Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesgesetz über die Informationssicherheit beim Bund
(Informationssicherheitsgesetz, ISG)

Änderung vom ...

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
nach Einsicht in die Botschaft des Bundesrates vom …
beschliesst:

I

Das Informationssicherheitsgesetz vom 18. Dezember 2020[1] wird wie folgt geändert:

Titel

Bundesgesetz über die Informationssicherheit (Informationssicherheitsgesetz, ISG)

Art. 1 Abs. 1

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 Cyberbedrohungen erhöhen.

Art. 2 Abs. 5

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.

1 SR **128**, AS **2022** 232

Art. 4 Abs. 1 und 1bis

[1] Das Öffentlichkeitsgesetz vom 17. Dezember 2004[2] (BGÖ) geht diesem Gesetz vor.

[1bis] Informationen Dritter, von denen das Nationale Zentrum für Cybersicherheit (NCSC) durch die Entgegennahme und Analyse von Meldungen gemäss dem 5. Kapitel Kenntnis erhält, dürfen nicht nach dem BGÖ zugänglich gemacht werden. Nicht als Dritte gelten Behörden, Organisationen und Personen nach Artikel 2 Absatz 1 BGÖ.

Art. 5 Einleitungssatz (Betrifft nur den französischen Text) und Bst. d–g

In diesem Gesetz bedeuten:

d. *Cybervorfall:* Ereignis bei der Nutzung von Informatikmitteln, das dazu führt, dass die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist;

e. *Cyberangriff:* Cybervorfall, der absichtlich ausgelöst wurde;

f. *Cyberbedrohung*: Jeder Umstand oder jedes Ereignis mit dem Potenzial, einen Cybervorfall zu ermöglichen;

g. *Schwachstelle*: Cyberbedrohung, die auf Schwächen oder Fehler in Informatikmitteln zurückzuführen ist.

Einfügen vor dem Gliederungstitel des 2. Abschnitts

Art. 10a Bearbeitung von Personendaten

[1] Die verpflichteten Behörden und Organisationen können die zur Gewährleistung der Informationssicherheit zweckmässigen Personendaten, insbesondere in dafür vorgesehenen Informationssystemen (ISMS-Anwendungen), bearbeiten.

[2] Sie können Personendaten nach Absatz 1 untereinander sowie mit nationalen, internationalen und ausländischen Organisationen des öffentlichen Rechts austauschen, sofern:

a. dies zur Gewährleistung der Informationssicherheit zweckmässig ist;

b. keine gesetzlichen oder vertraglichen Geheimhaltungspflichten verletzt werden;

c. die Vorgaben der Bundesgesetzgebung über den Datenschutz eingehalten werden; und

d. diese Organisation gesetzliche Aufgaben im Bereich der Informationssicherheit wahrnehmen, die denjenigen der bekanntgebenden Behörde oder Organisation entsprechen.

2 SR **152.3**

[3] Sie können ihre Informationssysteme, insbesondere die ISMS-Anwendungen, miteinander verknüpfen und Daten automatisch oder auf Anfrage über Schnittstellen austauschen.

[4] Sie können zur Einreichung und Bearbeitung von Anträgen und Meldungen im Bereich der Informationssicherheit digitale Formulare betreiben und diese mit ihren ISMS-Anwendungen oder anderen Informationssystemen verknüpfen.

[5] Sofern dies für die Bewältigung von Verletzungen der Informationssicherheit oder die Behebung von Schwachstellen erforderlich ist, können sie besonders schützenswerte Personendaten nach Artikel 5 Buchstabe c des Datenschutzgesetzes vom 25. September 2020[3] (DSG) von Personen, die daran beteiligt oder davon betroffen sind respektive sein könnten:

a. bearbeiten;

b. untereinander sowie mit nationalen, internationalen und ausländischen Organisationen des öffentlichen Rechts austauschen, sofern die Bedingungen nach Absatz 2 Buchstaben b erfüllt sind.

[6] Sie dürfen die besonders schützenswerten Personendaten bis zwei Jahre nach der Bewältigung der Verletzungen der Informationssicherheit oder die Behebung der Schwachstellen aufbewahren, höchstens aber zehn Jahre.

