Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Generalsekretariat VBS GS-VBS
Digitalisierung und Cybersicherheit VBS

8. November 2023

Ausführungsrecht zum Informationssicherheitsgesetz

Bericht über das Ergebnis des Vernehmlassungsverfahrens

Inhaltsverzeichnis

1 Ausgangslage

Der Bundesrat hat am 24. August 2022 das VBS beauftragt, bei den Kantonen, den politischen Parteien, den gesamtschweizerischen Dachverbänden der Gemeinden, Städte und Berggebiete, den gesamtschweizerischen Dachverbänden der Wirtschaft und den interessierten Kreisen ein Vernehmlassungsverfahren zum Ausführungsrecht des neuen Informationssicherheitsgesetzes (ISG) durchzuführen. Die Vernehmlassung dauerte bis am 24. November 2022.

Das Ausführungsrecht des ISG umfasst drei neue Verordnungen und die Änderung einer bestehenden Verordnung:

- *Informationssicherheitsverordnung (ISV; neu):* Die ISV regelt das Management der Informationssicherheit, den Schutz von klassifizierten Informationen, die Informatiksicherheit und die Massnahmen zur personellen und physischen Sicherheit für die Bundesverwaltung und die Armee. Sie legt die entsprechenden Aufgaben, Kompetenzen und Verantwortlichkeiten fest. Die wichtigste Änderung ist die Einführung eines Informationssicherheits-Managementsystems (ISMS) bei allen Verwaltungseinheiten;
- *Verordnung über die Personensicherheitsprüfungen (VPSP; neu):* Die VPSP fasst die Ausführungsbestimmungen zu den verschiedenen Personensicherheitsprüfungen (PSP) zusammen. Die Anzahl dieser Prüfungen soll auf Grundlage des ISG auf das Mindestmass reduziert werden, das zur Identifizierung von erheblichen Risiken für den Bund erforderlich ist;
- *Verordnung über das Betriebssicherheitsverfahren (VBSV; neu):* Die VBSV regelt die Einzelheiten des durch das ISG eingeführten Betriebssicherheitsverfahrens (BSV). Das BSV ist auf alle sicherheitsempfindlichen Aufträge anwendbar, die der Bund an Unternehmen der Privatwirtschaft vergibt;
- *Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV; Änderung)*: Die Teilrevision beinhaltet insbesondere eine Erweiterung des Geltungsbereichs auf die Verwaltungseinheiten der dezentralen Bundesverwaltung, sofern diese Zugriff auf Informatiksysteme der zentralen Bundesverwaltung haben.

Die Kantone wurden im Rahmen der Vernehmlassung gebeten, zu den folgende vier Fragen Stellung zu nehmen:

1. Ist die Umsetzung der Verordnungen für die Kantone verständlich *(Kap. 3.1.1)*?
2. Wie gedenken die Kantone, die Verordnungen umzusetzen *(Kap. 3.1.1)*?
3. Mit welchen finanziellen Auswirkungen rechnen die Kantone *(Kap. 3.1.2)*?
4. Die Kantone sollen für Fragen der Informationssicherheit eine Dienststelle als Ansprechpartner für die Bundesbehörden bezeichnen. Wer ist die Ansprechperson bei Ihrem Kanton?

2 Ergebnis aus der Vernehmlassung

	Adressaten	**Anzahl eingeladene Teilnehmende**	**Anzahl Stellungnahmen und Rückmeldungen** *(inkl. Schreiben mit ausdrücklichem Verzicht auf eine Stellungnahme)*
1	Kantone	26	27* *(*FR: 2)*
2	politische Parteien	11	2
3	Gesamtschweizerische Dachverbände der Gemeinden, Städte und Berggebiete	3	0
4	Gesamtschweizerische Dachverbände der Wirtschaft	8	2
5	Weitere interessierte Organisationen	14	2
6	Nicht individuell eingeladene Teilnehmende		3
	Total	**62**	**36**

Gesamtwürdigung	**Anzahl**	**Teilnehmende**
Ja: Vorbehaltslose Zustimmung	12	AI, BS, BE, FR, GL, GR, SH, SZ, SO, SG, TI, VS
Ja, aber: Grundsätzliche Zustimmung mit Änderungsanträgen oder Unklarheiten	22	AG, AR, BL, FR (ITA), GE, JU, LU, NE, NW, OW, TG, UR, VD, ZG, ZH, SP, SVP, asut, BA, PVB, Swissgrid, X. D.
Nein, aber: Grundsätzliche Ablehnung mit Änderungsanträgen oder Unklarheiten	0	
Nein: Vollumfängliche Ablehnung	1	sgv
Kein Kommentar: Ausdrücklicher Verzicht auf eine Stellungnahme	1	Schweizerischer Arbeitgeberverband

3 Stellungnahmen zum Ausführungsrecht und zum Erläuternden Bericht

Aus der Vernehmlassung sind einzelne Fragen und Bemerkungen eingegangen, die im Ergebnisbericht nicht berücksichtigt werden. Meldungen von Rechtschreibungsfehlern oder Verbesserung der Übersetzung werden nicht aufgezeigt.

