Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature]

[QR Code]

Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung

(Cyberrisikenverordnung, CyRV)

vom …

Der Schweizerische Bundesrat,

gestützt auf Artikel 30 des Bundesgesetzes vom 21. März 1997[1] über Massnahmen zur Wahrung der inneren Sicherheit
und auf die Artikel 43 Absätze 2 und 3, 47 Absatz 2 und 55 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997[2],

verordnet:

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Gegenstand

Diese Verordnung regelt die Organisation der Bundesverwaltung zum Schutz vor Cyberrisiken sowie die Aufgaben und Zuständigkeiten der verschiedenen Stellen im Bereich Cybersicherheit.

Art. 2 Geltungsbereich

Diese Verordnung gilt für:

a. die Verwaltungseinheiten der zentralen Bundesverwaltung nach Artikel 7 der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998[3];

b. die Behörden und Stellen, die sich gemäss Artikel 2 Absätze 2 und 3 der Bundesinformatikverordnung vom 9. Dezember 2011[4] (BinfV) dazu verpflichten, sie einzuhalten.

SR .....
1 SR **120**
2 SR **172.010**
3 SR **172.010.1**
4 SR **172.010.58**

Art. 3 Begriffe

In dieser Verordnung bedeuten:

a. *Cybersicherheit:* anzustrebender Zustand, bei dem die Datenbearbeitung, insbesondere der Datenaustausch zwischen Personen und Organisationen, über Informations- und Kommunikationsinfrastrukturen wie beabsichtigt funktioniert;

b. *Cybervorfall:* unbeabsichtigtes oder von Unbefugten beabsichtigtes Ereignis, das dazu führt, dass die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Daten beeinträchtigt ist oder es zu Funktionsstörungen kommen kann;

c. *Cyberrisiko:* Gefahr eines Cybervorfalls, deren Grösse durch das Produkt der Eintrittswahrscheinlichkeit und des Schadensausmasses bestimmt ist;

d. *Resilienz:* die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, intern oder extern verursachten Störungen zu widerstehen und das ordnungsgemässe Funktionieren zu erhalten oder dieses möglichst rasch und vollständig wiederzuerlangen;

e. *Informatiksicherheit*: der auf technische Systeme bezogene Aspekt der Cybersicherheit;

f. *Informatiksicherheitsvorgaben:* Sicherheitsanforderungen an die Organisation, die Prozesse, die Dienstleistungen und die Technik;

g. *kritische Infrastrukturen:* Prozesse, Systeme und Einrichtungen, die für das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung essenziell sind.

2. Kapitel: Grundsätze für den Schutz vor Cyberrisiken

Art. 4 Ziele

[1] Die Bundesverwaltung sorgt für eine angemessene Resilienz ihrer Organe und Systeme gegenüber Cyberrisiken.

[2] Sie arbeitet mit den Kantonen, den Gemeinden, der Wirtschaft, der Gesellschaft, der Wissenschaft und den internationalen Partnern zusammen, soweit dies dem Schutz der eigenen Sicherheitsinteressen dient, und fördert den Informationsaustausch.

Art. 5 Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken

Der Bundesrat legt in der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) den strategischen Rahmen für die Verbesserung der Prävention, Früherkennung, Reaktion und Resilienz zum Schutz vor Cyberrisiken fest.

Art. 6 Bereiche

Die Massnahmen zum Schutz vor Cyberrisiken sind in folgende drei Bereiche unterteilt:

a. Bereich Cybersicherheit: Gesamtheit der Massnahmen, die der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen und die internationale Zusammenarbeit zu diesem Zweck stärken;

b. Bereich Cyberdefence: Gesamtheit der nachrichtendienstlichen und militärischen Massnahmen, die dem Schutz der für die Landesverteidigung kritischen Systeme, der Abwehr von Cyberangriffen, der Gewährleistung der Einsatzbereitschaft der Armee in allen Lagen und dem Aufbau von Kapazitäten und Fähigkeiten zur subsidiären Unterstützung ziviler Behörden dienen; dazu zählen auch aktive Massnahmen zur Erkennung von Bedrohungen, zur Identifikation von Angreifern und zur Störung und Unterbindung von Angriffen;

c. Bereich Cyberstrafverfolgung: Gesamtheit aller Massnahmen der Polizei und der Staatsanwaltschaft von Bund und Kantonen zur Bekämpfung der Cyberkriminalität.

