesem Artikel geäussert. Er wurde viel diskutiert und es sind viele Änderungsanträge eingegangen. 2 Stellen begrüssen Artikel 73*c* Absatz 3, während 3 andere Artikel 73*c* Absatz 2 ablehnen.

❖ Allgemeine Bemerkungen zu Artikel 73*c*

Privatim fordert, dass die an den NDB oder an die Strafverfolgungsbehörden übermittelten Daten nach der Übermittlung an diese Stellen von den Servern des NCSC gelöscht werden.

Der Kanton GR verlangt, dass das Zusammenspiel von «Geheimhaltungsverpflichtungen der Betreiberinnen» und «Weiterleitung von Informationen im Rahmen der Meldepflicht» expliziter formuliert wird.

Swico begrüsst den Artikel zwar, verlangt aber, dass präzisiert wird, dass nur sicherheitsrelevante Informationen kommuniziert werden.

❖ Zustimmung zu Artikel 73*c*

AEROSUISSE begrüsst den vorliegenden Gesetzestext.

Der Kanton AG begrüsst die Lösung, bei welcher die Mitarbeitenden des NCSC von der Anzeigepflicht ausgenommen werden und dem NCSC ein Anzeigerecht erteilt wird.

Die Grünen und CH++ begrüssen Artikel 73*c* Absatz 3.

❖ Ablehnung von Artikel 73*c*

Die Piratenpartei und eGov-Schweiz sind nicht damit einverstanden, dass der NDB die im Rahmen der Meldepflicht an das NCSC übermittelten Daten bearbeitet.

Der Kanton BE und die KKJPD verlangen die Streichung von Artikel 73*c* Absatz 2, da sie der Meinung sind, dass das NCSC weiterhin sämtliche Offizialdelikte an die Strafverfolgungsbehörden weiterleiten solle.

Der Kanton NW fordert, Artikel 73*c* Absatz 2 zu streichen, da der Artikel seiner Ansicht nach potenziell willkürlich sei.

❖ Änderungsanträge und Anregungen zu Artikel 73*c*

- **Zu Absatz 1**

Die **GLP** verlangt, in Artikel 73*c* Absatz 1 explizit festzuhalten, dass anonyme Meldungen beim NCSC möglich sind.

Die Grünen und VUD beantragen, dass die Daten anonym an das NCSC übermittelt werden können und dass dies rechtlich geregelt wird.

- **Zu Absatz 2**

Der Kanton SZ ist der Ansicht, dass das NCSC sicherstellen müsse, dass schwere Verstösse konsequent zur Anklage gebracht würden.

Die Kantone BL, NW und SZ haben ob der mit einer solchen Bestimmung verbundenen potenziellen Willkür Bedenken.

- **Zu Absatz 3**

Digitalswitzerland, Sunrise, VUD, swissICT und asut sind der Meinung, dass ein Risiko bestehe, dass die meldende Person sich selbst belaste, und verlangen daher eine Anpassung des Textes.

Digitalswitzerland beantragt, dass Artikel 73*c* Absatz 3 wie folgt geändert wird: «Informationen, die dem NCSC im Rahmen einer Meldung bekanntgegeben wurden und die meldende Person selbst belasten könnten, dürfen in einem Strafverfahren gegen diese Person nur mit Einverständnis dieser Person verwendet werden».

VUD schlägt vor, die Pflicht zur Einholung des Einverständnisses auf sämtliche Mitarbeitenden und Organe eines Unternehmens oder einer Organisation, die einen Cybervorfall melden, auszudehnen.

3.3.2.8 Artikel 74 Unterstützung von Betreiberinnen von kritischen Infrastrukturen

[1] Das NCSC unterstützt die Betreiberinnen von kritischen Infrastrukturen beim Schutz vor Cyberrisiken.
[2] Es stellt ihnen dazu insbesondere folgende Hilfsmittel zur Verfügung:
a. ein Kommunikationssystem für den sicheren Informationsaustausch;
b. technische Informationen zu aktuellen Cyberrisiken und Schwachstellen sowie Empfehlungen für präventive Massnahmen;
c. technische Instrumente und Anleitungen zur Erkennung von Cybervorfällen, die auf den erhöhten Schutzbedarf von kritischen Infrastrukturen ausgerichtet sind.
[3] Es berät und unterstützt sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen, wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht und, sofern es sich um private Betreiberinnen handelt, die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist.
[4] Es kann zur Analyse eines Cybervorfalls mit dem Einverständnis der betroffenen Betreiberin auf deren Informationen und Informatikmittel zugreifen. Das Einverständnis kann unabhängig von allfälligen Geheimhaltungspflichten gewährt werden.

22 Vernehmlassungsteilnehmende haben sich konkret zu dieser Gesetzesbestimmung geäussert. Die meisten Anträge betreffen Textänderungen oder Klärungen. Eine einzige Stelle lehnt diesen Artikel ab.

- ❖ **Allgemeine Bemerkungen zu Artikel 74**

Die Grünen begrüssen, dass das NCSC die Betreiberinnen kritischer Infrastrukturen bei Cyberrisiken unterstützt.

Der SSV verlangt weitere Klärungen zur Unterstützung der Städte, insbesondere hinsichtlich der Einführung von Mitteln zur Erkennung und Identifikation von Cyberangriffen sowie deren Finanzierung.

Raiffeisen ist der Ansicht, dass der Einsatz der vom NCSC bereitgestellten Mittel freiwillig bleiben und keine Pflicht zur Nutzung dieser Mittel eingeführt werden solle.

UniBe verlangt, dass das NCSC die Betreiberinnen von kritischen Infrastrukturen über die von anderen Betreiberinnen von kritischen Infrastrukturen gemeldeten Cyberangriffe informiert.

❖ **Änderungsanträge und Bemerkungen zu Artikel 74**

- **Zu Abs. 2 Buchstabe a**

ISSS, Härting Rechtsanwälte und die Post fordern, dass das NCSC neben der Bereitstellung eines Kommunikationssystems für den gesicherten Informationsaustausch eine sichere Datenspeicherung gewährleistet.

- **Zu Abs. 2 Buchstabe b**

Der Kanton SH spricht sich für die Errichtung einer gemeinsamen Plattform für den Informationsaustausch aus.

- **Zu Abs. 2 Buchstabe c**

Die Post verlangt eine Umformulierung, damit eindeutig sichergestellt ist, dass der Einsatz solcher Techniken zwar empfohlen wird, dieser aber letztlich freiwillig und nicht verpflichtend ist.

- **Zu Absatz 3**

VSE begrüsst die Bestrebungen, die privatwirtschaftlichen Angebote nicht konkurrenzieren zu wollen, schlägt aber vor, dass das NCSC als GovCERT einen Schirm über die privatwirtschaftlichen CERT bildet und diese bei der Krisenbewältigung je nach Situation und Bedarf unterstützt. **VSE** verlangt zudem, dass relevantere Unterscheidungskriterien dafür festgelegt werden, wer Anspruch auf die Unterstützung des NCSC hat, und fordert die Anpassung von Artikel 74 Absatz 3 wie folgt: «Es berät und unterstützt sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen, wenn für die kritische Infrastruktur ein unmittelbares Risiko von gravierenden Auswirkungen besteht».

UniZH/UNIL NFP 77 sind der Meinung, dass die Bestimmung die Schadensfolgen auf die Mitarbeitenden, die Begünstigten, die Leistungen sowie (teilweise) auf die Gesellschaft ausdehnen müsste.

Die Post und der Kanton GE fordern Präzisierungen zum Begriff «unmittelbares Risiko» und **die Post** zusätzlich zum Begriff «gravierende Auswirkungen».

- **Zu Absatz 4**

Für diesen Absatz verlangt **digitalswitzerland,** dass klarer erläutert wird, wie das NCSC die Geheimhaltungspflichten schützt.

ISSS und Härting Rechtsanwälte beantragen, dass der Text wie folgt ersetzt wird: «Es kann zur Analyse eines Cybervorfalls mit dem Einverständnis der betroffenen Betreiberin auf deren Informationen und Informatikmittel zugreifen. Der Zugriff kann gewährt werden ohne allfällige Geheimhaltungspflichten zu verletzen».

Nach Ansicht von **UniZH/UNIL NFP 77** muss die Bestimmung umformuliert werden, indem eingefügt wird, dass das NCSC die Vertraulichkeit gewährleistet und dass die Betreiberin kein Geheimnis verletzt, wenn sie die Informationen weiterleitet und dem NCSC für die Analyse eines Vorfalls Zugang zu ihren Informatikmitteln gewährt.

3.3.2.9 Artikel 74*a* Meldepflicht

Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe nach deren Entdeckung so rasch als möglich melden, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

27 Vernehmlassungsteilnehmende haben sich dazu geäussert, 14 davon haben betont, dass es wichtig sei, eine Meldefrist festzulegen.

- **Änderungsanträge und Bemerkungen zu Artikel 74*a***

Die Grünen, AEROSUISSE und economiesuisse verlangen explizit, dass durch die Meldepflicht keine zusätzlichen Kosten entstehen, weder für die nationale Wirtschaft noch für die meldenden Institutionen. Zudem sei der administrative Aufwand beim Meldeprozess auf ein Minimum zu beschränken.

Die Grünen, GLP, ISSS, Härting Rechtsanwälte und Pour Demain sind der Meinung, dass die Meldepflicht auch für Cyberangriffe und «allgemeine» Cybervorfälle sowie für Schwachstellen gelten müsse.

Sunrise und Switch sind der Ansicht, dass die Meldepflicht nur für Unternehmen gelten sollte, die Cyberangriffe auf ihre eigene Infrastruktur erlitten haben; keine Meldung von Dritten.

Die Digitale Gesellschaft beantragt, die Meldepflicht auf alle Sektoren der Schweizer Wirtschaft sowie auf die staatlichen Behörden und auf NGOs auszudehnen, während die **Piratenpartei** der Meinung ist, dass die Meldepflicht mindestens auf Organisationen auszuweiten sei, die im Auftrag des Staates Aufgaben ausführen, auf sämtliche Unternehmen, die einer ordentlichen Revision unterstehen oder gemäss Artikel 11*a* DSG Datensammlungen anmelden müssen.

eAHV ist der Ansicht, dass spezifiziert werden müsse, dass eine Meldung auch verschiedene betroffene Organisationen umfassen könne und dass die Meldung auch explizit durch Dritte erfolgen könne.

Die Piratenpartei und die Grünen finden, dass die KI im vorliegenden Gesetzestext behandelt werden müsse.

Die SP verlangt, dass die von Cyberangriffen betroffenen Personen vom NCSC so rasch als möglich gewarnt werden müssen.

Asut weist darauf hin, dass es schwierig sei, einen Internetprovider zu verpflichten, sämtliche Cyberangriffe zu melden, die über sein Netzwerk auf Betreiberinnen von kritischen Infrastrukturen erfolgten. Unter Umständen sei eine Meldung durch den Internetprovider wegen der Bestimmungen des Datenschutzgesetzes oder vertraglicher Vereinbarungen auch gar nicht möglich.

Der Verband der Auslandbanken in der Schweiz, CH++, Pour Demain, Swiss Banking, Scienceindustries, die Kantone FR, GR und UR, Raiffeisen, Switch und die Grünen betonen, dass es wichtig sei, explizite Fristen für die Meldung und die Kommunikation detaillierter Informationen an das NCSC festzulegen. **Swiss Banking** beantragt die Ergänzung des vorliegenden Textes um einen Absatz 2, der eine Meldefrist vorgibt, während **Raiffeisen und das Digital Law Center UniGE** empfehlen, die zweistufigen Meldefristen aus der FINMA-Aufsichtsmitteilung 05/2020 zu übernehmen.