3.1 Allgemeine Stellungnahmen

Die Vernehmlassung hat ergeben, dass eine grosse Mehrheit der Vernehmlassungsteilnehmenden (**AG, AI, AR, BL, BS, BE, FR, GE, GL, GR, LU, NE, NW, OW, SH, SZ, SO, SG, TI, TG, UR, VD, VS, ZG, ZH, SP, SVP, asut, PVB, Swissgrid**) mit dem Ausführungsrecht zum ISG grundsätzlich einverstanden ist und dieses begrüsst. Es bestehen neben vereinzelten Anpassungswünschen einige Unklarheiten bezüglich der Umsetzung und Geltung gewisser Vorgaben für die Kantone. Lediglich der **Schweizerische Gewerbeverband (sgv)** lehnt die gesamte Vorlage ab, da sie über die gesetzliche Grundlage hinaus gehe und die von ihr generierten Kosten nicht dargelegt würden.

Die **SVP** begrüsst den mit dem neuen ISG stark verbesserten Rechtsvergleich mit anderen Ländern für eine bessere internationale Zusammenarbeit im Bereich der Informationssicherheit. Die von der Schweizerischen Eidgenossenschaft aufgenommenen und gespeicherten Personendaten müssten jedoch mindestens in der Kategorie der höchsten Klassifizierung zwingend in der Schweiz gelagert werden. Schliesslich sei für den Austausch der Daten zwingend der offizielle Dienstweg vorzusehen. Die **SVP** wünscht, dass die Kosten für die Umsetzung der Massnahmen und die zusätzlichen Stellenprozente transparent ausgewiesen werden. Sie fordert, dass durch die Massnahmen Kosteneinsparungen und eine Verbesserung des Datenschutzes erzielt werden.

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

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

NW und **OW** halten fest, dass der Begriff der Kantone im Ausführungsrecht neu definiert sei und auch öffentlich-rechtliche Körperschaften, Anstalten oder Stiftungen umfasse. Eine kohärente Begrifflichkeit, welche im Einklang mit der Definition gemäss Artikel 3 der Bundesverfassung steht, würde begrüsst. Die weiteren Körperschaften seien separat zu erwähnen.

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

3.1.1 Beurteilung der Umsetzbarkeit und Verständlichkeit

Die Vernehmlassung hat ergeben, dass die Ausführungsbestimmungen des ISG und deren Umsetzung für fast alle Kantone (**AG, AI, AR, BL, BS, BE, GE, GL, GR, LU, NE, NW, OW, SH, SZ, SO, SG, TI, TG, UR, VD, VS, ZG und ZH**) grundsätzlich verständlich sind. Zu den Auswirkungen bestehen aber noch Unklarheiten. Diese Unklarheiten betreffen nebst den Umsetzungskosten auch die «gleichwertige» Informationssicherheit und die anwendbaren, noch nicht vorliegenden Vorgaben und Mindestvorschriften. Für vereinzelte Vernehmlassungsteilnehmende (**FR (ITA)**, **JU und VD**) ist der Aufwand für die Umsetzung aufgrund dieser Unklarheiten schwierig zu beurteilen.

Verschiedene Kantone planen eine eigene Gesetzgebung zur Informationssicherheit (**AG, BE, FR**) oder prüfen, ob und in welcher Form die erforderlichen Bestimmungen erlassen bzw. bestehende Grundlagen angepasst werden müssen bzw. können (**NW, SH, UR** und **ZH**).

Eine Unklarheit für **BL** betrifft Gemeinden und andere Organisationen, wie öffentlich-rechtliche Anstalten und Betriebe in den Kantonen, die ebenfalls an Informationssystemen des Bundes angeschlossen sind. Das Ausführungsrecht mit Stand vom 24. August 2022 stelle nicht klar, wer für die Einhaltung der Sicherheitsmassnahmen durch diese Organisationen zu sorgen habe. Die Kantone könnten es für die Gemeinden nicht sein. Aus diesem Grund sei eine Ausgestaltung im vorgeschlagenen Rahmen wesentlich zielführender, wenn alle, die sich an Informationsmitteln des Bundes anschliessen wollen, die Vorgaben des Bundes für die jeweiligen Anschlüsse erfüllen müssten. Mit dieser Lösung würde viel mehr Klarheit und Einfachheit geschaffen werden und die Sicherheitsmassnahmen könnten wirkungsvoll umgesetzt werden.

Für **AR** ist fraglich, ob die Bundesverfassung die Kantone – ausserhalb der im Rahmen des Personendaten-, bzw. des Persönlichkeits- und Privatsphärenschutzes zu beachtenden Vorgaben zur (Personen-)Datensicherheit – zu allgemeiner Informationssicherheit verpflichte. Gleichzeitig sei augenscheinlich, dass durch eine Erhöhung der allgemeinen Informationssicherheit auch der Personendatenschutz profitieren würde.