[7] Die Archivierung der Daten richtet sich nach den Vorschriften der Archivierungsgesetzgebung.

[8] Die Bearbeitung von Personendaten durch das NCSC zur Erfüllung seiner Aufgaben richtet sich nach Artikel 75–79.

Art. 23 Abs. 3
Betrifft nur den französischen Text.

Art. 44 Abs. 2

[2] Die Einschränkung des Auskunftsrechts richtet sich nach Artikel 26 DSG[4].

Gliederungstitel nach Art. 73

3 SR **235.1**
4 SR **235.1**

5. Kapitel: Massnahmen des Bundes zum Schutz der Schweiz vor Cyberbedrohungen

1. Abschnitt: Allgemeine Bestimmungen

Art. 73a Grundsatz

[1] Zum Schutz der Schweiz vor Cyberbedrohungen erstellt das NCSC technische Analysen zur Bewertung und Abwehr von Cybervorfällen und Cyberbedrohungen sowie zur Identifikation und Behebung von Schwachstellen.

[2] Gestützt auf die Analysen nimmt das NCSC insbesondere folgende Aufgaben wahr:

a. Sensibilisierung und Warnung der Öffentlichkeit in Bezug auf Cyberbedrohungen;

b. Warnung von betroffenen Behörden, Organisationen und Personen bei unmittelbaren Cyberbedrohungen oder laufenden Cyberangriffen;

c. Veröffentlichung von Informationen zur Cybersicherheit sowie von Empfehlungen für präventive und reaktive Massnahmen gegen Cybervorfälle;

d. Entgegennahme und Bearbeitung von Meldungen zu Cybervorfällen und Cyberbedrohungen;

e. Unterstützung von Betreiberinnen von kritischen Infrastrukturen.

Art. 73b Meldungen

[1] Das NCSC nimmt Meldungen zu Cybervorfällen und Cyberbedrohungen entgegen. Die Meldungen können anonym erfolgen.

[2] Das NCSC analysiert die Meldungen bezüglich ihrer Bedeutung für den Schutz der Schweiz vor Cyberbedrohungen. Es gibt auf Wunsch eine Empfehlung zum weiteren Vorgehen ab, sofern dafür keine weiteren Analysen und Abklärungen erforderlich sind.

[3] Erhält das NCSC Kenntnis von einer Schwachstelle, so informiert es umgehend die Herstellerin der betroffenen Hard- oder Software und setzt ihr zur Behebung der Schwachstelle eine angemessene Frist. Es weist ihn darauf hin, dass eine Missachtung beschaffungsrechtlich sanktioniert werden kann (Art. 44 Abs. 1 Bst. f[bis] des Bundesgesetzes vom 21. Juni 2019[5] über das öffentliche Beschaffungswesen) und dass das NCSC nach Fristablauf die Schwachstelle gemäss Artikel 73*c* Absatz 2 veröffentlichen kann.

Art. 73c Veröffentlichung von Informationen aus Meldungen

[1] Das NCSC kann Informationen zu Cybervorfällen veröffentlichen, sofern dies dem Schutz vor Cyberbedrohungen dient. Diese Informationen dürfen nur dann Aufschluss über die betroffene natürliche oder juristische Person geben, sofern diese dazu

5 SR **172.056.1**

einwilligt und es sich um missbräuchlich verwendete Identifikationsmerkmale und Adressierungselemente handelt.

2 Das NCSC kann Informationen zu Schwachstellen unter Angabe der betroffenen Hard- oder Software veröffentlichen, sofern die Herstellerin einwilligt oder die Schwachstelle nicht innert der Frist nach Artikel 73*b* Absatz 3 behoben hat.

Art. 73d Weiterleitung von Informationen

1 Das NCSC kann Informationen aus Meldungen an Behörden und Organisationen weiterleiten, die im Bereich der Cybersicherheit tätig sind. Diese Informationen dürfen nur dann Personendaten umfassen, wenn die betroffene Person einwilligt.

2 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[6] (NDG) erforderlich sind, so leitet das NCSC diese Informationen an den NDB weiter.

