2552 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVII. GP

Regierungsvorlage

Bundesgesetz zur Einrichtung einer nationalen Behörde für die Cybersicherheitszertifizierung (Cybersicherheitszertifizierungs-Gesetz – CSZG)

Der Nationalrat hat beschlossen:

Inhaltsverzeichnis

1. Abschnitt
Allgemeine Bestimmungen

Anwendungsbereich und Durchführung von Rechtsakten der EU

§ 1. Dieses Bundesgesetz regelt Aspekte der Durchführung der Verordnung (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cyber- und digitale Sicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), ABl. Nr. L 151 vom 17.04.2019 S. 15.

Begriffsbestimmungen

§ 2. Für die in diesem Bundesgesetz verwendeten Begriffe gelten die Begriffsbestimmungen in Art. 2 der Verordnung (EU) 2019/881, wie insbesondere zu den Begriffen europäisches Cybersicherheitszertifikat, europäisches Schema für die Cybersicherheitszertifizierung, IKT-Produkt, IKT-Dienst, IKT-Prozess, Vertrauenswürdigkeitsstufe und Selbstbewertung der Konformität.

2. Abschnitt
Einrichtung und Aufgaben

Einrichtung und Aufgaben der nationalen Behörde für die Cybersicherheitszertifizierung

§ 3. (1) Der Bundeskanzler hat die Aufgaben der nationalen Behörde für die Cybersicherheitszertifizierung gemäß Art. 58 der Verordnung (EU) 2019/881 und das dafür erforderliche Technologiemanagement wahrzunehmen.

(2) Für die Ausübung von Tätigkeiten der nationalen Behörde für die Cybersicherheitszertifizierung im Zusammenhang mit der Ausstellung von Zertifikaten nach Art. 56 Abs. 5 Buchstabe a und Abs. 6 der Verordnung (EU) 2019/881 hat der Bundeskanzler sicherzustellen, dass diese Tätigkeiten von den Aufsichtstätigkeiten nach Art. 58 der Verordnung (EU) 2019/881 streng getrennt sind und die Tätigkeiten unabhängig voneinander durchgeführt werden.

(3) Der Bundeskanzler hat eine gemäß Art. 56 Abs. 8 der Verordnung (EU) 2019/881 erfolgte Mitteilung über eine festgestellte Sicherheitslücke oder Unregelmäßigkeit hinsichtlich der Sicherheit von zertifizierten IKT-Produkten, -Diensten oder -Prozessen unverzüglich im Rahmen des gemäß § 7 Abs. 1 des Netz- und Informationssystemsicherheitsgesetzes (NISG), BGBl. I Nr. 111/2018, eingerichteten Inneren Kreises der Operativen Koordinierungsstruktur (IKDOK) zum Zwecke der Erörterung und Aktualisierung des Lagebildes zu melden.

(4) Die Zuständigkeiten anderer Marktüberwachungsbehörden bleiben von diesem Bundesgesetz unberührt.

3. Abschnitt
Befugnisse und Datenverarbeitung

Befugnisse

§ 4. (1) Der Bundeskanzler hat die in der Verordnung (EU) 2019/881, insbesondere in Art. 58 Abs. 8, genannten Befugnisse auszuüben.

(2) Der Bundeskanzler ist ermächtigt,

1. nach Maßgabe von Art. 58 Abs. 8 Buchstabe c der Verordnung (EU) 2019/881
   a) Einsicht in die nach der Verordnung (EU) 2019/881 oder einem Schema für die Cybersicherheitszertifizierung durch Konformitätsbewertungsstellen, Inhaber europäischer Cybersicherheitszertifikate und Aussteller von EU-Konformitätserklärungen zu führenden Aufzeichnungen zu erhalten.
   b) Konformitätsbewertungsstellen, Inhabern europäischer Cybersicherheitszertifikate und Ausstellern von EU-Konformitätserklärungen zur Herstellung der Anforderungen nach der Verordnung (EU) 2019/881 oder einem europäischen Schema für die Cybersicherheitszertifizierung Empfehlungen auszusprechen. Für deren Befolgung und entsprechenden Nachweis kann erforderlichenfalls eine angemessene Frist gesetzt sowie die Befolgung bescheidmäßig angeordnet werden.
   c) von Konformitätsbewertungsstellen, Inhabern europäischer Cybersicherheitszertifikate und Ausstellern von EU-Konformitätserklärungen zu verlangen, dass IKT-Produkte, -Dienste und -Prozesse auf eigene Kosten an einem dafür bestimmten Ort und zu einem dafür bestimmten Zeitpunkt zur Prüfung bereitgestellt werden, wenn die Beurteilung, ob IKT-Produkte, -Dienste und -Prozesse der Verordnung (EU) 2019/881 oder einem europäischen Schema für die Cybersicherheitszertifizierung entsprechen, nicht ohne weiteres an Ort und Stelle getroffen werden kann und der Transport des IKT-Produkts, -Dienstes und -Prozesses ohne weiteres möglich ist. Der Bundeskanzler kann IKT-Produkte, -Dienste und -Prozesse von einer hierzu befugten Konformitätsbewertungsstelle oder einer sachkundigen Person oder Einrichtung prüfen lassen.

d) IKT-Produkte, -Dienste und -Prozesse zu besichtigen und in Betrieb nehmen zu lassen sowie, unbeschadet von Z 2, vor Ort zu prüfen oder prüfen zu lassen. Der Bundeskanzler kann erforderlichenfalls sachkundige Personen und Einrichtungen beiziehen.