FR (ITA) schlägt vor, dass bei der Erstellung der noch fehlenden Vorgaben die bisher heterogenen technischen Anforderungen des Bundes vereinheitlicht werden. Derzeit gebe es beim Bund beispielsweise drei parallele Public Key Infrastructures (PKI). Für den Kanton **FR** sei es schwierig nachzuvollziehen, welche Sicherheit er gewährleisten müsse, wenn der Bund mehrdeutige Anforderungen geltend macht. Wenn die Digitale Verwaltung Schweiz zu etwas dienen könnte, wäre dies in erster Linie die Funktion eines föderativen Organs in Bezug auf die Informationssysteme und damit auch im Bereich der Informationssicherheit. Es wird eine stärkere Einbindung der Digitalen Verwaltung Schweiz in Angelegenheiten, die die Kantone und ihre Informationssysteme betreffen. Ohne ein föderatives Organ würde die Informationslandschaft des Kantons unhandlich, insbesondere für die Kantone, die nicht über ähnliche Budgets wie der Bund verfügten.

JU und **VD** wünschen Ausführungen der Verordnungen in Bezug auf die Auswirkungen und Erwartungen gegenüber den Kantonen.

SG richte die Sicherheitsanforderungen im Kanton möglichst synchron auf die Grundschutzanforderungen des Bundes aus. Ein entsprechender Abgleich des kantonalen ISMS sei bereits in Arbeit. Eine Impactanalyse werde zeigen, welche konkreten Massnahmen in der Folge in Projekten umzusetzen sind. Die Zugriffrechte sollen im Einklang mit den Vorgaben des Bundes an diejenigen Rollenträger in den jeweiligen Ämtern erteilt werden, die diese für die Erfüllung ihrer gesetzlichen Aufgaben benötigten.

Für **TI** ist unklar, inwieweit Mitarbeitende der Verwaltungs- und Justizeinheiten der Kantonsverwaltung sowie anderer externer Stellen, die Aufgaben nach bundesrechtlichen Regelungen wahrnehmen, PSP unterzogen werden müssen. Die Unmöglichkeit, die vollständige und erschöpfende Liste der zu prüfenden Funktionen einzusehen, werfe Fragen hinsichtlich der praktischen Umsetzung auf.

VS verfüge über eine Politik der Informationssicherheit und über Rahmenrichtlinien, welche die Ziele, die allgemeinen Grundsätze und die Organisation der Informationssicherheit festlegen würden. Letztere würden für alle kantonalen Behörden gelten. Gemeinden und kantonale Institutionen würden hingegen nicht von den bestehenden Richtlinien erfasst. Allerdings würden alle Zugriffe auf den Bund, die über den Kanton laufen, von der Kantonsverwaltung verwaltet und gesichert. Der Kanton böte den Gemeinden, die dies wünschen würden, subsidiäre Unterstützung im Bereich der Cybersicherheit an und werde ab 2023 die eCyAd-Lösung zur Sensibilisierung anbieten, die vom Bund im Rahmen der zweiten Strategie zum Schutz der Schweiz vor Cyberrisiken fertiggestellt werde.

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

ZG stellt fest, dass die Hauptverantwortung für die Sicherheit bei der Bearbeitung von klassifizierten Informationen des Bundes bei den kantonalen Organen läge, die diese Daten bearbeiten bzw. die auf die Informatikmittel des Bundes zugreifen würden (namentlich: Amt für Zivilschutz und Militär, Notorganisation, Zuger Polizei, Verein für Arbeitsmarktmass nahmen). Diese Organe hätten die erforderlichen Prozesse, Zuständigkeiten und Massnahmen festzulegen, um das vom Bund verlangte Sicherheitsniveau sicherstellen zu können. Dabei kämen die Vorschriften des Bundes nur dann zur Anwendung, wenn die Vorschriften und Massnahmen der Kantone den Sicherheitsanforderungen des Bundes nicht genügen. Die Mitarbeitenden der Organe seien für die Einhaltung der Vorgaben beim Umgang mit den klassifizierten Informationen und den Informatikmitteln verantwortlich. Der richtige Umgang mit den klassifizierten Informationen und den Informatikmittel setze voraus, dass die Bundesbehörden den Organen entsprechende Vorgaben machen.

3.1.2 Beurteilung der finanziellen Auswirkungen

Die Vernehmlassung hat ein sehr breites Bild aufgezeigt, was die finanzielle Auswirkung für die Umsetzung des ISG betrifft.

Für **AI, AG, BL, BS, GL** und **VS** bringt die Umsetzung des ISG keine erheblichen Veränderungen und Zusatzkosten mit sich. **BL** erwartet lediglich einen beschränkten Mehraufwand im Bereich Compliance und eine temporäre Bindung von personellen Ressourcen. **VS** legt ein besonderes Augenmerk auf mögliche Änderungen im Zusammenhang mit Funktionen, die eine Überprüfung der Personensicherheit erfordern.