Digitalswitzerland schlägt die Einführung des Begriffs des «Meldepflichtigen» vor, um eine höhere Präzision zu erreichen und jegliche Missverständnisse zu vermeiden.
Ausserdem halten es **digitalswitzerland und economiesuisse** für notwendig**,** das Vertrauen der Wirtschaft in den Nutzen dieses Artikels zu stärken, indem hervorgehoben wird, dass die Vorteile dieser Bestimmung unmittelbarer Natur sind und die Verpflichtungen überwiegen. Denn die Verhältnismässigkeit der Massnahmen sei insbesondere für KMU und Startups ein wichtiges Kriterium.

Der Flughafen ZH und Raiffeisen fordern, dass sich die Meldepflicht auf erfolgreiche Angriffe konzentriert. Daher schlägt **der Flughafen ZH** vor, den Text wie folgt zu ergänzen: «*... [erfolgreiche]* Angriffe *[im Sinne von Art. 74d] …».*

UniZH/UNIL NFP 77 verlangen, dass der Begriff «Entdeckung» durch «Erkennung» ersetzt wird und in der französischen Version der Begriff «celui-ci» klarer definiert wird.

3.3.2.10 Artikel 74*b* Bereiche

Die Meldepflicht gilt für:

a. Hochschulen nach Artikel 2 Absatz 2 des Hochschulförderungs- und -koordinationsgesetzes vom 30. September 2011;
b. Bundes-, Kantons- oder Gemeindebehörden sowie interkantonale, kantonale und interkommunale Organisationen;
c. Organisationen mit öffentlich-rechtlichen Aufgaben in den Bereichen Sicherheit und Rettung, Trinkwasserversorgung, Abwasseraufbereitung und Abfallentsorgung;
d. Unternehmen, die in den Bereichen Energieversorgung nach Artikel 6 Absatz 1 des Energiegesetzes vom 30. September 2016, Energiehandel, -messung oder -steuerung tätig sind;
e. Unternehmen, die dem Bankengesetz vom 8. November 1934, dem Versicherungsaufsichtsgesetz vom 17. Dezember 2004 oder dem Finanzmarktinfrastrukturgesetz vom 19. Juni 2015 unterstehen;
f. Anbieterinnen von Online-Marktplätzen, Cloudcomputing, Suchmaschinen und weiteren digitalen Diensten sowie Registrare von Domain-Namen und Betreiberinnen von Rechenzentren, die in der Schweiz:
    1. von einer grossen Zahl von Nutzenden beansprucht werden,
    2. eine hohe Bedeutung für die digitale Wirtschaft haben, oder
    3. Sicherheits- und Vertrauensdienste anbieten;
g. Spitäler, die auf der kantonalen Spitalliste nach Artikel 39 Absatz 1 Buch-stabe e des Bundesgesetzes vom 18. März 1994 über die Krankenversicherung aufgeführt sind;
h. medizinische Laboratorien mit einer Bewilligung nach Artikel 16 Absatz 1 des Epidemiengesetzes vom 28. September 2012;
i. Unternehmen, die für die Herstellung, das Inverkehrbringen und die Ein-fuhr von Arzneimitteln eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 2000 (HMG) haben oder Medizinprodukte nach Artikel 4 Absatz 1 Buchstabe b HMG herstellen oder vertreiben;
j. Organisationen, die Leistungen der Sozialversicherungen zur Absicherung der Folgen von Krankheit, Unfall, Arbeits- und Erwerbsunfähigkeit, Alter, Invalidität und Hilflosigkeit erbringen;
k. Anbieterinnen von Fernmeldediensten nach Artikel 3 Buchstabe b FMG;
l. die Schweizerische Radio- und Fernsehgesellschaft;
m. Nachrichtenagenturen von nationaler Bedeutung;
n. Anbieterinnen von Postdiensten, die bei der Postkommission nach Artikel 4 Abs. 1 des Postgesetzes vom 17. Dezember 2010 registriert sind;
o. Transportunternehmen, die dem Bundesgesetz vom 18. Juni 2010 über die Sicherheitsorgane der Transportunternehmen im öffentlichen Verkehr unterstehen;
p. Unternehmen der Zivilluftfahrt, die über eine Bewilligung des Bundesamtes für Zivilluftfahrt verfügen;
q. Unternehmen, die nach dem Seeschifffahrtsgesetz vom 23. September 1953 Güter auf dem Rhein befördern sowie Unternehmen, die die Registrierung, Ladung oder Löschung im Hafen Basel betreiben;
r. Unternehmen, die die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen;
s. Hersteller von Hard- und Software, deren Produkte von kritischen Infrastrukturen genutzt werden, sofern die Hard- oder Software einen Fernwartungszugang hat oder zu einem der folgenden Zwecken eingesetzt wird:
    1. Steuerungstechnik und Überwachung von Systemen,

2. Betrieb von Medizinprodukten und Fernmeldeanlagen,
3. Gewährleistung der öffentlichen Sicherheit,
4. IT-Sicherheit, Verschlüsselung, Identifikation, Zugriffs- und Zutrittsberechtigung.

Dieser Artikel hat viele Reaktionen hervorgerufen. 39 Vernehmlassungsteilnehmende haben sich zu den vorgesehenen Bereichen für die Meldepflicht geäussert.

- **Allgemeine Bemerkungen zu Artikel 74*b***

Die Piratenpartei ist der Meinung, dass die in Artikel 74*b* genannten Bereiche auf die grossen Medienunternehmen ausgedehnt werden sollten.

Die SP beantragt, die Liste alle fünf Jahre zu überprüfen und allenfalls zu aktualisieren.

Economiesuisse verlangt, die Meldepflicht auf die Bereiche zu beschränken, deren Ausfall oder Beeinträchtigung zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen würden.

Digitalswitzerland fordert eine Folgenabschätzung sowie einen abgestuften Regulierungsansatz, der sich an der Kritikalität der Unternehmen orientiert.

Scienceindustries, SGV, der Kanton UR und Swico fordern eine explizitere Liste, insbesondere indem klar festgelegt werde, was unter dem Begriff «kritische Infrastruktur» zu verstehen sei. In diesem Sinne schlägt **swissICT** eine qualitative Gewichtung nach «sehr kritisch» oder «kritisch» vor.

Der Kanton ZG und swissuniversities beantragen, die Liste zu revidieren und zu kürzen.

Coop und Migros schlagen vor, die Meldepflicht auf die als kritisch eingestuften Tätigkeiten im Unternehmen zu beschränken.

Der Kanton AG beantragt, den Artikel wie folgt zu ändern: «Objekte, Organisationen und Unternehmen, die von den zuständigen Stellen von Bund oder Kanton als kritische Infrastrukturen im Sinne des Bevölkerungsschutzes erfasst sind».

Der Kanton GR schlägt eine Vereinfachung der Umsetzung dieses Artikels vor. Es solle geprüft werden, ob eine Priorisierung und eine entsprechende zeitliche Staffelung vorzunehmen seien, um die Liste während einer Pilotphase zu reduzieren.

Der Kanton SZ fordert, dass die Betreiberinnen elektronischer Patientendossiers gemäss Artikel 10 des Bundesgesetzes über das elektronische Patientendossier vom 19. Juni 2015 (SR 816.1) ebenfalls der Meldepflicht unterstellt werden.

Der Kanton UR schlägt zudem vor, dass zusätzlich zur Meldepflicht die Meldung von Cybervorfällen für alle weiteren Organisationen empfohlen werden sollte.

Die Grünen regen an, diesen Bereich auf die Demokratie (politische Parteien im Parlament und Politikerinnen und Politiker in relevanten Ämtern) oder auf Presseagenturen auszuweiten.

- **Zustimmung zu Artikel 74*b***

Der Verband **eGov-Schweiz, die Kantone AI, GR und BE** sowie **privatim** halten die vorgeschlagene Bestimmung für angemessen.

- **Ablehnung von Artikel 74*b***

VUD lehnt den vorliegenden Artikel wegen Unverhältnismässigkeit ab und schlägt stattdessen vor, die Meldepflicht von vornherein auf Cyberangriffe zu begrenzen, welche kritische Infrastrukturen im Sinne von Artikel 5 Bst. c ISG erheblich gefährden und deshalb von nationalem Interesse sind.

❖ Änderungsanträge und Bemerkungen zu Artikel 74*b*

- **Buchstabe b (Behörden)**

Der SSV verlangt, dass die Zuständigkeit für die Meldepflicht der Gemeindebehörden geklärt wird.

- **Buchstabe c (Blaulicht, Wasser, Abwasser, Abfall)**

Laut dem **Kanton AI** sollte eine Meldung reichen, wenn die kantonalen und die kommunalen Behörden den gleichen Informatikanbieter haben.

- **Buchstabe f (Digitale Dienste)**

Digitalswitzerland schlägt aus Gründen der Klarheit vor, den Begriff «Online-Marktplätze» aus dem obenstehenden Text zu streichen.

SwissICT beantragt, dass bei Buchstabe f die Ziffern 1, 2 und 3 besser definiert werden.

Swissmem erklärt sich mit der vorliegenden Bestimmung einverstanden, wünscht sich jedoch eine klarere Unterscheidung zwischen einer Betreiberin oder einer Anbieterin von Dienstleistungen und einer Betreiberin von Dateninfrastrukturen (Cloud-Dienste).

Migros spricht sich für eine technologieneutral formulierte Definition aus.

Switch sowie UniZH/UNIL NFP 77 verlangen, den extraterritorialen Aspekt dieser Bestimmung insbesondere hinsichtlich der Anwendung schweizerischen Rechts zu erörtern.

UniZH/UNIL NFP 77 wünschen sich mehr Details dazu, welche Anbieter von verwandten Telekommunikationsleistungen davon ebenfalls betroffen sind.

Der Kanton GE fordert eine präzisere Definition des Begriffs «Sicherheits- und Vertrauensdienste».

Switch beantragt, dass die Verwaltung von .ch-Domainnamen in diese Bestimmung aufgenommen wird.

Den Grünen und CH++ zufolge stellt die Anzahl Nutzende keine gute Kennzahl für die Bedeutung der Zielgruppe dar.

Die Grünen und CH++ verlangen, dass der Begriff «digital» aus Ziffer 2 gestrichen wird.

- **Buchstabe g (Spitäler)**

Der Kanton GL bittet um mehr Details dazu, welche Spitäler (Grösse der Infrastrukturen) als kritische Infrastrukturen gelten, und verlangt, dass die Plattformen für das EPD ebenfalls der Meldepflicht unterstellt werden.

- **Buchstabe i (Arzneimittel)**

Scienceindustries verlangt eine genaue Definition und eine spezifische Bezeichnung für die Unternehmen, die dieser Bestimmung unterstellt sind.

- **Buchstabe j (Sozialversicherungen)**

Inter-pension ist der Ansicht, dass der Begriff «Sozialversicherungen» in der beruflichen Vorsorge (überobligatorische Leistungen) nicht klar definiert sei.

- **Buchstabe k (Fernmeldedienste)**

UniZH/UNIL NFP 77 legen nahe, dass dieser Artikel einen extraterritorialen Aspekt umfasse, weshalb die Anwendung schweizerischen Rechts vorzusehen sei (siehe z. B. die Theorie betreffend

die Auswirkungen gemäss Art. 3 revDSG). **SuisseDigital** weist darauf hin, dass Over-the-Top (OTT) Dienste keine Anbieterinnen von Fernmeldediensten sind. Es sind Präzisierungen nötig.

- **Buchstabe p (Zivilluftfahrt)**

AEROSUISSE sowie die Flughäfen GE und ZH fordern, dass der Text so angepasst wird, dass er die Liste der Fluggesellschaften, die der Meldepflicht unterstehen, nicht auf diejenigen reduziert, die über eine Bewilligung des Bundesamtes für Zivilluftfahrt verfügen.