3 Erhalten Mitarbeitende des NCSC im Zusammenhang mit einer Meldung oder deren Analyse Hinweise auf eine mögliche Straftat, so zeigen sie diese abweichend von Artikel 22*a* Absatz 1 des Bundespersonalgesetzes vom 24. März 2000[7] ausschliesslich der Leiterin oder dem Leiter des NCSC an. Diese oder dieser kann Anzeige bei den Strafverfolgungsbehörden erstatten, sofern dies aufgrund der Schwere der möglichen Straftat geboten scheint.

4 Strafrechtlich geschützte Geheimnisse darf das NCSC nur nach den Vorgaben von Artikel 320 des Strafgesetzbuches[8] weiterleiten.

Art. 74 Unterstützung von Betreiberinnen von kritischen Infrastrukturen

1 Das NCSC unterstützt die Betreiberinnen von kritischen Infrastrukturen beim Schutz vor Cyberbedrohungen.

2 Es stellt ihnen insbesondere folgende Hilfsmittel unentgeltlich und zur freiwilligen Nutzung zur Verfügung:

a. ein Kommunikationssystem für den sicheren Informationsaustausch;

b. technische Informationen zu aktuellen Cyberbedrohungen sowie Empfehlungen für präventive und reaktive Massnahmen gegen Cybervorfälle;

c. technische Instrumente und Anleitungen zur Erkennung von Cybervorfällen, die auf den erhöhten Schutzbedarf von kritischen Infrastrukturen ausgerichtet sind.

6 SR **121**
7 SR **172.220.1**
8 SR **311.0**

[3] Es kann sie bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen beraten und unterstützen, wenn die Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährdet ist 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.

Gliederungstitel nach Art. 74

2. Abschnitt: Pflicht zur Meldung von Cyberangriffen

Art. 74a Grundsätze

[1] Behörden und Organisationen nach Artikel 74*b* müssen dafür sorgen, dass dem NCSC Cyberangriffe auf ihre Informatikmittel gemeldet werden.

[2] Das NCSC erteilt interessierten Behörden und Organisationen Auskunft darüber, ob sie der Meldepflicht unterstellt sind und erlässt auf Antrag eine Verfügung über die Unterstellung unter die Meldepflicht.

[3] Durch die Meldung eines Cyberangriffs haben die meldepflichtigen Behörden und Organisationen Anspruch auf die Unterstützung des NCSC bei der Vorfallbewältigung nach Artikel 74 Absatz 3.

[4] Die Meldepflicht dient ausschliesslich dazu, dass das NCSC Angriffsmuster auf kritische Infrastrukturen frühzeitig erkennen und dadurch mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Art. 74b Meldepflichtige Behörden und Organisationen

[1] Die Meldepflicht gilt für:

a. Hochschulen nach Artikel 2 Absatz 2 des Hochschulförderungs- und -koordinationsgesetzes vom 30. September 2011[9];

b. Bundes-, Kantons- und Gemeindebehörden sowie interkantonale, kantonale und interkommunale Organisationen, mit Ausnahme der Gruppe Verteidigung, wenn die Armee Assistenzdienst nach Artikel 67 oder Aktivdienst nach Artikel 76 des Militärgesetzes vom 3. Februar 1995[10] leistet;

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[11], Energiehandel,

9 SR **414.20**
10 SR **510.10**
11 SR **730.0**

Energiemessung oder Energiesteuerung tätig sind, mit Ausnahme der Bewilligungsinhaber gemäss Kernenergiegesetz vom 21. März 2003[12], sofern ein Cyberangriff auf eine Kernanlage erfolgt;

e. Unternehmen, die dem Bankengesetz vom 8. November 1934[13], dem Versicherungsaufsichtsgesetz vom 17. Dezember 2004[14] oder dem Finanzmarktinfrastrukturgesetz vom 19. Juni 2015[15] unterstehen;

f. Gesundheitseinrichtungen, die auf der kantonalen Spitalliste nach Artikel 39 Absatz 1 Buchstabe e des Bundesgesetzes vom 18. März 1994[16] über die Krankenversicherung aufgeführt sind;

g. medizinische Laboratorien mit einer Bewilligung nach Artikel 16 Absatz 1 des Epidemiengesetzes vom 28. September 2012[17];

h. Unternehmen, die für die Herstellung, das Inverkehrbringen und die Einfuhr von Arzneimitteln eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 2000[18] haben;