Mehrere Kantone (**AR, FR (ITA), GE**, **JU, SH, SZ, SG, TG, UR, und ZG**) konnten die finanziellen Auswirkungen zum Zeitpunkt der Vernehmlassung noch nicht genau abschätzen.

NE schätzt die Kosten zwischen 500'000 und 3 Millionen Franken für die Umsetzung eines ISMS und die Verstärkung der Sicherheit. Zusätzliche technische Anpassungen könnten sich auf mehrere Millionen belaufen.

NW schätzt die jährlichen Mehrkosten auf ca. 100'000 Franken.

OW schätzt die jährlichen Kosten auf 50'000 Franken.

SZ rechnet mit 425 zusätzlichen Stellenprozenten und Investitionen in ISMS und Sicherheitssysteme, welche ebenfalls indirekt mit der Umsetzung der Verordnungen zu tun hätten. Die zusätzlichen finanziellen Aufwände, welche im Zusammenhang mit dem neuen ISG stehen, werden für das erste Jahr grob auf 300'000 Franken für Personal und Investitionen geschätzt.

TI und **ZG** erwarten neben personellen Kosten, wie für Schulungen und die PSP, auch Kosten für die Umsetzung der technischen Sicherheitsmassnahmen.

ZH erwartet für die Sicherheitsakkreditierung von Informatikmitteln und für die regelmässige Prüfung der Sicherheit während des Lebenszyklus Zusatzkosten in der Höhe von jeweils ungefähr

10'000–50'000 Franken. Weitere Kosten könnten derzeit noch nicht abschliessend abgeschätzt werden.

3.2 Stellungnahmen zur Informationssicherheitsverordnung (ISV)

3.2.1 Allgemeine Bemerkungen zur ISV

Die Vereinheitlichung des ISMS bei allen Verwaltungseinheiten im Rahmen der neuen ISV wird begrüsst (**SVP**). Durch die Zentralisierung erhofft sich die **SVP** Kosteneinsparungen und einen effizienten Betrieb und Unterhalt. Es sei in allen Ämtern deshalb möglichst schnell das gleiche ISMS einzuführen.

GE weist auf die Komplexität und Kostspieligkeit der Umsetzung der Verordnung hin.

3.2.2 Stellungnahme zu den Artikeln der ISV

Artikel 2 Geltungsbereich

Absatz 6: Die Vernehmlassung hat ergeben, dass die Gleichwertigkeit der eigenen Gesetze mit dem ISG für mehrere Kantone (**AG, BL und ZH**) schwierig nachzuweisen ist.

AG wünscht, dass aufgezeigt wird, wie sich die Kantone bei einem vom Bund abgelehnten Zugriff zu Wehr setzen könnten, andernfalls bliebe die Ausnahmebestimmung (Art. 3 Abs. 2 ISG) sinnlos.

Artikel 6 Pflege der Rechtsgrundlagen und vertraglichen Verpflichtungen

NE ist unklar, ob die Kantone die Fachstelle des Bundes für Informationssicherheit konsultieren sollen, wenn sie ihre eigenen gesetzlichen Grundlagen schaffen, um ein gleichwertiges Sicherheitsniveau zu erreichen, oder wenn sie z. B. technische Empfehlungen umsetzten.

Artikel 9 Bewilligung und Verzeichnung von Ausnahmen

Absatz 2: **LU** wünscht eine Präzisierung, an wen die Fachstelle des Bundes für Informationssicherheit und die Departemente die Bewilligung von Ausnahmen delegieren können.

Absatz 4 Buchstabe b: **LU** stellt sich die Frage, ob die Verwaltungseinheiten, die Departemente und die Fachstelle des Bundes für Informationssicherheit in jedem Fall informiert werden, wenn die Bewilligung von Ausnahmen delegiert wurde, damit sie diese Ausnahmebewilligungen auch in ihrem Verzeichnis aufführen können. Um den Informationsfluss zu sichern, wäre eine Mitteilungs- und Informationspflicht derjenigen Stelle empfehlenswert, an welche eine Bewilligung von Ausnahmen delegiert wurde.

Artikel 12 Vorfallmanagement

Absatz 7 Buchstabe a: **LU** wünscht eine Präzisierung der mitzuteilenden Informationen. Ansonsten sei es vor allem aus datenschutzrechtlicher Sicht problematisch.

Artikel 16 Grundsätze

Der Artikel sei verständlich (**AG**). Der dazugehörige Aufwand sei aber nicht abschätzbar.

TG und **ZH** äussern die Unklarheit betreffend Zuständigkeit und Vorgehen im Falle von Einsichtsgesuchen für klassifizierte Informationen des Bundes an den Kanton. **TG** wünscht eine Erläuterung in Absatz 3, dass die kantonalen Öffentlichkeitsgesetze nicht gelten würden.

Artikel 17 Klassifizierende Stellen

Es sei für **AG** nicht ersichtlich, inwiefern diese Bestimmung für die Kantone von Belang sein solle, da sie nicht als klassifizierende Stelle aufgeführt seien.