- **Buchstabe r (Grundversorgung)**

Migros verlangt, dass einfach messbare Kriterien wie die Anzahl Mitarbeitende oder der Umsatz eingeführt wird, für die gewisse Erleichterungen oder Ausnahmen direkt im Gesetz vorgesehen werden.

Der Kanton GE und TPG fordern, in der französischen Fassung des Gesetzestextes den Begriff «chiffrage» anstelle von «cryptage» zu verwenden.

- **Buchstabe s (Hersteller Hard- und Software)**

Die Grünen und CH++ erachten die vorgeschlagene Bestimmung als angemessen und schlagen vor, die Lieferketten zu erwähnen.

eAHV findet, dass auch die Informationstechnologiehersteller der Exekutive zu erwähnen seien, deren Situation hier nicht klar definiert sei.

Economiesuisse vertritt die Meinung, dass die Tatsache, dass die Hersteller im vorliegenden Text erwähnt würden, die Unklarheit in Bezug auf die Instanzen, die der Meldepflicht unterständen, verstärke.

Der SSV macht sich Sorgen bezüglich der Anwendbarkeit dieser Bestimmung, insbesondere weil viele Hardware- und Softwarehersteller keinen Sitz in der Schweiz hätten.

Swico schlägt vor, die Ziffern 1–4 aus der Bestimmung zu streichen und stattdessen den Begriff «Fernwartungszugang» zu definieren, um damit auch die Lieferkettenproblematik zu lösen.

SwissICT verlangt hier eine Präzisierung, dass die Hersteller, die Software als Dienstleistung (SaaS) anbieten, keine kritischen Infrastrukturen betreiben.

Swissmem verlangt die Streichung von Artikel 74*b* Buchstabe s.

3.3.2.11 Artikel 74*c* Ausnahmen von der Meldepflicht

Der Bundesrat nimmt bestimmte Kategorien von Betreiberinnen von kritischen Infrastrukturen von der Meldepflicht aus, wenn durch Cyberangriffe auf ihre Infrastrukturen ausgelöste Funktionsausfälle oder Fehlfunktionen:

a. unwahrscheinlich sind, insbesondere wegen einer geringen Abhängigkeit von Informatikmitteln; oder
b. nur geringe Auswirkungen auf das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung haben, insbesondere, weil sie:
   1. nur eine geringe Anzahl Personen betreffen,
   2. von anderen kritischen Infrastrukturen aufgefangen werden, oder
   3. nur ein geringes volkswirtschaftliches Schadenspotenzial haben.

Insgesamt 20 Vernehmlassungsteilnehmende haben sich zu den Ausnahmen geäussert. Es handelte sich dabei mehrheitlich um allgemeine Bemerkungen und um viele Anträge zur Anpassung der Formulierung dieses Artikels. Nur 5 Vernehmlassungsteilnehmende haben sich gegen die Aufnahme der Bestimmung in das Gesetz ausgesprochen.

❖ **Allgemeine Bemerkungen zu Artikel 74*c***

Swiss Banking beantragt, dass dieser Artikel wie folgt geändert wird: «Der Bundesrat legt auf Verordnungsstufe klare Kriterien fest, anhand derer die Infrastrukturen meldepflichtig werden. Sinn dieser Kriterien ist es, jene Betreiberinnen kritischer Infrastrukturen von der Meldepflicht auszunehmen, bei denen durch Cyberangriffe ausgelöste Funktionsausfälle oder Fehlfunktionen …».

SuisseDigital verlangt, dass die Ausnahmebestimmungen präziser definiert werden.

Swico erachtet die in diesem Artikel erwähnten Kriterien als schwer umsetzbar und beantragt, sie durch folgendes Kriterium zu ersetzen: «das Ausmass des Einflusses einer Beeinträchtigung». Zudem würde **Swico** dem vorliegenden Artikel einen weiteren Buchstaben hinzufügen: «c. weil mitigierende Massnahmen solche Cyberangriffe unschädlich machen».

VUD hält die Bestimmungen von Artikel 74*c* Buchstaben a und b für widersprüchlich oder unklar und verlangt eine Präzisierung, insbesondere für folgende Sätze: «… wegen einer geringen Abhängigkeit von Informatikmitteln …» und «… nur geringe Auswirkungen auf das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung haben …».

Der Kanton BE beantragt das Einfügen einer zusätzlichen Bestimmung in den vorliegenden Text:
« Art. 74c^{bis} Bestimmungen des kantonalen Rechts
Die Kantone können
a. nach Anhörung des NCSC unter den Voraussetzungen des Artikels 74c kantonale oder kommunale Behörden oder Träger öffentlicher Aufgaben von der Meldepflicht ausnehmen,
b. die für die Meldung verantwortlichen Personen der kantonalen oder kommunalen Behörden oder Träger öffentlicher Aufgaben bestimmen.»

Migros bedauert das Fehlen einer risikobasierten Regelung.

Der Kanton LU und Switch beantragen, dass die kleinen Organisationen von der Meldepflicht befreit werden, da dieser Prozess laut dem **Kanton LU** zu kostenintensiv ist.

- **Zustimmung zu Artikel 74*c***

eGov-Schweiz und die Kantone AI und NW erachten diesen Artikel als angemessen.

- **Ablehnung von Artikel 74*c***

Die Grünen, CH++, Operation Libero sowie die Kantone TG und UR verlangen die Streichung dieses Artikels.

- **Änderungsanträge und Anregungen zu Artikel 74*c***

- **<u>Buchstabe a</u>**

Den Grünen, Operation Libero und Pour Demain zufolge scheint im 21. Jahrhundert eine geringe Abhängigkeit von Informatikmitteln immer weniger wahrscheinlich zu sein. Buchstabe a sei daher zu streichen.

Der Kanton GE vertritt die Meinung, dass diese Bestimmung im Widerspruch zum Datenschutzgesetz stehe.

- **<u>Buchstabe b</u>**

Laut **VUD** ist einzig und allein ausschlaggebend, ob ein Cyberangriff die nationale Sicherheit stark beeinträchtigt.

Dem Kanton GE zufolge widerspricht diese Bestimmung dem Zweck von Artikel 74*b,* der die Organisationen mit grosser Bedeutung aufführt.

Migros erachtet die in Buchstabe b vorgesehene Ausnahme als nicht praktikabel.

3.3.2.12 Artikel 74*d* Zu meldende Cyberangriffe

[1] Ein Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass:

a. die Funktionsfähigkeit der betroffenen kritischen Infrastruktur oder einer anderen kritischen Infrastruktur gefährdet ist;
b. ein fremder Staat ihn ausgeführt oder veranlasst hat;
c. er zu einem Abfluss oder zur Manipulation von Informationen geführt hat oder führen könnte; oder
d. er länger als 30 Tage unentdeckt blieb.

[2] Ein Cyberangriff auf eine kritische Infrastruktur muss immer gemeldet werden, wenn er mit Erpressung, Drohung oder Nötigung gegenüber der Betreiberin einer kritischen Infrastruktur oder ihren Mitarbeitenden verbunden ist.

Die Definition der zu meldenden Cyberangriffe hat viele Reaktionen hervorgerufen, hauptsächlich allgemeine Bemerkungen oder konkrete Änderungsanträge.
Insgesamt 36 Teilnehmende haben sich geäussert, wovon sich 1 Stelle ausdrücklich für die Einführung dieser Gesetzesbestimmung ausgesprochen hat. 4 Teilnehmende lehnen den Artikel hingegen klar ab.

- **Allgemeine Bemerkungen zu Artikel 74*d***

AEROSUISSE erachtet es für die Rechtssicherheit der betroffenen Unternehmen als notwendig, klar festzulegen, dass Artikel 74*d* als Kriterium definiert, wann ein Angriff auf eine kritische Infrastruktur gemeldet werden muss.

Economiesuisse, eGov-Schweiz, der Kanton ZH, SuisseDigital und Santésuisse finden, dass dieser Artikel zwingend überarbeitet werden müsse, insbesondere weil die Kriterien zu weit gefasst und für die Unternehmen nur schwer fassbar oder anwendbar seien. So wäre es **economiesuisse** zufolge sinnvoller, eine kürzere (Positiv-)Liste der zu meldenden Vorfälle zur Verfügung zu stellen und die Meldepflicht auf erfolgreiche oder besonders schwerwiegende Versuche zu beschränken.

Der **Kanton GR** verlangt eine klare Liste der zu meldenden Fälle.

ISSS, Härting Rechtsanwälte und UniZH/UNIL NFP 77 fordern einen anderen Titel für diesen Artikel: «Zu meldende Cyberangriffe – und Vorfälle»

Privatim spricht sich für eine präzisere Definition aus, was unter «schwerwiegend» zu verstehen sei, vor allem da hier implizit gemeint sei, dass Vorfälle gemeldet werden müssten, auch wenn ihr Schweregrad noch nicht ermittelt werden könne. Sollte das NCSC also feststellen, dass es sich nicht um einen schwerwiegenden Sicherheitsvorfall handelt und keine Zustimmung der betreffenden Person(en) vorliegt, müssten die Personendaten unverzüglich gelöscht oder anonym verarbeitet werden.

Scienceindustries verlangt, im Text explizit anzugeben, dass sich die Meldepflicht auf Angriffe auf Anlagen in der Schweiz beschränkt und keine Anlagen im Ausland betrifft. **UniZH/UNIL NFP 77** fordern hingegen, dass diese Bestimmung auch die Anlagen im Ausland abdeckt.

Coop ist der Meinung, dass die vorgeschlagene Definition zu allgemein sei und keine klare Unterscheidung zulasse zwischen Vorfällen, die sich nicht oder nur wenig auf die Geschäftstätigkeit auswirkten, und solchen, die direkt den Betrieb kritischer Infrastrukturen betreffen oder ein hohes Risiko darstellen würden. Zudem sei nicht klar, welche der erfolgreichen oder fehlgeschlagenen Cyberangriffe zu melden seien.

Der Flughafen ZH fordert, nur erfolgreiche Cyberangriffe der Meldepflicht zu unterstellen.

Laut dem **Kanton AG** sollte das NCSC die Triage der zu meldenden Angriffe vornehmen. Denn auch «unwichtige» Meldungen könnten sich als wichtig erweisen.

❖ Zustimmung zu Artikel 74*d*

Der **VSE** spricht sich für diese Bestimmung aus.

❖ Ablehnung von Artikel 74*d*

Swiss Banking und Raiffeisen beantragen die Streichung dieses Artikels und schlagen vor, ihn durch einen mit der Formulierung der FINMA kompatiblen Wortlaut zu ersetzen: «Zu melden sind Cyberangriffe mit erheblichen Auswirkungen auf die Geschäftstätigkeit des Unternehmens, insbesondere erfolgreiche oder teilweise erfolgreiche Angriffe auf kritische Funktionen, deren Ausfall oder Störung den Schutz der Kundinnen und Kunden oder das Funktionieren der Märkte stark beeinträchtigen würde.»

SwissICT fordert die Streichung dieser Bestimmung, da praktisch jeder Cyberangriff zu melden sei.

VUD zufolge ist die gesetzgeberische Lösung, wonach die zu meldenden Ereignisse breit gefasst werden (Art. 5 Bst. d und e ISG), nur um die Meldepflicht danach wieder zu begrenzen (Art. 74*d* ISG), abzulehnen und der Artikel zu streichen.

❖ Änderungsanträge und Anregungen zu Artikel 74*d*

- **<u>Zu Absatz 1</u>**

Laut **ISSS** widerspricht die Tatsache, dass die Anzeichen für einen Cyberangriff gemäss Artikel 74*d* bereits der Meldepflicht unterstehen, der *ratio legis.* Die vorliegende Bestimmung sei wie folgt zu ändern: «[1] Ein Cyberangriff oder ein Cybervorfall auf eine kritische Infrastruktur muss gemeldet werden, wenn die ernsten Befürchtungen bestehen, dass:».