3. Kapitel: Organisation und Zuständigkeiten

1. Abschnitt: Departementsübergreifende Zusammenarbeit

Art. 7 Bundesrat

Der Bundesrat nimmt folgende Funktionen wahr:

a. Er überwacht die Umsetzung der NCS anhand des strategischen Controllings und beschliesst bei Bedarf Massnahmen.

b. Er legt im Rahmen seiner Zuständigkeiten fest, in welchen Bereichen Vorgaben zum Schutz vor Cyberrisiken nötig sind oder angepasst werden sollen.

c. Er erlässt Weisungen über den Schutz der Bundesverwaltung vor Cyberrisiken.

d. Er bewilligt Abweichungen von seinen Vorgaben.

Art. 8 Kerngruppe Cyber

1 Die Kerngruppe Cyber (KGCy) setzt sich zusammen aus:

a. der oder dem Delegierten für Cybersicherheit (Art. 6*a* der Organisationsverordnung vom 17. Febr. 2010[5] für das Eidgenössische Finanzdepartement) als Vertreterin oder Vertreter des Eidgenössischen Finanzdepartements (EFD);

5 SR **172.215.1**

b. einer Vertreterin oder einem Vertreter des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS);

c. einer Vertreterin oder einem Vertreter des Eidgenössischen Justiz- und Polizeidepartements (EJPD);

d. einer Vertreterin oder einem Vertreter der Kantone, die oder der durch die zuständige Konferenz der Kantonsregierungen bestimmt wird.

2 Die oder der Delegierte für Cybersicherheit hat den Vorsitz.

3 Die KGCy informiert Vertreterinnen und Vertreter weiterer Verwaltungseinheiten des Bundes, die im Bereich Cyberrisiken tätig sind, über die Traktanden und kann sie für einzelne Sitzungen beiziehen. Bei Belangen mit aussenpolitischem Bezug involviert sie das Eidgenössische Departement für auswärtige Angelegenheiten (EDA). Zudem kann sie Expertinnen oder Experten aus Wirtschaft und Hochschulen beiziehen.

4 Die KGCy hat namentlich folgende Aufgaben:

a. Sie beurteilt aktuelle Cyberrisiken sowie deren mögliche Entwicklung anhand von Informationen aus den Bereichen Cybersicherheit, -defence und -strafverfolgung.

b. Sie bewertet laufend die bestehenden Dispositive in den Bereichen Cybersicherheit, -defence und -strafverfolgung und prüft, ob diese der Bedrohungslage angepasst sind.

c. Sie begleitet, wenn nötig unter Einbezug weiterer Stellen, die interdepartementale Vorfallbewältigung.

d. Sie informiert die Kerngruppe Sicherheit des Bundes (KGSi) über aussen- und sicherheitspolitisch relevante Cybervorfälle und Entwicklungen.

5 Die drei in der KGCy vertretenen Departemente stellen Informationen für die gemeinsame Lagebeurteilung zur Verfügung.

6 Der Nachrichtendienst des Bundes ist für die Darstellung der gesamtheitlichen Cyberbedrohungslage zuhanden der KGCy zuständig.

Art. 9 Steuerungsausschuss Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken

1 Der Bundesrat setzt einen Steuerungsausschuss Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (StA NCS) ein.

2 Der StA NCS setzt sich zusammen aus der oder dem Delegierten für Cybersicherheit, durch die zuständige Konferenz der Kantonsregierungen bestimmte Vertretungen der Kantone, Vertretungen der Wirtschaft und der Hochschulen sowie Vertreterinnen und Vertretern der Verwaltungseinheiten, welche die federführende Verantwortung für die Umsetzung einer NCS-Massnahme gemäss dem NCS-Umsetzungsplan haben. Jedes Departement und die Bundeskanzlei stellen mindestens eine Vertreterin oder einen Vertreter im StA NCS.

