Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBl 2020
www.bundesrecht.admin.ch
Massgebend ist die signierte elektronische Fassung

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:

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 Cyberrisiken 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.

SR **126**
[1] SR **126** [BBl **2020** 9975]

Vernehmlassung

Art. 5 Bst. d–e

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.

Gliederungstitel vor Art. 73a

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

1. Abschnitt: Allgemeine Bestimmungen

Art. 73a 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.

Art. 73b 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.

Vernehmlassung

[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.

Art. 73c 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[2] (NDG) relevant sind, so leitet das NCSC diese Informationen an den NDB weiter.

[2] Für Mitarbeitende des NCSC entfällt die Anzeigepflicht gemäss Artikel 22*a* des Bundespersonalgesetzes vom 24. März 2000[3], 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[4] weiterleiten.

Art. 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

2 SR **121**
3 SR **172.220.1**
4 SR **311.0**

Vernehmlassung

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.

Gliederungstitel vor Art. 74a

2. Abschnitt: Pflicht zur Meldung von Cyberangriffen auf kritische Infrastrukturen

Art. 74a 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.

Art. 74b Bereiche

Die Meldepflicht gilt für:

a. Hochschulen nach Artikel 2 Absatz 2 des Hochschulförderungs- und -koordinationsgesetzes vom 30. September 2011[5];

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[6], Energiehandel, -messung oder -steuerung tätig sind;

e. Unternehmen, die dem Bankengesetz vom 8. November 1934[7], dem Versicherungsaufsichtsgesetz vom 17. Dezember 2004[8] oder dem Finanzmarktinfrastrukturgesetz vom 19. Juni 2015[9] 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

5 SR **414.20**
6 SR **730.0**
7 SR **952.0**
8 SR **961.01**
9 SR **958.1**

Vernehmlassung

3. Sicherheits- und Vertrauensdienste anbieten;

g. Spitäler, die auf der kantonalen Spitalliste nach Artikel 39 Absatz 1 Buchstabe e des Bundesgesetzes vom 18. März 1994[10] über die Krankenversicherung aufgeführt sind;

h. medizinische Laboratorien mit einer Bewilligung nach Artikel 16 Absatz 1 des Epidemiengesetzes vom 28. September 2012[11];

i. Unternehmen, die für die Herstellung, das Inverkehrbringen und die Einfuhr von Arzneimitteln eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 2000[12] (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[13] registriert sind;

o. Transportunternehmen, die dem Bundesgesetz vom 18. Juni 2010[14] 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[15] 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,

10 SR **832.10**
11 SR **818.101**
12 SR **812.21**
13 SR **783.0**
14 SR **745.2**
15 SR **747.30**

Vernehmlassung

4. IT-Sicherheit, Verschlüsselung, Identifikation, Zugriffs- und Zutrittsberechtigung.

Art. 74c 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.

Art. 74d 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.

Art. 74e 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.

Art. 74f Übermittlung der Meldung

Vernehmlassung

[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.

Art. 74g 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.

Art. 74h 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*.

Art. 74i 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[16] 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.

16 SR **313.0**

Vernehmlassung

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 Adressierungselementen nach Artikel 3 Buchstabe f FMG[17] 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.

[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 18*a* Absatz 4 Buchstabe b und 18*b* DSG[18].

Art. 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.

Art. 76a 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 kriti-

17 SR **784.10**
18 SR **235.1**

Vernehmlassung

schen Infrastrukturen nach Artikel 6 Absätze 1 Buchstabe a, 2 und 5 NDG[19] 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.

Art. 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[20] 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.

Art. 78
Aufgehoben

Art. 79 Abs. 1

[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.

Art. 80
Aufgehoben

19 SR **121**
20 SR **235.1**

Vernehmlassung

II

Die nachstehenden Erlasse werden wie folgt geändert:

1. Stromversorgungsgesetz vom 23. März 2007[21]

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[22]

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.

III

[1] Dieses Gesetz untersteht dem fakultativen Referendum.

[2] Der Bundesrat bestimmt das Inkrafttreten.

Vernehmlassung

21 SR **734.7**
22 SR **235.1,** BBl 2020 7639