- **<u>Zu Absatz 1 Buchstabe a</u>**

Swissmem fordert, diese Bestimmung wie folgt zu ersetzen: «die Funktionsfähigkeit der betroffenen kritischen Infrastruktur oder einer anderen kritischen Infrastruktur wesentlich gefährdet ist;».

Da die Unternehmen häufig nicht in der Lage seien, eine Bedrohung zu beurteilen, sind **die Flughäfen GE und ZH, Swissgrid, santésuisse sowie der Kanton GE** der Ansicht, dass der folgende Text zu streichen sei: «oder einer anderen kritischen Infrastruktur».

- **<u>Zu Absatz 1 Buchstabe b</u>**

Economiesuisse, Coop, IG eHealth, Switch, der Kanton TG, ISSS, der Flughafen ZH, Axpo, UniZH/UNIL NFP 77, Scienceindustries, VUD, VöV und RAILplus stellen die Relevanz dieser zweiten Bedingung infrage, weil Cyberangriffe, die von Staaten ausgingen, häufig zu komplex seien, um überhaupt erkannt zu werden, und ihre Zuordnung ein politisches und kompliziertes Vorgehen darstelle. Daher beantragen **ISSS, Flughafen ZH, Axpo, UniZH/UNIL NFP 77, Scienceindustries, VUD, VöV und RAILplus** die Streichung dieser Bedingung. **RAILplus** schlägt vor, sie durch ein kumulatives Kriterium im Zusammenhang mit den Auswirkungen zu ersetzen (Beispiel: «Anzahl betroffener Nutzender oder Systeme»).

- **<u>Zu Absatz 1 Buchstabe c</u>**

Swissgrid ist der Meinung, dass die folgenden Punkte weiter ausgeführt werden müssten: «besonders schützenswerte Personendaten», «Informationen zu den kritischen Systemen», «Daten des Stromnetzbetriebs», «Infrastrukturen» und «Systeme des Kernbetriebs».

- **<u>Zu Absatz 1 Buchstabe d</u>**

Economiesuisse, der Flughafen ZH, SVV, VUD und Coop erachten die Frist von 30 Tagen als nicht sinnvoll.

IG eHealth beantragt, Punkt d (Cyberangriff bleibt länger als 30 Tage unentdeckt) keiner Meldepflicht zu unterstellen, wenn die Punkte a (Funktionsfähigkeit gefährdet) und c (möglicher Abfluss

oder zur Manipulation von Informationen) nicht erfüllt sind, d. h., der Angriff eine Bagatelle war oder einen tiefen bis mittleren Schweregrad aufwies.

Der SVV erachtet die Frist als nicht realistisch, weil dies implizieren würde, dass man auf einen Angriff reagieren müsste, von dem man noch keine Kenntnis habe und von dem man allenfalls nicht wissen könne, wann er eingetreten sei. Der **SVV** schlägt vor, Punkt d wie folgt zu ersetzen: «über einen längeren Zeitraum unentdeckt blieb».
Der Kanton TG beantragt, den vorliegenden Text wie folgt zu ersetzen:
«d. die direkt und unmittelbar für das Ziel des Cyberangriffs verwendeten Instrumente länger als 30 Tage unentdeckt blieben».

Migros sowie UniZH/UNIL NFP 77 zufolge sollte eine Zeitspanne für die «Nicht-Entdeckung» kein Einzel-Kriterium für eine Meldung darstellen.

- **<u>Zu Absatz 2</u>**

Laut **Scienceindustries** ist die Meldepflicht auf Erpressungen, Bedrohungen oder Zwang dahingehend zu beschränken, dass sie nur bei Vorliegen eines Bezuges zur Geschäftstätigkeit wirksam wird.

Der **SSV** ist der Ansicht, dass die abschliessend formulierte Aufzählung die Frage aufwirft, ob die Meldepflicht nicht auch dann gelten solle, wenn ein Cyberangriff mit Erpressung, Drohung oder Nötigung gegenüber Kunden und Kundinnen oder Patienten und Patientinnen einer Betreiberin verbunden sei.

Der Kanton BL beantragt, den Text zu ergänzen und den Tatbestand der Datenbeschädigung, der durch Verschlüsselung oder das Einschleusen von Malware verursacht wird, einzuschliessen.

Der Kanton GE weist darauf hin, dass die Institutionen, die gegen diesen Artikel verstossen, doppelt bestraft werden könnten.

UniZH/UNIL NFP 77 schlagen vor, den Text so zu ändern, dass eine Meldepflicht besteht, sobald «strafrechtlich relevante Handlungen» vorliegen statt nur bei Erpressungen.

3.3.2.13 Artikel 74*e* Inhalt der Meldung

[1] Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten.
[2] Sind zum Zeitpunkt der Meldung nicht alle erforderlichen Informationen bekannt, so ergänzt die Betreiberin der kritischen Infrastruktur die Meldung, sobald sie an neue Informationen gelangt.

15 Vernehmlassungsteilnehmende haben sich zu dieser Bestimmung geäussert. Die meisten Anträge zum Gesetzestext betreffen die Klärung und eine detailliertere Beschreibung der Informationen, die nach Artikel 74*e* verlangt werden.

- ❖ **Allgemeine Bemerkungen zu Artikel 74*e***

Die Grünen sind der Meinung, dass Artikel 74*e* so zu überarbeiten sei, dass eine Automatisierung der Meldungen möglich sei.

Der Verband der Auslandbanken in der Schweiz findet, dass es möglich sein sollte, die Meldungen auf Englisch und in den Amtssprachen zu verfassen.

Economiesuisse fordert, dass die Anforderungen an die Meldung einfach bleiben müssen, um die Hindernisse für die Unternehmen zu minimieren. Zudem müssten die zu meldenden Fälle klar abgegrenzt werden.

SwissICT, die Post sowie die Kantone GR und TG verlangen eine präzisere Beschreibung der im Rahmen von Artikel 74*e* geforderten Informationen, evtl. mithilfe einer Liste.

SwissICT und die Post fordern, dass die gemäss Artikel 74*e* verlangten Informationen mit anderen Behörden abgestimmt werden (z. B. mit der FINMA).

Laut **Axpo** muss die Meldung unabhängig vom Informationsniveau umgehend erfolgen.

❖ **Zustimmung zu Artikel 74*e***

Swiss Banking begrüsst diese Bestimmung.

❖ **Änderungsanträge und Anregungen zu Artikel 74*e***

- **<u>Zu Absatz 1</u>**

ISSS und Härting Rechtsanwälte verlangen, dass die vorliegende Bestimmung wie folgt geändert wird: «Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, des Cybervorfalles, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten».

Der Kanton GE beantragt, «und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur» durch «oder zu den von der betroffenen Einrichtung bereits eingeleiteten Schritten» zu ersetzen.

UniZH/UNIL NFP 77 beantragen ebenfalls eine Änderung der Bestimmung wie folgt: «… oder zu den bereits eingeleiteten oder geplanten Schritten».

- **<u>Zu Absatz 2</u>**

Der Kanton GE beantragt, die vorliegende Bestimmung so zu ändern, dass die Meldung nicht nur durch die Betreiberin zu ergänzen ist, sobald sie an neue Informationen gelangt, sondern auch wenn solche Informationen eingeholt werden können.

3.3.2.14 Artikel 74*f* Übermittlung der Meldung

[1] Für die elektronische Meldung von Cyberangriffen stellt das NCSC ein sicheres System zur Übermittlung der Meldung an das NCSC zur Verfügung.

[2] Das System muss der Betreiberin einer kritischen Infrastruktur ermöglichen, die Meldung des Cyberangriffs oder seiner Auswirkungen gesamthaft oder in Teilen an weitere Stellen und Behörden zu übermitteln.

[3] Benötigt eine Stelle oder Behörde Informationen, die über Art. 74e hinausgehen, kann die Betreiberin diese über das System direkt an die betreffende Stelle oder Behörde übermitteln.

34 Teilnehmende haben sich zum Artikel 74*f* geäussert, wovon 4 (RAILplus, santésuisse, UniBE und die Post) den Text in der vorliegenden Form annehmen. Der Text wurde von keiner Stelle vollumfänglich abgelehnt. Die meisten Diskussionen betrafen die Zentralisierung der Übermittlungskanäle für die Informationen an das NCSC und an die im Gesetz bezeichneten Behörden.

❖ **Allgemeine Bemerkungen zu Artikel 74*f***

CH++ findet, dass in Artikel 74*f* explizit zu erwähnen sei, dass die Datenübermittlung über eine gesicherte Schnittstelle erfolge. Zudem sei ein API-basierter Ansatz, wie er von den Partnernetzwerken von Meta/Facebook oder AT&T erfolgreich praktiziert werde, durch das NCSC weiter zu verfolgen. Diesbezüglich sei eine geeignete Rechtsgrundlage zu schaffen.

Pour Demain und Operation Libero sind der Meinung, dass auch eine Informatikschnittstelle (API) für die Übermittlung automatisierter Meldungen an das NCSC zu erstellen sei.

Der SVV, swissuniversities, der Kanton ZH und Swico fordern, dass die Meldung in einer einfachen Form erfolgen kann.

Der Kanton GR verlangt eine Klarstellung, welche Informationen übermittelt werden, an welche Behörden sie gehen und wer sie einsehen kann.

UniZH/UNIL NFP 77 fordern, dass die Behörden keinen Zugriff auf Informationen haben sollen, die für andere Stellen bestimmt sind.

Swico verlangt einen möglichst freien Meldemechanismus, um etwa automatische Meldungen über RSS- oder API-Feeds oder über den bestehenden Datenaustausch über das System MISP zu ermöglichen, über die viele kritische Infrastrukturen verfügen. Zudem fordert **Swico,** dass der bestehende Kanal für die Übermittlung von Informationen zwischen GovCERT und den kritischen Infrastrukturen weiterhin für die Meldung von Cyberangriffen an das NCSC genutzt werden können sollte.

SwissICT ist der Ansicht, dass die Übermittlung von Informationen an andere Behörden neben dem NCSC nur für die Behörden eine Pflicht sei, nicht aber für die Unternehmen.

Raiffeisen begrüsst diese Bestimmung und wünscht die Ergänzung um folgenden Absatz: «Dieses System ist auch von den Bundesbehörden zu benutzen, die Meldepflichten im Zusammenhang von Cyberangriffen etablieren.»

Swissgrid verlangt, dass das System eine gleichzeitige Übermittlung von Meldedaten an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) erlaubt.

Switch fordert, dass die Meldungen ebenfalls über eine gemeinsame Sektor-CERT erfolgen können. Da dies vom Gesetz nicht explizit ausgeschlossen werde, gehe **Switch** davon aus, dass die betreffenden Organisationen die Freiheit hätten, sich entsprechend zu organisieren.

- **Zustimmung zu Artikel 74*f***

RAILplus, santésuisse, UniBE und die Post begrüssen den vorliegenden Text, insbesondere die Möglichkeit, Informationen über eine gesicherte Plattform zu übermitteln, die den höchsten Sicherheitsstandards entspricht, sowie die Tatsache, dass auch andere Mittel für die Meldung verwendet werden können, namentlich das bestehende Formular des NCSC, E-Mail oder Telefon.

- **Änderungsanträge und Anregungen zu Artikel 74*f***

- **<u>Zu Absatz 1</u>**

Der Kanton GE fordert, dass auf die Kostenlosigkeit des Systems hingewiesen wird.