3 Die oder der Delegierte für Cybersicherheit hat den Vorsitz.

4 Der StA NCS hat folgende Aufgaben:

a. Er sorgt für die strategische Kohärenz bei der Umsetzung der NCS-Massnahmen und prüft deren Fortschritt laufend mittels strategischem Controlling.

b. Er definiert bei verzögerter oder unvollständiger Umsetzung der NCS-Massnahmen Vorschläge für Sondermassnahmen.

c. Er sorgt für die laufende Weiterentwicklung der NCS; hierzu verfolgt er im Austausch mit der KGCy die Entwicklung der Bedrohungslage und erarbeitet bei Bedarf Anpassungsvorschläge für die NCS.

d. Er erstattet dem Bundesrat und der Öffentlichkeit jährlich Bericht über die Umsetzung der NCS.

e. Er sorgt für ein koordiniertes Vorgehen aller beteiligten Stellen aus Bund, Kantonen, Wirtschaft und Hochschulen bei der Umsetzung der NCS-Massnahmen.

f. Er stellt sicher, dass bei der Umsetzung der NCS-Massnahmen die Risikopolitik des Bundes, die Nationale Strategie zum Schutz kritischer Infrastrukturen sowie die Strategien des Bundesrates im Informatikbereich berücksichtigt werden.

Art. 10 Ausschuss Informatiksicherheit

1 Der Ausschuss Informatiksicherheit (A-IS) setzt sich aus einer Vertreterin oder einem Vertreter des Nationalen Zentrums für Cybersicherheit (NCSC[6]), den Informatiksicherheitsbeauftragten der Departemente und der Bundeskanzlei sowie der oder dem Informatiksicherheitsbeauftragten der Standarddienste der Informations- und Kommunikationstechnik (IKT) zusammen.

2 Fallweise können weitere Personen beratend beigezogen werden.

3 Die Vertreterin oder der Vertreter des NCSC hat den Vorsitz.

4 Der A-IS fungiert als Konsultativorgan für das NCSC betreffend Informatiksicherheitsfragen in der Bundesverwaltung.

Art. 11 Delegierte oder Delegierter für Cybersicherheit

1 Die oder der Delegierte für Cybersicherheit nimmt folgende Aufgaben wahr:

a. Sie oder er leitet das NCSC.

b. Sie oder er sorgt für eine optimale Abstimmung der überdepartementalen Arbeiten der Bereiche Cybersicherheit, -defence und -strafverfolgung.

c. Sie oder er sorgt für die Visibilität der Aktivitäten des Bundes im Bereich Cyberrisiken, trägt zu optimalen Rahmenbedingungen für eine innovative Cybersicherheitswirtschaft bei, ist die massgebende Ansprechperson des Bundes zu Cyberrisiken und vertritt diesen in den massgeblichen Kommissi-

6 National Cyber Security Centre

onen und Arbeitsgruppen; sie oder er sorgt für eine optimale Abstimmung der Arbeiten der Kantone und des Bundes zum Schutz der Schweiz vor Cyberrisiken.

d. Sie oder er vertritt das NCSC in den Krisenstäben des Bundes.

e. Sie oder er erlässt Informatiksicherheitsvorgaben.

f. Sie oder er entscheidet über Abweichungen von den von ihr oder ihm erlassenen Vorgaben; betreffen die Abweichungen auch IKT-Vorgaben des Informatiksteuerungsorgans des Bundes (ISB), so hört sie oder er vorgängig das ISB an.

[2] Sie oder er informiert das EFD zuhanden des Bundesrates regelmässig über den Stand der Informatiksicherheit in den Departementen und der Bundeskanzlei.

[3] Sie oder er kann sich an der Erarbeitung von Informatikvorgaben der Bundesverwaltung mit Bezug zur Cybersicherheit und an sicherheitsrelevanten Informatikvorhaben beteiligen. Namentlich kann sie oder er Informationen verlangen, dazu Stellung nehmen und Änderungen verlangen.