2. im Zuge der Ausübung der Befugnis nach Art. 58 Abs. 8 Buchstabe d der Verordnung (EU) 2019/881 ist die Nachschau, außer bei Gefahr im Verzug, während der üblichen Geschäfts- oder Betriebsstunden und unter Beiziehung eines informierten Betriebsangehörigen vorzunehmen. Bei der Nachschau ist darauf Bedacht zu nehmen, dass jede nicht unbedingt erforderliche Störung oder Behinderung des Betriebes vermieden wird. Der Bundeskanzler kann erforderlichenfalls sachkundige Personen und Einrichtungen beiziehen.
3. nach Maßgabe von Art. 58 Abs. 8 Buchstabe e und f der Verordnung (EU) 2019/881 europäische Cybersicherheitszertifikate, die von den nationalen Behörden für die Cybersicherheitszertifizierung oder nach Art. 56 Abs. 6 der Verordnung (EU) 2019/881 von den Konformitätsbewertungsstellen ausgestellt wurden, zu widerrufen sowie EU-Konformitätserklärungen im Sinne der Verordnung (EU) 2019/881 für ungültig zu erklären, sofern diese Zertifikate oder EU-Konformitätserklärungen den Anforderungen der Verordnung (EU) 2019/881 oder eines europäischen Schemas für die Cybersicherheitszertifizierung nicht genügen und einer Anordnung nach Z 1 lit. b nicht nachgekommen wurde.

Datenverarbeitung

§ 5. (1) Der Bundeskanzler ist zum Zwecke der Erfüllung der in der Verordnung (EU) 2019/881 und in diesem Hauptstück definierten Aufgaben als datenschutzrechtlicher Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO ermächtigt, personenbezogene Daten im Sinne des Art. 4 Nr. 1 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DSGVO), ABl. Nr. L 119 vom 04.05.2016 S. 1, in der Fassung der Berichtigung ABl. Nr. L 74 vom 04.03.2021 S. 35, zu verarbeiten.

(2) Bei den in Abs. 1 genannten personenbezogenen Daten handelt es sich insbesondere um:

1. Kontakt- und Identitätsdaten von Teilnehmern und ihren Organisationseinheiten, die zur Ermöglichung und im Zuge der Teilnahme an internationalen, EU-weiten und nationalen Gremien mit Relevanz für die Cybersicherheitszertifizierung erforderlich sind;
2. Daten von Personen, die an einem Geschäftsfall mitwirken oder davon betroffen sind, insbesondere von Konformitätsbewertungsstellen, Herstellern und Anbietern von IKT-Produkten, -Diensten und -Prozessen, Inhabern europäischer Cybersicherheitszertifikate und Ausstellern von EU-Konformitätserklärungen sowie von Antragstellern und Beschwerdeführern nach der Verordnung (EU) 2019/881 und nach diesem Hauptstück;
3. Daten von Personen sowie technische Daten, die mit einer gemäß § 3 Abs. 3 erfolgten Mitteilung über eine festgestellte Sicherheitslücke oder Unregelmäßigkeit in Zusammenhang stehen.

(3) Jede Abfrage, Übermittlung und Änderung personenbezogener Daten ist zu protokollieren. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen.

(4) Personenbezogene Daten sind unverzüglich zu löschen, sofern sie zur Wahrnehmung der festgelegten Befugnisse und Aufgaben nicht mehr erforderlich sind, spätestens aber sieben Jahre nach rechtskräftiger Entscheidung eines Verfahrens.

4. Abschnitt

Cybersicherheitszertifizierung für die Vertrauenswürdigkeitsstufe „hoch“

Allgemeine Ermächtigung zur Ausstellung von europäischen Cybersicherheitszertifikaten

§ 6. Der Bundeskanzler kann nach Maßgabe von Art. 56 Abs. 6 Buchstabe b der Verordnung (EU) 2019/881 die Aufgabe der Ausstellung von europäischen Cybersicherheitszertifikaten, für die im Rahmen eines europäischen Schemas für die Cybersicherheitszertifizierung die Vertrauenswürdigkeitsstufe „hoch“ erforderlich ist, allgemein einer Konformitätsbewertungsstelle übertragen.