Artikel 18–20 Klassifizierungsstufen INTERN, VERTRAULICH und GEHEIM

Die Bestimmungen seien für **AG** verständlich. Es sei jedoch unklar, ob und inwiefern es Kongruenzprobleme und Schwierigkeiten der eigenen Klassifizierungsstufen und derjenigen des Bundes gibt.

GE beantragt, dass das Kriterium «Offenlegung der Identität besonders exponierter Personen» bei der Klassifizierungsstufe VERTRAULICH in Artikel 19 Buchstabe c gestrichen werde, damit es nur ein Kriterium für die Klassifizierungsstufe GEHEIM in Artikel 20 Buchstabe c ist. Der Aspekt des Schadens für die Quelle selbst, wenn sie Zugang zu ihrer Identität erhält, werde nicht berücksichtigt, was problematisch sei und dem Staat auch schaden könne.

Bei Artikel 18 Buchstabe c weist **VD** darauf hin, dass Folgen einer psychischen Verletzung schwerwiegender sein können als diejenigen einer körperlichen Verletzung. In Buchstabe c sei jedoch bloss die körperliche Verletzung aufgeführt.

VD beantragt eine Anpassung der Bestimmungen zu den Klassifizierungsstufen. Neben den Interessen des Bundes sollten auch die Interessen von Unternehmen und Privatpersonen im Falle eines Angriffes auf die Informatiksicherheit der Systeme des Bundes rechtlich geschützt sein.

Artikel 21 Bearbeitungsvorgaben

Da gemäss Artikel 21 ISV die generell-abstrakten Weisungen einzig für die Stellen nach Artikel 2 Absätze 1–3 ISV gelten würden, ist für **AG** unklar, welche Vorgaben für die Kantone gelten und von wem sie erlassen werden.

Artikel 22 Einsatzbezogene Sicherheitsmassnahmen

Für **AG** ist unklar, wieso diese Bestimmung durch die Kantone umzusetzen sei.

X. D. beantragt eine Ergänzung von Absatz 1 mit dem Chef des militärischen Nachrichtendienstes und Dienst für präventiven Schutz der Armee sowie dem Direktor der Zoll- und Grenzsicherheit.

Artikel 23 Sicherheitsakkreditierung von Informatikmitteln

Für **AG** ist unklar, wieso diese Bestimmung durch die Kantone umzusetzen sei.

Artikel 24 Schutz bei der Gefährdung von klassifizierten Informationen

Für **AG** ist die Bestimmung verständlich und umsetzbar. Der Aufwand zur Umsetzung dürfe klein sein.

Artikel 25 Überprüfung von Schutzbedarf und Kreis der Berechtigten

AG nimmt Stellung, dass die Bestimmung für die Kantone nicht von Belang sei, da es in den Kantonen keine klassifizierenden Stellen gemäss Artikel 17 ISV gäbe.

Artikel 26 Archivierung

Für **AG** ist die Bestimmung verständlich und umsetzbar. Der Aufwand zur Umsetzung sei aber nicht abschätzbar.

Artikel 28 Zuordnung zu den Sicherheitsstufen «hoher Schutz» und «sehr hoher Schutz»

Für **AG** ist die Bestimmung verständlich und umsetzbar. Der Aufwand zur Umsetzung sei aber nicht abschätzbar.

Artikel 29 Sicherheitsmassnahmen

Da gemäss Artikel 29 Absatz 1 ISV die generell-abstrakten Weisungen einzig für die Stellen nach Artikel 2 Absätze 1–3 ISV gelten würden, ist für **AG** unklar, welche Mindestanforderungen für die jeweiligen Sicherheitsstufen für die Kantone gelten und von wem sie erlassen würden.

Die Bestimmung ist für **AG** verständlich und umsetzbar, soweit die Bestimmung doch für die Kantone gelte. Die Umsetzbarkeit hinge von den noch nicht vorliegenden Weisungen über die Mindestanforderungen ab.

Artikel 30 Sicherheit beim Betrieb

Für **AG** ist die Bestimmung verständlich und umsetzbar. Der Aufwand zur Umsetzung sei aber nicht abschätzbar.

Artikel 34 physische Schutzmassnahmen

Da gemäss Artikel 34 Absatz 1 ISV die generell-abstrakten Weisungen einzig für die Stellen nach Artikel 2 Absätze 1–3 ISV gelten würden, ist für **AG** unklar, welche minimal erforderlichen Massnahmen zum physischen Schutz von Informationen und Informatikmitteln für die Kantone gelten und von wem sie erlassen würden. Die Bestimmung ist für **AG** verständlich und umsetzbar, soweit die Bestimmung für die Kantone gelte. Die Umsetzbarkeit hinge von den noch nicht vorliegenden Minimalanforderungen ab.