[4] Sie oder er kann nach Anhörung der Eidgenössischen Finanzkontrolle Überprüfungen der Informatiksicherheit verlangen.

2. Abschnitt: Organe des Bereichs Cybersicherheit

Art. 12 Nationales Zentrum für Cybersicherheit

[1] Das Nationale Zentrum für Cybersicherheit (NCSC) ist das Kompetenzzentrum des Bundes für Cyberrisiken und koordiniert die Arbeiten des Bundes im Bereich Cybersicherheit. Es hat folgende Aufgaben:

a. Es betreibt die nationale Anlaufstelle für Cyberrisiken; diese nimmt Meldungen aus der Bundesverwaltung, der Wirtschaft, den Kantonen und der Bevölkerung entgegen, analysiert sie und kann Empfehlungen dazu abgeben.

b. Es sorgt mit den zuständigen Kooperationspartnern in der Bundesverwaltung für die subsidiäre Unterstützung der Betreiber kritischer Infrastrukturen und fördert unter diesen den Informationsaustausch zu Cyberrisiken.

c. Es betreibt das «Computer Emergency Response Team» (GovCERT); dieses ist die nationale Fachstelle für die technische Vorfallbewältigung, die Analyse technischer Fragestellungen, die Einschätzungen der Bedrohungslage aus technischer Sicht und die technische Unterstützung der nationalen Anlaufstelle.

d. Es betreibt eine Fachstelle für die Informatiksicherheit des Bundes; diese erarbeitet Informatiksicherheitsvorgaben, berät die Verwaltungseinheiten bei deren Umsetzung und erhebt den Stand der Informatiksicherheit in den Departementen und der Bundeskanzlei.

e. Es stellt die Informatiksicherheitsbeauftragten des Bundes (ISBB).

f. Es koordiniert die Umsetzung der NCS, führt ein strategisches Controlling durch und bereitet die Sitzungen der KGCy und des StA NCS vor.

g. Es verfügt über einen Expertenpool, aus dem Expertinnen und Experten zur Unterstützung der Fachämter bei der Umsetzung von NCS-Massnahmen sowie bei der Entwicklung, Umsetzung und Prüfung von Standards und Regulierungen in Bezug auf die Cybersicherheit zur Verfügung gestellt werden.

h. Es trägt mit gezielten Informationen zur Sensibilisierung der Bundesverwaltung und der Öffentlichkeit in Bezug auf Cyberrisiken bei, informiert über die aktuelle Lage und gibt Anleitungen für präventive und reaktive Massnahmen heraus.

i. Es betreibt eine resiliente Analyse- und Kommunikationsinfrastruktur, die unabhängig von der restlichen Bundesinformatik funktionieren muss.

j. Es informiert die KGCy sowie bei aussen- und sicherheitspolitischer Bedeutung die KGSi über relevante Cybervorfälle.

[2] Es kann, sofern dies direkt oder indirekt dem Schutz der Bundesverwaltung vor Cyberrisiken dient, Daten zu Cybervorfällen und damit verbundenen Kommunikationsflüssen bearbeiten. Es kann sie staatlichen und privaten Sicherheitsteams bekanntgeben, sofern:

a. der Datenlieferant einverstanden ist; und

b. keine gesetzlichen Geheimhaltungspflichten verletzt werden.

[3] Eine Bekanntgabe von Personendaten ins Ausland ist nur zulässig, sofern die diesbezüglichen Vorgaben der Bundesgesetzgebung über den Datenschutz eingehalten werden.

[4] Besonders schützenswerte Personendaten dürfen nur bearbeitet werden, soweit für deren Bearbeitung mit Mitteln der Bundesinformatik die erforderliche gesetzliche Grundlage besteht.