i. Organisationen, die Leistungen zur Absicherung gegen die Folgen von Krankheit, Unfall, Arbeits- und Erwerbsunfähigkeit, Alter, Invalidität und Hilflosigkeit erbringen;

j. die Schweizerische Radio- und Fernsehgesellschaft;

k. Nachrichtenagenturen von nationaler Bedeutung;

l. Anbieterinnen von Postdiensten, die gemäss Artikel 4 Absatz 1 des Postgesetzes vom 17. Dezember 2010[19] bei der Postkommission registriert sind;

m. Eisenbahnunternehmen nach Artikel 5 oder 8*c* des Eisenbahngesetzes vom 20. Dezember 1957[20] sowie Seilbahn-, Trolleybus-, Autobus- und Schifffahrtsunternehmen mit einer Konzession nach Artikel 6 des Personenbeförderungsgesetzes vom 20. März 2009[21];

n. Unternehmen der Zivilluftfahrt, die über eine Bewilligung des Bundesamtes für Zivilluftfahrt verfügen, sowie die Landesflughäfen gemäss Sachplan Infrastruktur der Luftfahrt;

o. Unternehmen, die nach dem Seeschifffahrtsgesetz vom 23. September 1953[22] Güter auf dem Rhein befördern, sowie Unternehmen, welche die Registrierung, Ladung oder Löschung im Hafen Basel betreiben;

12 SR **732.1**
13 SR **952.0**
14 SR **961.01**
15 SR **958.1**
16 SR **832.10**
17 SR **818.101**
18 SR **812.21**
19 SR **783.0**
20 SR **742.101**
21 SR **745.1**
22 SR **747.30**

p. Unternehmen, welche die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen und deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen führen würde;

q. Anbieterinnen von Fernmeldediensten, die beim Bundesamt für Kommunikation nach Artikel 4 Absatz 1 FMG[23] registriert sind;

r. Registerbetreiberinnen und Registrare von Internet-Domains nach Artikel 28*b* FMG;

s. Anbieterinnen und Betreiberinnen von Diensten und Infrastrukturen, die der Ausübung der politischen Rechte dienen;

t. Anbieterinnen und Betreiberinnen von Cloudcomputing, Suchmaschinen, digitalen Sicherheits- und Vertrauensdiensten sowie Rechenzentren, sofern sie einen Sitz in der Schweiz haben;

u. Herstellerinnen von Hard- oder 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. Steuerung und Überwachung von betriebstechnischen Systemen und Prozessen,

2. Gewährleistung der öffentlichen Sicherheit.

[2] Bei Behörden und Organisationen, die auch Tätigkeiten ausüben, die nicht unter Absatz 1 fallen, besteht keine Meldepflicht für Cyberangriffe, die sich ausschliesslich auf diese Tätigkeiten auswirken.

[3] Die Meldepflicht nach Absatz 1 gilt für Cyberangriffe, die sich in der Schweiz auswirken, auch wenn sich die betroffenen Informatikmittel im Ausland befinden.

Art. 74c Ausnahmen von der Meldepflicht

Der Bundesrat nimmt Organisationen und Behörden von der Meldepflicht nach Artikel 74*b* aus, wenn durch Cyberangriffe ausgelöste Funktionsstörungen nur geringe Auswirkungen auf das Funktionieren der Wirtschaft beziehungsweise das Wohlergehen der Bevölkerung haben.

Art. 74d Zu meldende Cyberangriffe

Ein Cyberangriff muss gemeldet werden, wenn er:

a. die Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährdet;

b. zu einer Manipulation oder zu einem Abfluss von Informationen geführt hat;

c. über einen längeren Zeitraum unentdeckt blieb, insbesondere wenn Anzeichen dafür bestehen, dass er zur Vorbereitung weiterer Cyberangriffe ausgeführt wurde; oder

d. mit Erpressung, Drohung oder Nötigung verbunden ist.

Art. 74e Frist und Inhalt der Meldung

[1] Die Meldung muss innert 24 Stunden nach der Entdeckung des Cyberangriffs erfolgen.