Artikel 35 Sicherheitszonen

GE weist darauf hin, dass die generell-abstrakten Weisungen zu den Sicherheitszonen zu Änderung von Räumlichkeiten führen könnte, damit die Geheimhaltungsstufe weiterhin erfüllt werden könne.

X. D. beantragt, dass das Recht eingeräumt werde, in der Umgebung der Sicherheitszonen den böswilligen Einsatz von elektromagnetischen Wellen zu kontrollieren.

Artikel 44 Allgemeines

X. D. beantragt, die gesetzliche Grundlage bezüglich des Austausches von Personendaten zu prüfen und allenfalls den Artikel der ISV zu präzisieren.

3.3 Stellungnahmen zur Änderung der Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV)

3.3.1 Allgemeine Bemerkungen zur IAMV

VD nimmt mit Interesse zur Kenntnis, dass die Vernetzung mit einem kantonalen IAM durch diese neue Version der Verordnung nunmehr erlaubt sei, und werde gegebenenfalls die Einführung dieser neuen Möglichkeit evaluieren. Er weist darauf hin, dass die Revision dieser Verordnung vor allem technische Aspekte von Systemen zur Verwaltung von Identifikationsdaten betreffe. Diese könnten sich auf das Identitätsmanagement des IAM-Portals des Kantons oder anderer Datenbanken auswirken, insbesondere im Hinblick auf die Verpflichtung zur Verwaltung von Akkreditierungen und Zugängen zu Informationssystemen des Bundes. Es handle sich hierbei um «Dritte», die ebenfalls diese Identifikationssysteme verwenden würden.

Die **SVP** begrüsst die Ausdehnung des Geltungsbereiches auf die Verwaltungseinheiten der dezentralen Bundesverwaltung hinsichtlich der Personenprüfung. Es seien aber die Auswirkungen auf den Datenschutz, insbesondere durch die erweiterte Bearbeitung biometrischer Daten, kritisch zu begleiten.

VS nimmt mit Interesse zur Kenntnis, dass die Vernetzung mit einem kantonalen IAM durch diese neue Version der Verordnung nunmehr erlaubt sei, und werde gegebenenfalls die Umsetzung dieser neuen Möglichkeit evaluieren.

3.3.2 Stellungnahmen zu den Artikeln der IAMV

Artikel 13 Zentraler Identitätsspeicher als Verteiler

Absatz 4: **GE** stellt die Frage, ob mit «das jeweilige System» das Quellsystem oder ein anderes internes Informationssystem der Bundesverwaltung gemeint sei.

Artikel 18 Anforderungen an die Informationssicherheit

Absatz 2: **GE** beantragt die Präzisierung, durch wen und in welchem Rahmen die Mindestanforderungen definiert werden.

Artikel 21 Anschluss externer IAM-Systeme: Voraussetzungen

Buchstabe c: **GE** bemerkt, dass das sein kantonales IAM-System Daten von Personen enthalte, welche die vom Bund zur Verfügung gestellten Informationssysteme nicht nutzen würden. **GE** fragt deshalb, ob in seinem IAM-System nur die Untergruppe von Personen, die auf Informatiksysteme des Bundes zugreifen würden, an das IAM-System des Bundes angeschlossen werden dürfe.

Anhang

Buchstabe e: technische Angaben: **GE** beantragt zur Datenkategorie «7. Passwörter» eine Präzisierung, dass die Daten je nach Bedarf gut verschlüsselt oder gehasht sein sollten.

3.4 Stellungnahmen zur Verordnung über die Personensicherheitsprüfungen (VPSP)

3.4.1 Allgemeine Bemerkungen zur VPSP

Die **SVP** wünscht, die Reduktion der Prüffälle von Mindestens 30 Prozent positiv hervorzuheben. Nachzuvollziehen sei die damit verbundene Ersetzung älterer Verordnungen.

VD weist darauf hin, dass sich die VPSP auf die Stellen auswirken werde, die im kantonalen Rahmen für personenbezogene Sicherheitsüberprüfungen zuständig sind. Es sei nicht zu vergessen, dass die geplante umfangreiche Datenerhebung und die Verarbeitung sensibler Personendaten eine strenge Aufsicht erfordern würden, die mit der Datenschutzgesetzgebung vereinbar sei.

X. D. weist darauf hin, dass die VPSP in Bezug auf die verfassungsrechtlichen und gesetzlichen Grundlagen extrem problematisch sei. Die Verordnung sei in dieser Hinsicht nochmals zu prüfen oder prüfen lassen.

3.4.2 Stellungnahme zu den Artikeln der VPSP

Artikel 2 Geltungsbereich

Swissgrid beantragt die Aufnahme des StromVG in den Geltungsbereich, da das StromVG eine eigenständige gesetzliche Grundlage sei: «*Diese Verordnung gilt unter Vorbehalt von Artikel 84 Absatz 3 ISG und Artikel 2 Absätze 2–5 der Informationssicherheitsverordnung vom… für die verpflichteten Behörden und Organisationen nach Artikel 2 ISG sowie Artikel 20a StromVG.*»

Artikel 3 Zuordnung

Absatz 3: **Swissgrid** beantragt folgende Ergänzung, da **Swissgrid** weder zur zentralen noch dezentralen Bundesverwaltung zähle:

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

Artikel 5 Veröffentlichung, Aufbewahrung und Bekanntgabe

Swissgrid würde es begrüssen, wenn die betreffende Funktionenliste aufgrund ihrer Vertraulichkeit und zum Schutz von **Swissgrid** und ihre Mitarbeitenden nicht in der Amtlichen Sammlung publiziert würde.