- **<u>Zu Absatz 2</u>**

Der Verband der Auslandbanken in der Schweiz, Swiss Banking, die Grünen, CH++, asut, ISSS und GLP vertreten die Ansicht, dass bei der Umsetzung sicherzustellen sei, dass die Meldepflichten, die sich überlappen würden (DSG, FINMA usw.), durch ein einziges Meldeverfahren abgedeckt werden müssten. **GLP, VSE, digitalswitzerland, economiesuisse und die Digitale Gesellschaft** gehen noch weiter und schlagen die Einrichtung einer eidgenössischen Meldestelle vor, bei der sämtliche Meldepflichten mit einem einzigen Onlineformular erfüllt werden können.

ISSS und Härting Rechtsanwälte begrüssen die Schaffung einer einzigen Stelle im Rahmen der obigen Bestimmung, verlangen jedoch Klarstellungen, an wen welche Informationen weitergegeben werden dürfen und mit welchem Inhalt. So sei etwa nicht klar, ob Meldungen an das NCSC, die an den EDÖB weitergeleitet würden, ebenfalls unter dem Vorbehalt der Nichtbelastung im Strafverfahren nach Artikel 24 Absatz 6 revDSG fallen würden oder nicht. Da gemäss Artikel 74*g* das NCSC weitere Auskünfte verlangen könne, erweitere dies sodann den Umfang der Kommunikation gegenüber Dritten. Eine solche, oft auch sehr informelle Kommunikation auf technischer

Ebene solle nicht Gegenstand eines Strafverfahrens nach dem revDSG werden können, wenn denn Personendaten involviert seien. Es brauche folglich eine detailliertere Regelung, mit wem welche Informationen geteilt werden könnten und welche Konsequenzen dies haben könne oder eben nicht habe.

UniZH/UNIL NFP 77 weisen darauf hin, dass Artikel 73*c* anzupassen und ein expliziter Verweis aufzunehmen sei, wenn effektiv die Absicht bestehe, Artikel 73*c* Absätze 1, 2 und 3 E-ISG auf die Meldungen von Cyberangriffen anzuwenden. Dies diene dazu, dass das NCSC die Informationen bei Fällen gemäss Artikel 73*c* Absätze 1 und 2 rechtmässig an andere Behörden weiterleiten dürfe.

- **Zu Absatz 3**

ISSS und Härting Rechtsanwälte verlangen, dass dieser Absatz gestrichen wird, um sicherzustellen, dass andere Stellen und Behörden nur die Informationen erhalten, die sie rechtlich erhalten dürfen oder die im Rahmen des Zwecks der zugrunde liegenden Gesetzgebung gerechtfertigt sind.

Der Kanton GE beantragt, dass der Absatz verdeutlicht, dass die Stelle oder Behörde die betreffenden Informationen «berechtigterweise» benötigt.

3.3.2.15 Artikel 74*g* Auskunftspflicht

Die Betreiberin der kritischen Infrastruktur muss dem NCSC ergänzende Auskünfte zu den Inhalten der Meldung nach Artikel 74*e* erteilen, die es zur Erfüllung seiner Aufgaben in Bezug auf die Abwehr weiterer Cyberangriffe auf kritische Infrastrukturen benötigt.

9 Vernehmlassungsteilnehmende haben sich zu diesem Artikel geäussert; keiner hat dem Artikel in der vorliegenden Form zugestimmt.

- **Allgemeine Bemerkungen zu Artikel 74*g***

Laut **ISSS und Härting Rechtsanwälte** erweitert diese Bestimmung den Umfang der Kommunikation gegenüber Dritten. Es sei daher festzulegen, wie weit eine Auskunftspflicht gehen könne.

Scienceindustries ist der Meinung, dass die ergänzenden Auskünfte, die das NCSC einfordern dürfe, klar festzulegen sind.

SwissICT vertritt die Ansicht, dass die ergänzenden Informationen während eines Angriffs nur dann eingeholt werden dürften, wenn dies für die Sicherheit der jeweiligen Versorgung zwingend notwendig sei, um die Unternehmen, Institutionen, Behörden und Gemeinden in schwierigen Zeiten nicht noch mehr zu belasten.

Der **Kanton TG** verlangt eine nuanciertere Formulierung dieses Artikels, um es den Kantonen zu erlauben, auch ihre eigenen IT-Sicherheits-Richtlinien einzuhalten.

UniBE fordert Klarstellungen in Bezug auf die Erwartungen hinsichtlich des Inhalts und der zeitlichen Vorstellungen im Zusammenhang mit dieser Pflicht.

- **Ablehnung von Artikel 74*g***

VUD erachtet diese Bestimmung als zu vage und würde sie ersatzlos streichen, da der Inhalt dieser Meldung in Artikel 74*e* schon abschliessend geregelt sei.

- **Änderungsanträge und Anregungen zu Artikel 74*g***

Scienceindustries beantragt, die Bestimmung wie folgt zu ändern: « … kritischen Infrastruktur erteilt, wenn möglich, dem NCSC ergänzende Auskünfte zu den Inhalten der Meldung nach Artikel 74*e*, die ...».

Der **Kanton GE** verlangt, dass die Auskünfte dem NCSC «sobald wie möglich» zu erteilen seien.

3.3.2.16 Artikel 74*h* Verletzung der Melde- oder Auskunftspflicht

[1] Bestehen Anzeichen für eine Verletzung der Melde- oder Auskunftspflicht, so informiert das NCSC die Betreiberin der kritischen Infrastruktur darüber.

[2] Kommt die Betreiberin trotz dieser Information ihrer Pflicht nicht nach, so erlässt das NCSC eine Verfügung über die umzusetzenden Pflichten, setzt ihr darin eine Frist und verweist auf die Bussandrohung nach Artikel 74*i*.

Nur 4 Vernehmlassungsteilnehmende haben sich mit der Frage der Verletzung der Melde- oder der Auskunftspflicht auseinandergesetzt.

❖ Zustimmung zu Artikel 74*h*

Centre Patronal begrüsst den vorliegenden Gesetzestext.

❖ Ablehnung von Artikel 74*h*

Scienceindustries, Flughafen GE und **Digitalswitzerland** sprechen sich gegen diesen Artikel aus, da eine Meldepflicht ihrer Meinung nach ein Unternehmen dazu bringen könnte, gegen die Datenschutzgesetzgebung im Land, wo es seinen Sitz hat, zu verstossen oder die Auskunftspflicht in der Schweiz zu verletzen.

❖ Änderungsanträge und Anregungen zu Artikel 74*g*

UniZH/UNIL NFP 77 verlangt, dass dieser Artikel den betreffenden Institutionen das rechtliche Gehör gewähren muss.

3.3.2.17 Artikel 74*i* Widerhandlungen gegen Verfügungen des NCSC

[1] Mit Busse bis zu 100 000 Franken wird bestraft, wer einer vom NCSC unter Hinweis auf die Strafdrohung dieses Artikels erlassenen rechtskräftigen Verfügung oder dem Entscheid einer Rechtsmittelinstanz vorsätzlich nicht Folge leistet.

[2] Bei Widerhandlungen in Geschäftsbetrieben ist Artikel 6 des Bundesgesetzes vom 22. März 1974[3] über das Verwaltungsstrafrecht (VStrR) anwendbar.

[3] Fällt eine Busse von höchstens 20 000 Franken in Betracht und würde die Ermittlung der nach Artikel 6 VStrR strafbaren Personen Untersuchungsmassnahmen bedingen, die im Hinblick auf die verwirkte Strafe unverhältnismässig wären, so kann die Behörde von einer Verfolgung dieser Personen absehen und an ihrer Stelle den Geschäftsbetrieb zur Bezahlung der Busse verurteilen.

[4] Bei einer Widerhandlung gegen eine Verfügung des NCSC obliegt die Verfolgung und die Beurteilung den Kantonen.

30 der Vernehmlassungsteilnehmenden haben sich zu diesem Artikel geäussert, 13 davon haben die Streichung beantragt.

❖ Allgemeine Bemerkungen zu Artikel 74*i*

Den Grünen und CH++ zufolge soll der Artikel die Tatsache, dass die vorgesehenen Sanktionen auf Ebene der Leitung der Organisationen und nicht auf Ebene der Fachpersonen zum Tragen kommen, expliziter erläutern.

RAILplus schlägt vor, dass nur juristische Personen bestraft werden können sollten (unabhängig von der Höhe der Sanktion). Zudem verlangt **RAILplus,** dass die Situationen geregelt werden, in denen die Subunternehmer im Ausland ansässig sind.

[3] SR **313.0**

Die Piratenpartei und der Kanton GE erklären, dass der Gesetzgeber zur Sicherstellung verhältnismässiger Bussen die Abstufung im Verhältnis zum Umsatz des Unternehmens festlegen müsse (z. B. 4 % des Jahresumsatzes).

Die SP erachtet die Massnahmen in Artikel 74*i* als sinnvoll. Allerdings sei nach fünf Jahren zu prüfen, ob die in Artikel 74*i* genannten Sanktionsmöglichkeiten ausreichen würden und ob die Grundsätze der Gleichbehandlung und der Verhältnismässigkeit eingehalten worden seien.

Die Kantone SO und UR verlangen, dass eine Busse erst nach (schriftlicher) Konsultation des NCSC mit dem Urheber des Verstosses ausgesprochen wird.

UniZH/UNIL NFP 77 erachten die Höhe der Busse nicht als abschreckend, insbesondere im Vergleich zur Höhe gemäss DSG.

❖ **Ablehnung von Artikel 74*i***

AEROSUISSE, die Post, Raiffeisen, Swisscom, Sunrise, Switch, Coop, asut, economiesuisse, SuisseDigital, Scienceindustries, digitalswitzerland, Swico, ISSS, Härting Rechtsanwälte, Swiss Banking, Flughfen GE und Helvetia Versicherungen erachten die Durchsetzung der neuen Pflichten durch Strafbestimmungen als nicht sinnvoll und lehnen diese prinzipiell ab.

Des Weiteren sind **scienceindustries, die Kantone SO und TG, VöV und SGV** der Meinung, dass der Höchstbetrag der verhängten Bussen auf administrativer Ebene eine Gefahr für die Existenz darstelle, weil übertrieben hohe und unverhältnismässige Bussen drohen würden, besonders für kleine und mittelgrosse Unternehmen.

❖ **Änderungsanträge und Anregungen zu Artikel 74*i***

- **<u>Zu Absatz 1</u>**

Der VöV beantragt, den Text wie folgt zu ändern: «Mit Busse bis zu [*10 000*] Franken wird bestraft …».

- **<u>Zu Absatz 3</u>**

SwissICT findet, dass der Betrag von CHF 20 000 auf CHF 50 000 angehoben werden müsse. Einerseits würde dies in unwichtigen Fällen unverhältnismässige Ermittlungskosten vermeiden und andererseits würde dies es erlauben, sich im Rahmen von Artikel 64 Absatz 2 revDSG zu bewegen.

Der VöV beantragt, den Text wie folgt zu ändern: «Fällt eine Busse von höchstens [*5000*] Franken in Betracht ...».

3.3.2.18 Artikel 75 Bearbeitung von Personendaten

[1] Das NCSC kann zur Erfüllung seiner Aufgaben Personendaten bearbeiten, einschliesslich Adressierungselementen nach Artikel 3 Buchstabe f FMG[4] und damit zusammenhängenden besonders schützenswerte Personendaten, die Informationen enthalten über:

a. religiöse, weltanschauliche oder politische Ansichten enthalten; die Bearbeitung ist nur zulässig, wenn sie für die Bewertung von konkreten Bedrohungen und Gefahren im Bereich der Cybersicherheit erforderlich ist;

b. administrative oder strafrechtliche Verfolgungen und Sanktionen enthalten.

4 SR **784.10**

[2] Es kann die Personendaten bearbeiten, ohne dass dies für die betroffenen Personen erkennbar ist, falls sonst der Zweck der Bearbeitung gefährdet wäre oder die Information der betroffenen Person nur mit unverhältnismässigem Aufwand erreicht werden könnte.