[2] Sie muss Informationen zur meldepflichtigen Behörde oder Organisation, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen, zu ergriffenen Massnahmen und, soweit bekannt, zum geplanten weiteren Vorgehen enthalten.

[3] Sind zum Zeitpunkt der Meldung nicht alle erforderlichen Informationen bekannt, so ergänzt die meldepflichtige Behörde oder Organisation die Meldung, sobald sie über neue Informationen verfügt.

[4] Wer die Meldepflicht für eine Behörde oder Organisation zu erfüllen hat, muss im Rahmen der Meldung keine Angaben machen, die sie oder ihn strafrechtlich belasten.

[5] Das NCSC informiert die meldepflichtige Behörde oder Organisation, sobald alle Angaben zur Erfüllung der Meldepflicht vorliegen.

Art. 74f 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 den meldepflichtigen Behörden und Organisationen ermöglichen, die Meldung des Cyberangriffs oder seiner Auswirkungen gesamthaft oder in Teilen an weitere Behörden zu übermitteln.

[3] Sind zur Erfüllung einer Meldepflicht gegenüber weiteren Behörden Informationen erforderlich, die über Artikel 74*e* hinausgehen, so muss das System den meldepflichtigen Behörden und Organisationen ermöglichen, diese Informationen direkt an die betreffenden Behörden zu übermitteln, ohne dass das NCSC darauf Zugriff hat.

Art. 74g Verletzung der Meldepflicht

[1] Bestehen Anzeichen für eine Verletzung der Meldepflicht, so informiert das NCSC die meldepflichtige Behörde oder Organisation darüber und setzt ihr eine angemessene Frist, um der Meldepflicht nachzukommen.

[2] Kommt die meldepflichtige Behörde oder Organisation ihrer Pflicht innert dieser Frist nicht nach, so erlässt das NCSC eine Verfügung über diese Pflicht, setzt darin eine neue Frist und verweist auf die Bussandrohung nach Artikel 74*h*.

Art. 74h Missachten von 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 nach Absatz 1 in Geschäftsbetrieben ist Artikel 6 des Bundesgesetzes vom 22. März 1974[24] über das Verwaltungsstrafrecht (VStrR) anwendbar.

[24] SR **313.0**

[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.

Gliederungstitel vor Art. 75

3. Abschnitt: Datenschutz und Informationsaustausch

Art. 75 Bearbeitung von Personendaten

[1] Das NCSC kann zur Erfüllung seiner Aufgaben Personendaten bearbeiten, einschliesslich Adressierungselemente nach Artikel 3 Buchstabe f FMG[25] und damit zusammenhängende besonders schützenswerte Personendaten, die Informationen enthalten über:

a. religiöse, weltanschauliche oder politische Ansichten; 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.

[2] Bei der Bearbeitung von Personendaten oder bei konkreten Hinweisen auf den Missbrauch einer Identität oder auf die unberechtigte Verwendung von Adressierungselementen informiert das NCSC die betroffenen Personen, sofern dies nicht mit unverhältnismässigem Aufwand verbunden ist und keine überwiegenden öffentlichen Interessen entgegenstehen.

Art. 76 Zusammenarbeit im Inland

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

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

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

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

25 SR **784.10**

Art. 76a Unterstützung für Behörden

[1] Das NCSC unterstützt den NDB mit periodischen Auswertungen zu Anzahl, Art und Ausmass von Cyberangriffen sowie, auf Anfrage, mit technischen Analysen von Cyberbedrohungen.

[2] Es gewährt dem NDB zum Zweck des frühzeitigen Erkennens und Verhinderns von Bedrohungen der inneren oder äusseren Sicherheit, zur Beurteilung der Bedrohungslage und zur nachrichtendienstlichen Frühwarnung zum Schutz von kritischen Infrastrukturen nach Artikel 6 Absätze 1 Buchstabe a, 2 und 5 NDG[26] Zugriff auf Informationen, welche die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen betreffen.

[3] Es gewährt den Strafverfolgungsbehörden Zugriff auf Informationen, welche die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen betreffen.

[4] Es gewährt den kantonalen Stellen, die für die Cybersicherheit zuständig sind, Zugriff auf Informationen, die für den Schutz vor Cyberbedrohungen erforderlich sind.