Artikel 8 Prüfungen bei kantonalen Angestellten und Dritten

Absatz 1: **AG** wünscht die Festlegung der Funktionen kantonaler Angestellter, die nach Artikel 29 Absatz 1 Buchstabe b ISG einer Prüfung unterstehen sollen. Es solle ebenfalls der Ablauf der Antragsstellung an das VBS definiert werden.

Die Funktionen innerhalb des Kantons **VS**, die eine persönliche Sicherheitsüberprüfung erfordern, seien bekannt und die Überprüfungen würden bereits seit mehreren Jahren durchgeführt. **VS** stellt jedoch fest, dass das VBS gemäss der Erklärung zu Artikel 8 des erläuternden Berichts den Auftrag erhalten hat, die Praktiken zu vereinheitlichen. Dies könne potenziell eine Ausweitung der Kontrollen im Kanton bedeuten, was mit erheblichen finanziellen Kosten verbunden wäre.

Artikel 11 Prüfung der Vertrauenswürdigkeit nach dem BPG

Absatz 1 Buchstabe c und Absatz 2: Die **BA** beantragt als Strafverfolgungsbehörde die Ergänzung der Grundlage für die Grundsicherheitsprüfung und erweiterte PSP für internes und externes Personal der BA aufgrund des Risikos einer erheblichen resp. schwerwiegenden Beeinträchtigung.

Artikel 14 Prüfungen der Vertrauenswürdigkeit nach dem StromVG

Swissgrid ist mit dem Wortlaut einverstanden und dankt für die Berücksichtigung der entsprechenden Eingaben.

Artikel 15 Einleitende und entscheidende Stellen

Absatz 4: **Swissgrid** begrüsst die enthaltene Bestimmung, wonach die nationale Netzgesellschaft einleitende und entscheidende Stelle ist.

Artikel 19 Datenerhebung

X. D. äussert seine starke Unzufriedenheit mit diesem Artikel. Der Artikel solle in 5–6 kleinere Artikel gekürzt werden und sei in legistischer Hinsicht der redaktionellen Qualität der Gesetze und Verordnungen des Schweizer Rechts nicht würdig.

Absatz 2 Buchstabe c: **Swissgrid** beantragt die Aufnahme der nationalen Netzgesellschaft in eine neue Ziffer 8, wodurch in jedem Fall bei einer erweiterten PSP eine Befragung durchgeführt werde. Dies aufgrund Erfahrungen mit PSP auf privatrechtlicher Basis.

Artikel 26 f. Ordentliche und Ausserordentliche Wiederholung

NE fragt sich, wie lange eine PSP gültig sei und ob die PSP im Falle einer Wiederholung aufgrund eines Sicherheitsrisikos die bisherige Bewertung ergänze oder ersetze.

Artikel 30 Sicherheitsbescheinigung im internationalen Verhältnis

X. D. schlägt vor, diesen Artikel zu erweitern und festzulegen, dass eine Erteilung von Amtes wegen für verschiedene Funktionen des NDB, des MND und der AB-ND erfolge, um den Verwaltungsaufwand in Bezug auf die Anzahl der Anträge auf Erteilung von Bescheinigungen zu verringern.

Artikel 35 Leistungen der Fachstellen PSP zugunsten der Kantone

AG sieht derzeit nicht vor, PSP künftig an den Bund auszulagern. Die Anforderungen seien aber machbar und die Höhe der Gebühren angemessen.

GE weist darauf hin, dass die Höhe der Gebühren beispielsweise für die Polizei oder das kantonale Amt für Informationssysteme und Digitalisierung beträchtlich sein könnte.

GE überprüft, ob eine Grundlage für die PSP zum Zwecke der eigenen Informationssicherheit geschaffen werden solle.

NE stellt sich die Frage, ob die geltend gemachten Sicherheitsgründe in den kantonalen gesetzlichen Grundlagen definiert werden müssten oder ob es dieselben sind wie in der VPSP.

Artikel 38 Übergangsbestimmungen

Absatz 4: **Swissgrid** beantragt folgende Anpassung des Absatzes: «*Sicherheitsprüfungen, die die nationale Netzgesellschaft vor und bis ein Jahr nach Inkrafttreten dieser Verordnung ~~und vor Ablauf der Frist nach Absatz 5 auf privatrechtlicher Basis~~ erhalten hat, bleiben im Rahmen der Wiederholungsfristen nach den Artikeln 26 und 27 wie folgt anwendbar: […]*»

Absatz 5: **Swissgrid** beantragt die Streichung des Absatzes.