[3] Liegen konkrete Hinweise auf den Missbrauch einer Identität oder auf die unberechtigte Verwendung von Adressierungselementen vor, so informiert es die Personen, deren Identität oder Adressierungselemente missbraucht werden; vorbehalten bleiben die Artikel 18a Absatz 4 Buchstabe b und 18b DSG[5].

Keine der befragten Instanzen wollte den Artikel in seiner jetzigen Form beibehalten.

❖ **Allgemeine Bemerkungen zu Artikel 75**

Privatim spricht sich für diesen Artikel aus, fragt sich aber, ob die Verarbeitung mit anonymisierten Daten erfolgen soll, wenn Daten ohne Personenbezug ausreichen.

Scienceindustries fordert, dass mögliche Konflikte mit der ausländischen Datenschutzgesetzgebung bei der Übermittlung von Personendaten berücksichtigt und rechtlich geregelt werden.

Die Post verlangt, dass die Verarbeitung vertraulicher Daten genauer geregelt wird, damit die Vertraulichkeit der Meldungen gewährleistet ist.

Swisscom und die Post verlangen im Zuge der vorliegenden Revision des ISG die Einführung einer Ausnahmeregelung, die im Sinne eines *lex specialis* Vorrang vor dem Öffentlichkeitsprinzip nach BGÖ hat.

Raiffeisen ist der Ansicht, dass die Meldungen gemäss der neuen Regelung das Berufsgeheimnis wahren müssten, und schlägt vor, einen Absatz hinzuzufügen: «Weitergegebene Informationen sind durch die Empfängerbehörde vertraulich zu behandeln. Sie dürfen nicht weitergegeben werden, wenn dadurch die Sicherheit des betroffenen Unternehmens oder der betroffenen Personen gefährdet würde.»

❖ **Ablehnung von Artikel 75**

Der **Kanton TG** vertritt die Meinung, dass das NCSC keinen Zugang zu Personendaten haben solle, und lehnt diesen Artikel daher ab.

❖ **Änderungsanträge und Anregungen zu Artikel 75**

- **<u>Zu Absatz 1</u>**

Egov-Schweiz findet, dass die Kompetenzen zur Bearbeitung von besonders schützenswerten Personendaten durch das NCSC gemäss Artikel 75, insbesondere in Verbindung mit den Möglichkeiten der Weitergabe im In- und im Ausland gemäss den Artikeln 76 und 77, problematisch seien. **Egov-Schweiz** geht daher davon aus, dass das NCSC bei Bedarf polizeiliche und geheimdienstliche Unterstützung herbeizieht und keine eigene Bearbeitung anstrebt.

Da das NCSC nicht die Aufgaben des NDB übernimmt und keine Strafverfolgungsbehörde ist, scheint **privatim** zufolge das Volumen an Personendaten, das gemäss Artikel 75 E-ISG verarbeitet wird, ohne weitere Beschränkungen (insbesondere über die unbedingte Notwendigkeit, die Aufgaben zu erfüllen) nicht verhältnismässig. **Privatim** empfiehlt, die erforderlichen Einschränkungen vorzusehen.

- **<u>Zu Absatz 1 Buchstabe a</u>**

Der Kanton GR fordert die Streichung dieser Bestimmung.

5 SR **235.1**

Die GLP kritisiert den Umfang der Personendaten, die das NCSC gemäss dem Vorentwurf verarbeiten darf, und verlangt, dass die Weitergabe besonders schützenswerter Daten zwischen NCSC, Strafverfolgungsbehörden und dem NDB spezifiziert wird. Hinzu komme, dass momentan keine besondere Aufsicht vorgesehen sei. Es sei daher nicht gewährleistet, dass diese Daten nicht missbräuchlich genutzt würden.

- **Zu Absatz 2**

Privatim findet, dass die Verteilung der Kompetenzen zwischen dem NCSC, den Strafverfolgungsbehörden und dem NDB deutlich mehr Aufmerksamkeit verdiene. Daher müsse Artikel 75 Absatz 2 ISG (Bearbeitung von Personendaten, ohne dass dies für die betroffenen Personen ersichtlich sei) auf laufende Strafverfahren beschränkt werden.

- **Zu Absatz 3**

Migros gibt an, dass die vorliegende Bestimmung mit den Bestimmungen von Artikel 24 revDSG in Einklang zu bringen sei.

3.3.2.19 Artikel 76 Zusammenarbeit im Inland

[1] Das NCSC kann den Betreiberinnen von kritischen Infrastrukturen Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

[2] Die Betreiberinnen von kritischen Infrastrukturen können dem NCSC Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

[3] Das NCSC kann den Fernmeldedienstanbieterinnen Adressierungselemente und damit zusammenhängende Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

[4] Die Fernmeldedienstanbieterinnen können dem NCSC Adressierungselemente und damit zusammenhängende Personendaten bekanntgeben, sofern dies zum Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

7 Teilnehmende haben sich zu diesem Gesetzestext geäussert.

❖ **Allgemeine Bemerkungen zu Artikel 76**

Scienceindustries ist der Meinung, dass zumindest in den Absätzen 1 und 2 einschränkend vorzusehen sei, dass die Weitergabe solcher Informationen, speziell an Mitbewerber in ähnlichen Märkten nicht ohne Zustimmung des Dateninhabers erfolgen dürfe.

Swico betont, wie wichtig die Beibehaltung der bereits bestehenden Kommunikationskanäle zwischen dem NCSC, den kritischen Infrastrukturen und weiteren Parteien sei.

VöV verlangt, dass das Verhältnis der Bestimmungen von Artikel 76 Absatz 1 zu Artikel 73*b* Absatz 2 sowie Artikel 73*c* so klargestellt wird, dass das NCSC den Betreiberinnen kritischer Infrastrukturen die Personendaten nur unter der Bedingung bekanntgibt, dass dies für den Schutz von kritischen Infrastrukturen vor Cyberrisiken erforderlich ist.

Der Kanton GE bittet um Klärung, ob es sich im vorliegenden Text um kritische Infrastrukturen im Sinne von Artikel 74*b* mit den (oder ohne die) Ausnahmen von Artikel 74*c* handele. Zudem verlangt **der Kanton GE** die Erwähnung des EDÖB.

❖ **Änderungsanträge und Anregungen zu Artikel 76**

- **Zu Absatz 1**

UniZH/UNIL NFP 77 beantragen, im französischen Text «utiles» durch «nécessaires» zu ersetzen.

- **Zu Absatz 2**

ISSS beantragt, den Text wie folgt anzupassen: «… sofern dies zum Schutz [*ihrer*] kritischen Infrastrukturen …».

- **Zu Absatz 3**

ISSS beantragt, den Text wie folgt anzupassen: «… Fernmeldedienstanbieterinnen[, *die nicht kritische Infrastrukturanbieterinnen sind*,] Adressierungselemente …».

- **Zu Absatz 4**

ISSS beantragt, den Text wie folgt anzupassen: «… Fernmeldedienstanbieterinnen[, *die nicht kritische Infrastrukturanbieterinnen sind,*] können dem NCSC Adressierungselemente …».

Nach **UniZH/UNIL NFP 77** sollte der Text eher vorsehen, dass die Fernmeldedienstanbieterinnen dem NCSC Personendaten, einschliesslich Adressierungselementen, bekanntgeben könnten.

3.3.2.20 Artikel 76*a* Unterstützung für Behörden

[1] Das NCSC unterstützt den NDB beim frühzeitigen Erkennen und Verhindern von Bedrohungen der inneren oder äusseren Sicherheit, bei der Beurteilung der Bedrohungslage und bei der nachrichtendienstlichen Frühwarnung zum Schutz von kritischen Infrastrukturen nach Artikel 6 Absätze 1 Buchstabe a, 2 und 5 NDG6 mit Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie technischen Analysen von Cyberrisiken.

[2] Es gewährt dem NDB Zugriff auf Informationen im Abrufverfahren, die Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben.

[3] Es gewährt den Strafverfolgungsbehörden Zugriff auf Informationen im Abrufverfahren, die Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben.

[4] Es kann den kantonalen Stellen, die für die Cybersicherheit zuständig sind, Zugriff auf Informationen im Abrufverfahren gewähren, die für den Schutz kantonaler Behörden und kantonaler kritischer Infrastrukturen vor Cyberrisiken erforderlich sind.

7 Vernehmlassungsteilnehmende haben sich zur Unterstützung für Behörden geäussert.

❖ Allgemeine Bemerkungen zu Artikel 76*a*

Der Kanton UR fordert, dass Informationen zur Identität und zur Vorgehensweise der Angreifenden vollumfänglich übermittelt werden dürfen.

Der Kanton NW findet, dass die mit den NDB geteilten Informationen ebenfalls allen Strafverfolgungsbehörden zur Verfügung gestellt werden müssten.

Der Kanton ZG ist der Meinung, dass der Kreis der Adressaten der Auswertungen und der technischen Analysen auf die Strafverfolgungsbehörden auszudehnen sei.

❖ Zustimmung zu Artikel 76*a*

Swiss Banking spricht sich für diese Regelung aus.

❖ Änderungsanträge und Anregungen zu Artikel 76*a*

- **Zu Absatz 2**

Der VöV beantragt, den Text wie folgt anzupassen: «… Abrufverfahren, [*die ausschliesslich*] Aufschluss ...».

6 SR **121**

- **Zu Absatz 3**

Der VöV beantragt, den Text wie folgt anzupassen: «… Abrufverfahren, [*die ausschliesslich*] Aufschluss ...».

Der Kanton BE beantragt die Streichung dieser Bestimmung, sollte Artikel 73*c* gestrichen werden.

Laut **privatim** muss der Zugang im Abrufverfahren zu den Informationen, die das NCSC im Rahmen der Meldepflicht erhält, für den NDB (Art. 76*a* Abs. 2 ISG), für die Strafverfolgungsbehörden (Art. 76*a* Abs. 3 ISG) und für die kantonalen Stellen für Cybersicherheit (Art. 76*a* Abs. 3 ISG) eingeschränkt oder mithilfe eines «Push»-Verfahrens realisiert werden.

- **Zu Absatz 4**

Der Kanton BE beantragt die Streichung dieses Absatzes, sollte Artikel 73*c* gestrichen werden.

3.3.2.21 Artikel 77 Internationale Zusammenarbeit

[1] Das NCSC kann mit ausländischen und internationalen Stellen, die für die Cybersicherheit zuständig sind, Informationen austauschen, wenn sie diese zur Erfüllung von Aufgaben benötigen, die denjenigen des NCSC entsprechen. Umfasst der Informationsaustausch auch Personendaten nach Artikel 75, ist Artikel 6 DSG[7] zu beachten.
[2] Der Informationsaustausch nach Absatz 1 ist nur dann zulässig, wenn die ausländischen und internationalen Stellen die bestimmungsgemässe Verwendung gewährleisten.
[3] Werden die Informationen für ein rechtliches Verfahren im Ausland benötigt, so gelten die Bestimmungen über die Amts- und Rechtshilfe.

7 Vernehmlassungsteilnehmende haben sich zur Frage der internationalen Zusammenarbeit geäussert. Niemand hat diese Bestimmung abgelehnt.

❖ Allgemeine Bemerkungen zu Artikel 77

Swiss Banking unterstützt Artikel 77, wenn die Informationen für die Bekämpfung von Cyberrisiken und insbesondere für die Zwecke dieses Gesetzes nötig sind (eine in Art. 77 Abs. 1 erster Satz ausdrücklich vorgesehene und begrüssenswerte Einschränkung). Wenn Personendaten im Sinne von Artikel 75 involviert seien, sei bei deren Übermittlung ins Ausland Artikel 6 DSG zu beachten.