Art. 77 Internationale Zusammenarbeit

[1] Das NCSC kann mit ausländischen und internationalen Stellen, die für die Cybersicherheit zuständig sind, Informationen austauschen, die Aufschluss über die Identität und die Vorgehensweise der Verursacherinnen und Verursacher von Cyberangriffen geben, wenn sie diese zur Erfüllung von Aufgaben benötigen, die denjenigen des NCSC entsprechen. Umfasst der Informationsaustausch auch Personendaten, sind Artikel 16 und 17 DSG[27] zu beachten.

[2] Der Informationsaustausch nach Absatz 1 ist nur dann zulässig, wenn die ausländischen und internationalen Stellen die bestimmungsgemässe Verwendung gewährleisten.

Art. 78

Aufgehoben

Art. 79 Abs. 1

[1] Das NCSC bewahrt Personendaten nur so lange auf, wie dies zur Erkennung von Cyberbedrohungen oder zur Bewältigung von Cybervorfällen zweckmässig ist, höchstens jedoch fünf Jahre ab der letzten Verwendung zu diesem Zweck. Bei besonders schützenswerten Personendaten beträgt die Frist zwei Jahre.

Art. 80

Aufgehoben

26 SR **121**
27 SR **235.1**

II

Die nachstehenden Erlasse werden wie folgt geändert:

1. Bundesgesetz vom 21. Juni 2019[28] über das öffentliche Beschaffungswesen

*Art. 44 Abs. 1 Bst. f^bis^*

[1] Die Auftraggeberin kann eine Anbieterin von einem Vergabeverfahren ausschliessen, aus einem Verzeichnis streichen oder einen ihr bereits erteilten Zuschlag widerrufen, wenn festgestellt wird, dass auf die betreffende Anbieterin, ihre Organe, eine beigezogene Drittperson oder deren Organe einer der folgenden Sachverhalte zutrifft:

f^bis^. Sie beheben eine Schwachstelle in der von ihnen hergestellten Hard- oder Software nicht innert der Frist, die das Nationale Zentrum für Cybersicherheit nach Artikel 73*b* Absatz 3 des Informationssicherheitsgesetzes vom 18. Dezember 2020[29] gesetzt hat.

2. Datenschutzgesetz vom 25. September 2020[30]

*Art. 24 Abs. 5^bis^*

[5bis] Der EDÖB kann die Meldung mit dem Einverständnis des 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 Verantwortlichen.

3. Kernenergiegesetz vom 21. März 2003[31]

Art. 102 Abs. 2

[2] Erhält das ENSI eine Meldung zu einem Cyberangriff auf eine Kernanlage, der die Voraussetzungen von Artikel 74*d* des Informationssicherheitsgesetzes vom 18. Dezember 2020[32] erfüllt, so leitet es diese Meldung dem Nationalen Zentrum für Cybersicherheit weiter.

28 SR **172.056.1**
29 SR **128,** AS **2022** 232
30 SR **235.1**, AS **2022** 491
31 SR **732.1**
32 SR **128**, AS **2022** 232

4. Stromversorgungsgesetz vom 23. März 2007[33]

Art. 8a Schutz vor Cyberbedrohungen

[1] Die Netzbetreiber, die Erzeuger und die Speicherbetreiber müssen Massnahmen für einen angemessenen Schutz ihrer Anlagen vor Cyberbedrohungen treffen.

[2] Der Bundesrat kann Ausnahmen vorsehen und, sofern zur Sicherstellung der Versorgung notwendig, die Pflicht nach Absatz 1 auf andere Dienstleister im Bereich der Elektrizitätsversorgung ausdehnen.

5. Finanzmarktaufsichtsgesetz vom 22. Juni 2007[34]

Art. 39 Abs. 1

[1] Die FINMA ist befugt, anderen inländischen Aufsichtsbehörden, dem Nationalen Zentrum für Cybersicherheit sowie der Schweizerischen Nationalbank nicht öffentlich zugängliche Informationen zu übermitteln, die diese zur Erfüllung ihrer Aufgaben benötigen.

III

Dieses Gesetz untersteht dem fakultativen Referendum.

Der Bundesrat bestimmt das Inkrafttreten.

33 SR **734.7**
34 SR **956.1**