5. Abschnitt

Strafbestimmungen

Verwaltungsstrafbestimmungen

§ 7. (1) Eine Verwaltungsübertretung begeht, wer

1. einem Auskunftsverlangen gemäß Art. 58 Abs. 8 Buchstabe a der Verordnung (EU) 2019/881 nicht oder nicht vollständig nachkommt;
2. einem Untersuchungsverlangen gemäß Art. 58 Abs. 8 Buchstabe b der Verordnung (EU) 2019/881 nicht nachkommt;
3. einem Einsichtsverlangen in die Aufzeichnungen gemäß § 4 Abs. 2 Z 1 lit. a iVm Art. 58 Abs. 8 Buchstabe c der Verordnung (EU) 2019/881 nicht nachkommt;
4. die bescheidmäßig ergangenen Anordnungen gemäß § 4 Abs. 2 Z 1 lit. b iVm Art. 58 Abs. 8 Buchstabe c der Verordnung (EU) 2019/881 nicht oder nicht fristgerecht umsetzt;
5. einer Überprüfungsaufforderung gemäß § 4 Abs. 2 Z 1 lit. c iVm Art. 58 Abs. 8 Buchstabe c der Verordnung (EU) 2019/881 nicht nachkommt;
6. einem Besichtigungs-, Inbetriebnahme- oder Prüfungsverlangen gemäß § 4 Abs. 2 Z 1 lit. d iVm Art. 58 Abs. 8 Buchstabe c der Verordnung (EU) 2019/881 nicht nachkommt;
7. keinen Zugang zu den Räumlichkeiten gemäß § 4 Abs. 2 Z 2 iVm Art. 58 Abs. 8 Buchstabe d der Verordnung (EU) 2019/881 gewährt oder
8. entgegen der Vorgaben von § 6 oder Art. 60 Abs. 3 der Verordnung (EU) 2019/881 Cybersicherheitszertifikate ausstellt.

Die Begehung ist mit Geldstrafe bis zu 50 000 Euro, im Wiederholungsfall bis zu 100 000 Euro, zu bestrafen.

(2) Die Bezirksverwaltungsbehörden sind für die Verhängung von Geldstrafen nach diesem Bundesgesetz zuständig. Sie haben den Bundeskanzler unverzüglich über jede rechtskräftige Bestrafung nach Abs. 1 Z 1 bis 8 unter Angabe der Verwaltungsübertretung und der Höhe der verhängten Geldstrafe zur Wahrnehmung seiner Aufgabe gemäß Art. 58 Abs. 7 lit. g iVm Abs. 8 lit. f der Verordnung (EU) 2019/881 zu informieren.

(3) Eine Verwaltungsübertretung gemäß Abs. 1 liegt nicht vor, wenn die Tat den Tatbestand einer in die Zuständigkeit der ordentlichen Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist.

(4) Die Bezirksverwaltungsbehörden können Geldstrafen gegen eine juristische Person oder eingetragene Personengesellschaft verhängen, wenn Verwaltungsübertretungen gemäß Abs. 1 durch Personen begangen wurden, die entweder allein oder als Teil eines Organs der juristischen Person oder der eingetragenen Personengesellschaft gehandelt haben und eine Führungsposition aufgrund

1. der Befugnis zur Vertretung der juristischen Person oder der eingetragenen Personengesellschaft,
2. der Befugnis, Entscheidungen im Namen der juristischen Person oder der eingetragenen Personengesellschaft zu treffen, oder
3. einer Kontrollbefugnis innerhalb der juristischen Person oder der eingetragenen Personengesellschaft

innehaben.

(5) Juristische Personen oder eingetragene Personengesellschaften können wegen Verwaltungsübertretungen gemäß Abs. 1 auch verantwortlich gemacht werden, wenn mangelnde Überwachung oder Kontrolle durch eine in Abs. 4 genannte Person die Begehung dieser Verstöße durch eine für die juristische Person oder der eingetragenen Personengesellschaft tätige Person ermöglicht hat, sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung erfüllt.

(6) Von der Bestrafung eines Verantwortlichen gemäß § 9 des Verwaltungsstrafgesetzes 1991 – VStG, BGBl. Nr. 52/1991, kann abgesehen werden, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird.

(7) Gegen Behörden und sonstige Stellen der öffentlichen Verwaltung, unabhängig davon, ob sie hoheitlich oder im Rahmen der Privatwirtschaftsverwaltung eingerichtet oder tätig sind, können keine Geldstrafen verhängt werden.

6. Abschnitt
Schlussbestimmungen

Personenbezogene Bezeichnungen

§ 8. Alle in diesem Bundesgesetz verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für alle Geschlechter.

Verweisungen

§ 9. Verweisungen in diesem Bundesgesetz auf andere Bundesgesetze sind als Verweisungen auf die jeweils geltende Fassung zu verstehen.

Vollziehung

§ 10. (1) Mit der Vollziehung dieses Bundesgesetzes ist der Bundeskanzler betraut.

(2) Die Mitarbeiter des Vereins „Zentrum für sichere Informationstechnologie – Austria (A-SIT)“ stehen dem Bundeskanzler als Amtssachverständige zur Verfügung.

Inkrafttreten

§ 11. Dieses Bundesgesetz tritt mit xx. xxx 2024 in Kraft.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-05-15T12:33:20+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	