[5] Das NCSC übernimmt in der Bundesverwaltung nach Rücksprache mit den betroffenen Dienststellen die Federführung bei der Bewältigung eines Cybervorfalls, wenn dieser das ordnungsgemässe Funktionieren der Bundesverwaltung gefährdet. Dabei hat es folgende Aufgaben und Kompetenzen:

a. Es kann die betroffenen Leistungserbringer und -bezüger verpflichten, ihm alle nötigen Informationen zur Verfügung zu stellen.

b. Es kann Sofortmassnahmen anordnen.

c. Es informiert die Leitung der betroffenen Verwaltungseinheiten über den Verlauf.

[6] Wurde nach einem Cybervorfall die Gefährdung der Vertraulichkeit oder der Funktionsfähigkeit der Bundesverwaltung durch die getroffenen Massnahmen genügend reduziert und sind die nötigen Folgearbeiten sowie deren Finanzierung definiert, so übergibt das NCSC die Verantwortung für die Weiterbearbeitung wieder an die betroffenen Stellen.

Art. 13 Departemente und Bundeskanzlei

1 Die Departemente und die Bundeskanzlei berichten dem NCSC zum Jahresende über den Stand der Informatiksicherheit.

2 Die internen Leistungserbringer nach den Artikeln 23 und 24 BinfV[7] erstatten dem NCSC regelmässig Bericht über entdeckte Schwachstellen und Cybervorfälle sowie über geplante und getroffene Massnahmen zu deren Behebung.

3 Die Departemente und die Bundeskanzlei bestimmen je eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten (ISBD).

Art. 14 Verwaltungseinheiten und ihre Leistungserbringer

1 Die Verwaltungseinheiten bestimmen je eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten (ISBO). Das ISB bestimmt zusätzlich eine Informatiksicherheitsbeauftragte oder einen Informatiksicherheitsbeauftragten für die IKT-Standarddienste.

2 Die Verwaltungseinheiten sind für den Schutz ihrer Informatiksysteme, Anwendungen und Daten (Schutzobjekte) verantwortlich. Sie nehmen folgende Funktionen wahr:

a. Sie prüfen ihre Schutzobjekte regelmässig und ergreifen die notwendigen Sicherheitsmassnahmen; sie stellen namentlich sicher, dass diese für die einzelnen Schutzobjekte in aktueller Form dokumentiert sind.

b. Sie sind für die Einhaltung der Informatiksicherheitsvorgaben und der Beschlüsse des Bundesrates, des NCSC und der Departemente beziehungsweise der Bundeskanzlei in ihrem Zuständigkeitsbereich verantwortlich.

c. Sie sind unter Vorbehalt von Artikel 12 Absatz 5 verantwortlich für die Bewältigung von Cybervorfällen, die ihre Schutzobjekte betreffen.

d. Sie stellen sicher, dass beim Bezug von Leistungen bei einem externen Leistungserbringer die Informatiksicherheitsvorgaben Teil des Vertragsverhältnisses mit diesem sind.

e. Sie überprüfen die Einhaltung der Informatiksicherheitsvorgaben durch externe Leistungserbringer in geeigneter Weise.

3 Die Leistungserbringer stellen sicher, dass sie über die nötigen Kapazitäten zur Bewältigung von Cybervorfällen bei sich und ihren Leistungsbezügern verfügen.

4 Die Leistungserbringer melden den Leistungsbezügern entdeckte Schwachstellen und Sicherheitsvorfälle unverzüglich.

5 Die Leistungsbezüger definieren in Zusammenarbeit mit den Leistungserbringern einen Prozess für die Bewältigung von Cybervorfällen. Darin werden namentlich die Entscheidkompetenzen für Sofortmassnahmen geregelt.

7 SR **172.010.58**

6 Kann ein Cybervorfall nicht im Rahmen des definierten Prozesses bewältigt werden, so informieren die Betroffenen das NCSC, um das weitere Vorgehen zu bestimmen.

7 Die Verwaltungseinheiten konsultieren das NCSC bei sicherheitsrelevanten Informatikvorgaben sowie -vorhaben.

8 Die Verwaltungseinheiten sind für die Entwicklung, Umsetzung und Prüfung von Standards und Regulierungen in Bezug auf die Cybersicherheit in ihren Sektoren verantwortlich. Das NCSC stellt ihnen im Rahmen der Möglichkeiten Expertinnen und Experten aus dem Pool nach Artikel 12 Absatz 1 Buchstabe g zur Verfügung.