Anhang 6 Funktionen nach Artikel 20a Absatz 1 StromVG

Swissgrid schlägt für die Unterscheidung der Funktionen nach den einzelnen Tätigkeiten eine Differenzierung der Funktionen nach Typen vor.

Anhang 7 Datenerhebung und -bearbeitung

Die Vernehmlassung hat ergeben, dass für diverse Teilnehmende (**GE, TG, UR, SP, PVB, sgv und X. D.**) der Anhang bezüglich Datenbearbeitung von besonders schützenswerten Personendaten zu weit geht.

Die **SP** fordert, dass das Wort «insbesondere» in Anhang 7 VPSP überall ersatzlos gestrichen wird. Die staatliche Kompetenz soll explizit erwähnt und glasklar definiert sein. Eine nicht abschliessende Liste wird abgelehnt.

3.5 Stellungnahmen zur Verordnung über das Betriebssicherheitsverfahren (VBSV)

3.5.1 Allgemeine Bemerkungen zur VBSV

Die VBSV sei nötig (**SVP**) und die Ersetzung der Geheimschutzverordnung überfällig.

AG wünscht sich die Möglichkeit zum Leistungsbezug betreffend die Durchführung von BSV analog der VPSP.

UR stellt fest, dass keine Umsetzung der VBSV für die Kantone erforderlich sei.

Der **sgv** stellt fest, dass die Umsetzung über den Verordnungsweg noch regulierungsintensiver ausfalle als im Gesetz vorgesehen. Es fehlten zudem Angaben über die damit verbundenen Regulierungskosten und Zusatzkosten für die Kantone.

3.5.2 Stellungnahme zu den Artikeln der VBSV

Artikel 2 Betroffene Betriebe

VD beantragt eine Prüfung des Verhältnisses zwischen Artikel 2 Absatz 1, wonach die Verordnung nur auf Betriebe mit Sitz in der Schweiz anwendbar ist, und Artikel 6, in welchem die Modalitäten für die Einleitung des Verfahrens bei ausländischen Betrieben geregelt werden.

Artikel 14 Inhalt und Prüfung des Sicherheitskonzepts

VD beantragt, dass das Sicherheitskonzept bei technischen Entwicklungen oder Änderungen der Risiken angepasst werde.

Artikel 17 Meldungen des Betriebs

GE beantragt Präzisierungen. In Absatz 1 Buchstabe a soll präzisiert werden, dass dies auch für die Tochtergesellschaften gelte. In Absatz 1 Buchstabe e soll «in der Schweiz und anderen Ländern» ergänzt werden. In Absatz 2 sei es in Bezug auf Vorfälle im Bereich der Sicherheit relevant, Datenschutzverletzungen im Sinne des nDSG hinzuzufügen.

4 Anhang: Vernehmlassungsteilnehmende und Änderungsanträge

Abkürzung	Teilnehmende	Änderungsanträge und Unklarheiten Verordnung/Erläuternder Bericht				
		ISV	IAMV	VPSP	VBSV	AT[1] Erl. Be-
Kantone						
ZH	Zürich	x				x
BE	Bern					
LU	Luzern	x				
UR	Uri			x		
SZ	Schwyz					
OW	Obwalden					x
NW	Nidwalden					x
GL	Glarus					
ZG	Zug					x
FR	Freiburg					
FR (ITA)	Freiburg, Amt für Informatik und Telekommunikation	x				
SO	Solothurn					
BS	Basel-Stadt					
BL	Basel-Landschaft	x				x
SH	Schaffhausen					
AR	Appenzell Ausserrhoden	x				
AI	Appenzell Innerrhoden					
SG	St. Gallen					
GR	Graubünden					
AG	Aargau	x		x	x	
TG	Thurgau	x		x		
TI	Tessin					
VD	Waadt	x	x	x		
VS	Wallis					
NE	Neuenburg	x		x		

[1] AT=Allgemeiner Teil

Abkürzung	Teilnehmende	Änderungsanträge und Unklarheiten Verordnung/Erläuternder Bericht				
		ISV	IAMV	VPSP	VBSV	AT[1] Erl. Be-
GE	Genf	x	x	x	x	
JU	Jura	x				
Politische Parteien						
SVP	Schweizerische Volkspartei SVP					
SP	Sozialdemokratische Partei der Schweiz SPS			x		
Gesamtschweizerische Dachverbände der Wirtschaft						
SGV	Schweizerischer Gewerbeverband (SGV)			x		
	Schweizerischer Arbeitgeberverband					
Weitere interessierte Organisationen						
PVB	Personalverband des Bundes (PVB)			x		
	Swissgrid AG			x		
Nicht individuell eingeladene Teilnehmende						
Asut	asut – Schweizerischer Verband der Tele-kommunikation				x	
BA	Bundesanwaltschaft			x		
X. D.	Xavier Dufour	x		x		