Scienceindustries steht der Weitergabe von vertraulichen Daten, insbesondere von Personendaten, kritisch gegenüber. Es wäre sinnvoll, hier zumindest mit Gültigkeit für die Absätze 1, 2 und 3 einschränkend vorzusehen, dass die Weitergabe solcher Informationen nicht ohne die Zustimmung des Dateninhabers erfolgen dürfe.

VUD fordert, dass der Informationsaustausch mit ausländischen Behörden gemäss Artikel 77 ISG streng anonym erfolgt.

Laut **BA** sollte sich dieser Gesetzestext in den Rahmen der bereits bestehenden Bestimmungen zur internationalen Zusammenarbeit einfügen, insbesondere im Bereich der Rechtshilfe.

❖ Änderungsanträge und Anregungen zu Artikel 77

- **Zu Absatz 1**

Der VöV hält das Verhältnis der Bestimmungen von Artikel 77 Absatz 1 zu Artikel 73*b* Absatz 2 und Artikel 73*c* für unklar und verlangt folglich, dass der Text wie folgt angepasst wird: «… nach Art. 75, [*sind Artikel 73b Abs. 2 und 73c sowie*] Artikel 6 DSG zu beachten».

7 SR **235.1**

Privatim begrüsst diesen Absatz.

ISSS beantragt, den Text wie folgt anzupassen: «… Artikel 75, ist Artikel 6 [*und Art. 10a DSG*] zu beachten ...».

- **Zu Absatz 2**

Damit beim Informationsaustausch gewährleistet sei, dass die ausländische Schwesterbehörde die erhaltenen Informationen für den Zweck der Bekämpfung von Cyberrisiken verwende, schlägt **Swiss Banking** vor, die Regelung wie folgt zu ergänzen: «Weitergegebene Informationen sind durch die Empfängerbehörde vertraulich zu behandeln. Sie dürfen nicht weitergegeben werden, wenn dadurch die Sicherheit des betroffenen Unternehmens oder der betroffenen Personen gefährdet würde».

ISSS beantragt, den Text wie folgt anzupassen: «… bestimmungsgemässe [*datenschutzkonforme*] Verwendung …».

- **Zu Absatz 3**

Die BA verlangt, in diesem Text einen Koordinationsmechanismus einzuführen, und schlägt folgende Formulierung vor: «… Amts- und Rechtshilfe. [*Die übermittelten Informationen können zur Substantiierung eines Rechts- oder Amtshilfeersuchens verwendet werden*] …».

Im Wissen, dass das NCSC keine Strafverfolgungsbehörde sei, verlangt **privatim** Präzisierungen in Bezug auf die Bestimmungen, aus denen sich die nationalen Kompetenzen für Amts- und Rechtshilfe ableiten würden.

3.3.2.22 Artikel 79 Abs. 1 (Datenaufbewahrung und -archivierung)

[1] Das NCSC bewahrt Personendaten nur so lange auf, wie dies zur Abwehr von Gefahren oder zur Erkennung von Vorfällen zweckmässig ist, höchstens jedoch fünf Jahre ab der letzten Verwendung; bei besonders schützenswerten Personendaten beträgt die Frist zwei Jahre.

10 Vernehmlassungsteilnehmende haben sich zur Frist für die Aufbewahrung von Personendaten durch das NCSC geäussert.

❖ Allgemeine Bemerkungen zu Artikel 79 Abs. 1

CH++ beantragt, den Begriff «Verwendung» zu präzisieren, z. B. «zwingende Verwendung». Das blosse Öffnen eines Datensatzes könne selbstverständlich nicht zur Verlängerung der erlaubten Aufbewahrungsfrist führen.

VöV, Migros sowie UniZH/UNIL NFP 77 fordern eine Präzisierung des Begriffs «letzte Verwendung».

Laut **ISSS, Härting Rechtsanwälte und privatim** verlangt der Grundsatz der Verhältnismässigkeit, dass die Daten nur so lange aufbewahrt werden, wie dies für die Zweckerfüllung erforderlich ist. Aus den Personendaten könnten anonymisierte Muster generiert werden. **ISSS und Härting Rechtsanwälte** schlagen folgende Umformulierung vor: «… beträgt die Frist [*6 Monate. In anonymisierter Form sowie als erkannte Muster dürfen die aus Personendaten gewonnenen Erkenntnisse unbefristet aufbewahrt werden*]».

Die KKJPD verlangt, die Aufbewahrungsfrist für die Daten an die Artikel 97 und 109 des Schweizerischen Strafgesetzbuches anzupassen.

Der Kanton BE beantragt eine Anpassung dieser Bestimmung, damit die Daten grundsätzlich nicht vor dem Ende der Verfolgungsverjährung der in Frage kommenden Delikte gelöscht werden.

3.3.2.23 Änderungserlasse

Die nachstehenden Erlasse werden wie folgt geändert:

1. Stromversorgungsgesetz vom 23. März 2007[8]

Art. 8a Schutz vor Cyberrisiken

1 Die Netzbetreiber, die Erzeuger und die Speicherbetreiber treffen Massnahmen für einen angemessenen Schutz ihrer Anlagen vor Cyberrisiken.

2 Der Bundesrat kann diese Pflicht auf weitere Beteiligte ausdehnen.

2. Datenschutzgesetz vom 25. September 2020[9]

Art. 24 Abs. 5bis

5bis Der EDÖB kann die Meldung mit dem Einverständnis des meldepflichtigen Verantwortlichen zur Analyse des Vorfalls an das Nationale Zentrum für Cybersicherheit weiterleiten. Die Mitteilung kann Personendaten enthalten, einschliesslich besonders schützenswerter Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen betreffend den meldepflichtigen Verantwortlichen.

Nur 6 Vernehmlassungsteilnehmende haben sich zu den zwei obigen Gesetzestexten geäussert. Keine der befragten Instanzen hat die Streichung von Artikel 8*a* StromVG beantragt. **ISSS und Härting Rechtsanwälte** haben die Streichung von Artikel 24 Absatz 5bis DSG verlangt.

- **Allgemeine Bemerkungen zu Artikel 24 Abs. 5bis Datenschutzgesetz**

Der VöV beantragt, die Bestimmung wie folgt anzupassen: «Der EDÖB kann die Meldung [*ausschliesslich*] mit dem …».

Der **Kanton GE** ist der Meinung, dass die Mitteilung des NCSC an den EDÖB verpflichtend sein sollte; die Mitteilung des EDÖB sollte nicht des Einverständnisses der meldepflichtigen Person bedürfen, wenn die Bedingungen des vorliegenden Gesetzes erfüllt seien.

UniZH/UNIL NFP 77 weisen darauf hin, dass es möglich sein müsse, sämtliche besonders schützenswerten Personendaten zu übermitteln und nicht nur bestimmte.

- **Ablehnung von Artikel 24 Abs. 5bis Datenschutzgesetz**

ISSS und Härting Rechtsanwälte verlangen die Streichung dieser Bestimmung. Denn wenn eine zentrale Stelle geschaffen werde, um alle Meldungen zu registrieren, sei dieser Zusatz nicht mehr notwendig.

3.4 Weitere Anträge und Anregungen zum Vorentwurf

Swiss Banking verlangt, den Gesetzestext an die FINMA-Aufsichtsmitteilung 05/2020 betreffend die Meldepflicht von Cyber-Attacken gemäss Artikel 29 Absatz 2 FINMAG anzupassen.

Die IG eHealth verlangt, dass Bundesrat und Parlament sicherstellen, dass das NCSC ausreichende Personalressourcen erhält.

Der Kanton ZH schlägt vor, die Meldepflicht etappenweise (z. B. sektorweise) einzuführen, um so zuerst Erfahrungen zu sammeln.

Die KKPKS beantragt zu regeln, wie Strafverfolgungsbehörden mit Meldungen umgehen müssen, wenn diese an sie statt ans NCSC gelangen.

8 SR **734.7**
9 SR **235.1,** BBl 2020 7639

Asut, Swisscom und Sunrise verlangen eine gute Koordination der Vorlage mit der Revision der Fernmeldeverordnung.

3.5 Anträge und Anregungen zu Themen ausserhalb der Vorlage

CH++ und Pour Demain unterstützen die Umwandlung des NCSC in ein Bundesamt. Die **Piratenpartei** verlangt die Schaffung eines Departements für Digitalisierung.

Der Kanton FR fordert, dass neben der Einführung einer Meldepflicht auch weitere Massnahmen zum Schutz vor Cyberbedrohungen (wie z. B. die Sensibilisierung der Bevölkerung) umgesetzt werden.

Die Piratenpartei fordert, dass bei kritischen Infrastrukturen künftig nur noch Open Source Software (OSS) verwendet werden darf. Es brauche zudem einen finanziell gut ausgestatteten Fonds, aus dem Sicherheitsaudits von weit verbreiteter Software (bspw. Open Source / FOSS) finanziert würden. Die Schweiz müsse langfristig Ressourcen aufbauen, um Hard- und Software für kritische Infrastruktur selbst zu entwickeln und zu produzieren.

4 Anhang

4.1 Kantone

ZH	Staatskanzlei des Kantons Zürich	Neumühlequai 10 Postfach 8090 Zürich staatskanzlei@sk.zh.ch
BE	Staatskanzlei des Kantons Bern	Postgasse 68 3000 Bern 8 info@sta.be.ch
LU	Staatskanzlei des Kantons Luzern	Bahnhofstrasse 15 6002 Luzern staatskanzlei@lu.ch
UR	Standeskanzlei des Kantons Uri	Rathausplatz 1 6460 Altdorf ds.la@ur.ch
SZ	Staatskanzlei des Kantons Schwyz	Regierungsgebäude Bahnhofstrasse 9 Postfach 1260 6431 Schwyz stk@sz.ch
OW	Staatskanzlei des Kantons Obwalden	Rathaus 6061 Sarnen staatskanzlei@ow.ch
NW	Staatskanzlei des Kantons Nidwalden	Dorfplatz 2 Postfach 1246 6371 Stans staatskanzlei@nw.ch
GL	Staatskanzlei des Kantons Glarus	Rathaus 8750 Glarus staatskanzlei@gl.ch
ZG	Staatskanzlei des Kantons Zug	Seestrasse 2 Regierungsgebäude am Postplatz 6300 Zug info@zg.ch
FR	Staatskanzlei des Kantons Freiburg	Rue des Chanoines 17 1701 Fribourg chancellerie@fr.ch
SO	Staatskanzlei des Kantons Solothurn	Rathaus Barfüssergasse 24 4509 Solothurn kanzlei@sk.so.ch
BS	Staatskanzlei des Kantons Basel-Stadt	Marktplatz 9 4001 Basel staatskanzlei@bs.ch
BL	Landeskanzlei des Kantons Basel-Landschaft	Regierungsgebäude Rathausstrasse 2 4410 Liestal landeskanzlei@bl.ch
SH	Staatskanzlei des Kantons Schaffhausen	Beckenstube 7 8200 Schaffhausen staatskanzlei@ktsh.ch