4. Kapitel: Schlussbestimmungen

Art. 15 Änderung anderer Erlasse

Die Änderung anderer Erlasse ist im Anhang geregelt.

Art. 16 Übergangsbestimmung zu Artikel 2 Buchstabe b

1 Behörden und Stellen, die sich vor Inkrafttreten dieser Verordnung durch Vereinbarung mit dem ISB verpflichtet haben, die Bestimmungen der BinfV[8] einzuhalten, unterstehen bis am 31. Dezember 2021 den Verpflichtungen gemäss dieser Verordnung im Umfang der bisherigen Regelung.

2 Sie unterstehen ab dem 1. Januar 2022 dieser Verordnung, sofern die Vereinbarung nicht spätestens per 31. Dezember 2021 aufgelöst wurde.

Art. 17 Übergangsbestimmung zu Artikel 11 Absatz 1 Buchstabe e

1 Vor dem Inkrafttreten dieser Verordnung durch das ISB erlassene IKT-Sicherheitsvorgaben und bewilligte Ausnahmen gelten weiter.

2 Über Änderungen an Vorgaben und bewilligten Ausnahmen entscheidet das NCSC.

Art. 18 Inkrafttreten

Diese Verordnung tritt am 1. Juli 2020 in Kraft.

… Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Simonetta Sommaruga
Der Bundeskanzler: Walter Thurnherr

8 SR **172.010.58**

Anhang
(Art. 15)

Änderung anderer Erlasse

Die nachstehenden Verordnungen werden wie folgt geändert:

1. Bundesinformatikverordnung vom 9. Dezember 2011[9]

Art. 2 Abs. 3

[3] Behörden und Stellen, die sich nach Absatz 2 verpflichten, diese Verordnung und die darauf gestützten Vorgaben einzuhalten, verpflichten sich damit auch, die Cyberrisikenverordnung vom …[10] (CyRV) und die darauf gestützten Vorgaben einzuhalten.

Art. 3 Abs. 4 Bst. d und Abs. 8, 3. Kap. (Art. 10 und 11) sowie Art. 14 Bst. e

Aufgehoben

Art. 16a Nationales Zentrum für Cybersicherheit

Das Nationale Zentrum für Cybersicherheit (NCSC[11]) nach Artikel 12 der CyRV[12] wird bei der Erarbeitung von Informatikvorgaben der Bundesverwaltung mit Bezug zur Cybersicherheit und bei sicherheitsrelevanten Informatikvorhaben konsultiert.

Art. 17 Abs. 1 Bst. e–i

[1] Das ISB hat namentlich folgende Aufgaben:

e. Es entscheidet über Abweichungen von den von ihm erlassenen Vorgaben; sind diese Abweichungen sicherheitsrelevant, so hört es vorgängig den Delegierten oder die Delegierte für Cybersicherheit an.

f.–g. *Aufgehoben*

h. Es stellt einen Informatiksicherheitsbeauftragten oder eine Informatiksicherheitsbeauftragte für die Standarddienste.

i. *Aufgehoben*

9 SR **172.010.58**
10 SR …
11 National Cyber Security Centre
12 SR …

Art. 18 Abs. 1

[1] Der Informatikrat des Bundes (IRB) setzt sich zusammen aus dem oder der Delegierten für die IKT-Steuerung (Art. 20*a* Abs. 2 der Organisationsverordnung vom 17. Febr. 2010[13] für das Eidgenössische Finanzdepartement) und je einem namentlich bezeichneten Vertreter oder einer namentlich bezeichneten Vertreterin jedes Departements, der Bundeskanzlei und des NCSC. Der oder die Delegierte hat den Vorsitz.

Art. 19

Aufgehoben

2. Organisationsverordnung vom 17. Februar 2010[14] für das Eidgenössische Finanzdepartement

Art. 20a Abs. 3 Bst. c

Aufgehoben

13 SR **172.215.1**
14 SR **172.215.1**