AR	Kantonskanzlei des Kantons Appenzell Ausserrhoden	Regierungsgebäude 9102 Herisau Kantonskanzlei@ar.ch
AI	Ratskanzlei des Kantons Appenzell Innerrhoden	Marktgasse 2 9050 Appenzell info@rk.ai.ch
SG	Staatskanzlei des Kantons St. Gallen	Regierungsgebäude 9001 St. Gallen info.sk@sg.ch
GR	Standeskanzlei des Kantons Graubünden	Reichsgasse 35 7001 Chur info@gr.ch
AG	Staatskanzlei des Kantons Aargau	Regierungsgebäude 5001 Aarau staatskanzlei@ag.ch
TG	Staatskanzlei des Kantons Thurgau	Regierungsgebäude Zürcherstrasse 188 8510 Frauenfeld staatskanzlei@tg.ch
TI	Cancelleria dello Stato del Cantone Ticino	Piazza Governo 6 6501 Bellinzona can-scds@ti.ch
VD	Chancellerie d'Etat du Canton de Vaud	Place du Château 4 1014 Lausanne info.chancellerie@vd.ch
VS	Chancellerie d'Etat du Canton du Valais	Planta 3 1950 Sion Chancellerie@admin.vs.ch
NE	Chancellerie d'Etat du Canton de Neuchâtel	Le Château Rue de la Collégiale 12 2000 Neuchâtel Secretariat.chancelle-rie@ne.ch
GE	Chancellerie d'Etat du Canton de Genève	Rue de l'Hôtel-de-Ville 2 Case postale 3964 1211 Genève 3 service-adm.ce@etat.ge.ch
JU	Chancellerie d'Etat du Canton du Jura	2, rue de l'Hôpital 2800 Delémont chancellerie@jura.ch
KKJPD	KKJPD Konferenz der Kantonalen Justiz- und Polizeidirektorin-nen und -direktoren (KKJPD)	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@kkjpd.ch
GDK	GDK Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren	Haus der Kantone Speichergasse 6 Postfach 3001 Bern office@gdk-cds.ch
RK MZF	RK MZF Regierungskonferenz Militär, Zivilschutz, Feuerwehr	Haus der Kantone Speichergasse 6 Postfach 3001 Bern

KKPKS	KKPKS Konferenz der Kantonalen Polizeikommandanten der Schweiz	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@kkpks.ch
SSK	Schweizerische Staatsanwälte-Konferenz	Haus der Kantone Speichergasse 6 Postfach 3001 Bern info@ssk-cps.ch

4.2 In der Bundesversammlung vertretene politische Parteien

Die Mitte	Die Mitte	Generalsekretariat Hirschengraben 9 Postfach 3001 Bern info@die-mitte.ch
FDP	FDP. Die Liberalen	Generalsekretariat Neuengasse 20 Postfach 3001 Bern info@fdp.ch
Die Grünen	Grüne Partei der Schweiz GPS	Waisenhausplatz 21 3011 Bern gruene@gruene.ch
GLP	Grünliberale Partei Schweiz GLP	Monbijoustrasse 30 3011 Bern schweiz@grunliberale.ch
SVP	Schweizerische Volkspartei SVP	Generalsekretariat Postfach 8252 3001 Bern gs@svp.ch
SP	Sozialdemokratische Partei der Schweiz SP	Zentralsekretariat Theaterplatz 4 Postfach 3001 Bern verena.lo-embe@spschweiz.ch

4.3 Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete

SSV	Schweizerischer Städteverband (SSV)	Monbijoustrasse 8 Postfach 3001 Bern info@staedteverband.ch

4.4 Gesamtschweizerische Dachverbände der Wirtschaft

econo-mie-suisse	Verband der Schweizer Unternehmen	Hegibachstrasse 47 Postfach 8032 Zürich 8032 Zürich info@economiesuisse.ch

		bern@economiesuisse.ch sandra.spieser@economiesu-isse.ch
Swiss Banking	Schweizerische Bankiervereinigung	Hotelgasse 10, 3011 Bern
SGV	Schweizerischer Gewerbeverband	Schwarztorstrasse 26 Postfach 3001 Bern info@sgv-usam.ch
SGB	Schweizerischer Gewerkschaftsbund	Monbijoustrasse 61, 3007 Bern, info@sgb.ch

4.5 Weitere interessierte Kreise – Stellungnahmen auf Einladung

eGov-Schweiz	Verein eGov-Schweiz	c/o mundi consulting ag Marktgasse 55 Postfach 3001 Bern info@eGov-Schweiz.ch
privatim	privatim, Konferenz der schweizerischen Datenschutz-beauftragten	c/o Dr. Beat Rudin, Advokat, Postfach 205 4010 Basel kommunikation@privatim.ch
Digitale Gesell-schaft	Digitale Gesellschaft	4000 Basel office@digitale-gesell-schaft.ch
eHealth	Interessengemeinschaft eHealth	Amthausgasse 18 3011 Bern info@ig-ehealth.ch
asut	Schweizerischer Verband der Telekommunikation	Hirschengraben 8 3011 Bern info@asut.ch
Inter-pension	Inter-pension Interessengemeinschaft autonomer Sammel- und Gemeinschaftseinrichtungen	Gartenstrasse 2 3063 Ittigen info@inter-pension.ch
RAILplus AG	RAILplus AG	Bahnhofstrasse 85 5001 Aarau info@railplus.ch
AEROS UISSE	Dachverband der Schweizerischen Luft- und Raumfahrt	Kapellenstrasse 14 Postfach 3001 Bern info@aerosuisse.ch

4.6 Weitere interessierte Kreise – spontane Stellungnahmen

eAHV/IV	eAHV/IV	p.a. mundi consulting ag Marktgasse 55 Postfach 3001 Bern jerome.brugger@mundicon-sulting.com
ISSS	Information Security Society Switzerland	Kochergasse 6, 3011 Bern sekretariat@isss.ch
Centre Patronal	Centre Patronal	Route du Lac 2 1094 Paudex info@centrepatronal.ch
Verein CH++	Verein CH++	marcel.sa-lathe@chplusplus.org
Ausland-banken	Verband der Auslandbanken in der Schweiz	Usteristrasse 23 8001 Zürich info@afbs.ch
BA	Bundesanwaltschaft BA	Guisanplatz 1 3003 Bern info@ba.admin.ch
Post CH AG	Post CH AG	Wankdorfallee 4 Postfach 3030 Bern regulatoryaffairs@post.ch
digital-switzer-land	digitalswitzerland	Waisenhausplatz 14 3011 Bern office@digitalswitzerland-bern.ch
FER	Fédération des Entreprises Romandes (FER)	98 rue de Saint-Jean 1211 Genève 11 yannic.forney@fer-ge.ch
Swico	Swico	Lagerstrasse 33 8004 Zürich info@Swico.ch
GEM	Groupement des Entreprises Multinationales	Rue de Saint-Jean 98 1211 Genf 3 info@gemonline.ch
Pour Demain	Pour Demain	Marktgasse 46 3011 Bern info@pourdemain.ch
santé-suisse	Branchenorganisation der Schweizer Krankenversicherer im Bereich der sozialen Krankenversicherung	Römerstrasse 20 Postfach CH-4502 Solothurn mail@santesuisse.ch
Swiss-ICT	SwissICT	Vulkanstr. 120 8048 Zürich info@swissict.ch
Swiss-mem	Verband für KMU und Grossfirmen der Schweizer Tech-Industrie	Pfingstweidstrasse 102 Postfach CH-8037 Zürich r.rudolph@swissmem.ch

swiss-universi-ties	Dachorganisation der Schweizer Hochschulen	swissuniversities Effingerstrasse 15 Case Postale 3001 Bern weiss@swissuniversities.ch
VUD	Verein Unternehmens-Datenschutz	Verein Unternehmens-Daten-schutz VUD c/o IT & Law Consulting GmbH Sternenstrasse 18, 8002 Zürich info@vud.ch
VöV	Verband öffentlicher Verkehr	Dählhölzliweg 12 CH-3000 Bern 6 info@voev.ch
VSE	Verband Schweizerischer Elektrizitätsunternehmen	Hintere Bahnhofstrasse 10 5000 Aarau info@strom.ch
ASIP	Schweizerischer Pensionskassenverband	Kreuzstrasse 26 8008 Zurich info@asip.ch
Science-indust-ries	Wirtschaftsverband Chemie Pharma Life Sciences	Nordstrasse 15 Postfach 8021 Zürich Schweiz
Suisse-digital	Verband für Kommunikationsnetze	Bollwerk 15 CH-3011 Bern info@suissedigital.ch
SVGW	Schweizerischer Verein des Gas- und Wasserfaches	Grütlistrasse 44 | Postfach | 8027 Zürich info@svgw.ch
SVV	Schweizerische Versicherungsverband	Conrad-Ferdinand-Meyer-Strasse 14 Case postale CH-8022 Zürich info@svv.ch
VAV	Vereinigung Schweizerischer Assetmanagement- und Vermögensverwaltungsbanken	
Gach-nang	Gemeinde Gachnang (TG)	Hôtel de ville de Gachnang Islikonerstrasse 7 8547 GACHNANG Schweiz
NFP 77 ETHZ UNIL	Gemeinsame Stellungnahme	
Opera-tion Libero	Bewegung	OPERATION LIBERO CH-3000 Bern futur@operation-libero.ch
AEIS	Stiftung Auffangeinrichtung BVG	Elias-Canetti-Strasse 2 Postfach 8050 Zurich urs.mueller@aeis.ch
Trust Valley	Fondation Trust Valley	Trust Valley EPFL Innovation Park, Bâti-ment C CH-1015 Lausanne

UniBE	Universität Bern	Dr. Cord-Ulrich Fündeling Leiter Informatikdienste Hochschulstrasse 6 3012 Bern cord.fuendeling@unibe.ch
UniGE Digital Law Centre	Universität Genf	Digital Law Center - Uni Mail - Bd du Pont d'Arve 40 - CH-1211 Genf 4 Schweiz digitallawcenter@unige.ch
Abraxas	Entreprise Abraxas Informatik AG	The Circle 68 | CH-8058 Zürich-Flughafen peter.gassmann@abraxas.ch
Axpo	Axpo services AG	Axpo Services AG Parkstrasse 23 | 5401 Baden | Switzerland thomas.porchet@axpo.com
Beat Lehmann		Acting Counsel Alcan Holdings Switzerland AG Kongoweg 9 (Home Office) 5034 Suhr b.lehmann-aarau@bluewin.ch
Coop	Coop Genossenschaft	Thiersteinerallee 12 Postfach 2550 4002 Basel Damian.Misteli@coop.ch
Flughafen ZH		Zürich Flughafen CH-8058 Andrew.karim@zurich-airport.ch
Flughafen GE		Aéroport international de Genève CP100 CH 1215 Genf
Härting Rechtsanwälte		Landis Gyr Strasse 1 6300 Zug office@haerting.ch
Helvetia	Helvetia Versicherungen AG	Helvetia Versicherungen Hauptsitz St. Alban-Anlage 26 4002 Basel martin.jara@helvetia.ch
Migros	Migros-Genossenschafts-Bund	
Raffeisen		cecile.kessler@raiffeisen.ch
Romande Energie		Rue de Lausanne 53 1110 Morges Oscar.parado@romande-energie.ch
Salt		Salt Mobile SA Rue du Caudray 4 CH-1020 Renens 1
SBB		
Sunrise	Sunrise UPC	Sunrise UPC GmbH Thurgauerstrasse 101B, 8152 Glattpark (Opfikon)

		Marcel.Huber@sunrise.net
Suva		Fluhmattstrasse 1 Case postale 4358 6004 Luzern Marc.epelbaum@suva.ch
Swiss		Swiss International Air Lines AG P.O. Box ZRHS/V/ABRO CH-8 ronald.abegglen@swiss.com 058 Zürich-Flughafen
Swisscom		Alte Tiefenaustrasse 6 3048 Worblaufen Lorenz.Ing-lin@swisscom.com
Swiss-grid		Bleichemattstrasse 31 Postfach 5001 Aarau info@swissgrid.ch
Switch		Werdtstrasse 2 Postfach 8021 Zürich
TPG	Transports publics genevois	Route de la Chapelle 1 -.Case postale 950 - 1212 Grand-Lancy 1 - Schweiz Meyer.G@tpg.ch
Piraten-partei Schweiz	Piratenpartei Schweiz	Piratenpartei Bern, 3000 Bern info@be.piratenpartei.ch