1 von 7

Entwurf

Erläuterungen

I. Allgemeiner Teil

Am 27. Juni 2019 trat die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (IKT) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit), ABl. Nr. L 151 vom 17.04.2019 S. 15, auf Englisch „Cybersecurity Act“ (kurz CSA), in Kraft. Der CSA verpflichtet die Mitgliedstaaten zur Benennung von nationalen Behörden für die Cybersicherheitszertifizierung zur Aufsicht und Durchführung des CSA und der sich aus diesem ableitenden europäischen Schemata für die Cybersicherheitszertifizierung. Mit dem vorliegenden Gesetzesvorhaben werden die innerstaatliche Maßnahmen zur Durchführung des CSA erlassen. Aufgrund der Verbote der speziellen Transformation, der inhaltlichen Präzisierung und der inhaltlichen Wiederholung von EU-Verordnungen wird nur das unionsrechtlich zwingend Erforderliche geregelt.

Der CSA schafft u.a. einen europäischen Zertifizierungsrahmen für die Cybersicherheit. Dieser legt einen Mechanismus fest, mit dem europäische Schemata für die Cybersicherheitszertifizierung geschaffen werden. In weiterer Folge soll der europäische Zertifizierungsrahmen für die Cybersicherheit bescheinigen, dass IKT-Produkte, -Dienste und -Prozesse, die nach einem solchen Schema bewertet wurden, den festgelegten Sicherheitsanforderungen genügen. Anbieter und Hersteller können sich zukünftig freiwillig zu einer Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen entscheiden. Doch zeichnen sich verpflichtende Zertifizierungen in anderen derzeit auf EU-Ebene befindlichen Rechtsakten ab, etwa bei der Brieftasche für die Europäische Digitale Identität. Ein Cybersicherheitszertifikat wird EU-weit anerkannt. Durch den Nachweis, dass ein Produkt oder Dienst die angegebenen Sicherheitsfunktionen erfüllt oder bestimmte Sicherheitsanforderungen einhält, kann Cybersicherheitszertifizierung wesentlich dazu beitragen, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu stärken und damit das ordnungsgemäße Funktionieren des digitalen Binnenmarktes gewährleisten.

Derzeit befinden sich drei Schemata für die Cybersicherheitszertifizierung auf EU-Ebene in Ausarbeitung. Das „European Union Common Criteria Scheme“ (EUCC) soll der Nachfolger des bestehenden SOG-IS (Senior Officials Group Information Systems Security) und MRA (Mutual Recognition Agreement) werden. Unter dem EUCC wird eine Zertifizierung der Cybersicherheit von IKT-Produkten vorgesehen. Das EUCC basiert auf Common Criteria, Common Methodology for Information Technology Security Evaluation und den entsprechenden Normen ISO/IEC 15408 und ISO/IEC 18045. Des Weiteren wird das „European Union Cybersecurity Certification Scheme on Cloud Services“ (EUCS) erarbeitet, welches die Sicherheit von Cloud-Diensten regeln soll. Ziel ist es, die Sicherheit von Cloud-Diensten mit EU-Vorschriften, internationalen Standards, bewährten Praktiken der Industrie sowie mit bestehenden Zertifizierungen in EU-Mitgliedstaaten zu harmonisieren und das Vertrauen in Cloud-Dienste zu stärken. Das dritte in Ausarbeitung befindliche Schema läuft unter dem Namen EU5G und hat die Cybersicherheit von 5G-Netzwerken zum Gegenstand. Das Schema soll sich beim Anwendungsbereich auf das GSMA Network Equipment Security Assurance Scheme sowie auf relevante Common Criteria-Schutzprofile für embedded Universal Integrated Circuit Card (eUICC) beziehen.

Die Hauptgesichtspunkte sind im Einzelnen:

- Einrichtung einer nationalen Behörde für die Cybersicherheitszertifizierung.

Zuständigkeit des Bundes

Die Zuständigkeit des Bundes für die Erlassung und Vollziehung dieses Bundesgesetzes beruht auf dem Kompetenztatbestand „Angelegenheiten des Gewerbes und der Industrie“ gemäß Art. 10 Abs. 1 Z 8 B-VG.

II. Besonderer Teil

Zu § 1 (Anwendungsbereich und Durchführung von Rechtsakten der EU)

Gegenstand des vorliegenden Bundesgesetzes soll die Durchführung bestimmter Aspekte des CSA sein. Insbesondere hat jeder Mitgliedstaat gemäß Art. 58 Abs. 1 CSA eine oder mehrere nationale Behörden für die Cyber- und digitale Sicherheitszertifizierung in seinem Hoheitsgebiet zu benennen.

Zu § 2 (Begriffsbestimmungen)

§ 2 stellt klar, dass für die in diesem Bundesgesetz verwendeten Begriffe die Begriffsbestimmungen in Art. 2 CSA gelten sollen. Dies bezieht sich insbesondere auf die im vorliegenden Bundesgesetz häufig verwendeten Begriffe europäisches Cybersicherheitszertifikat (siehe Art. 2 Nr. 11 CSA), europäisches Schema für die Cybersicherheitszertifizierung (siehe Art. 2 Nr. 9 CSA), IKT-Produkt (siehe Art. 2 Nr. 12 CSA), IKT-Dienst (siehe Art. 2 Nr. 13 CSA), IKT-Prozess (siehe Art. 2 Nr. 14 CSA), Vertrauenswürdigkeitsstufe (siehe Art. 2 Nr. 21 CSA) und Selbstbewertung der Konformität (siehe Art. 2 Nr. 22 CSA).

Wird in diesem Bundesgesetz auf ein europäisches Schema für die Cybersicherheitszertifizierung Bezug genommen, so soll darunter jeweils das Schema verstanden werden, nach welchem ein bestimmtes IKT-Produkt, ein bestimmter IKT-Dienst oder ein bestimmter IKT-Prozess zertifiziert oder eine Selbstbewertung der EU-Konformität durchgeführt wurde.

Zu § 3 (Einrichtung und Aufgaben der nationalen Behörde für die Cybersicherheitszertifizierung)

Abs. 1:

Gemäß Art. 58 Abs. 1 CSA hat jeder Mitgliedstaat eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung in seinem Hoheitsgebiet zu benennen. Mit § 3 Abs. 1 soll Art. 58 CSA durchgeführt und für Österreich der Bundeskanzler als nationale Behörde für die Cybersicherheitszertifizierung benannt werden. Daraus folgt, dass der Bundeskanzler die Aufgaben der nationalen Behörde für die Cybersicherheitszertifizierung, die sich insbesondere aus Art. 58 Abs. 7 CSA ergeben, wahrnehmen soll.

Abs. 2:

Durch Abs. 2 soll der Bundeskanzler verpflichtet werden, die Tätigkeiten der Ausstellung von Zertifikaten nach Art. 56 Abs. 5 Buchstabe a CSA und Abs. 6 von den Aufsichtstätigkeiten organisatorisch streng zu trennen. Dies kann dadurch erreicht werden, indem beispielsweise unterschiedliche Organisationseinheiten mit den jeweiligen Tätigkeiten betraut werden. Dadurch soll der in Art. 58 Abs. 4 CSA geforderten Differenzierung und Unabhängigkeit der Aufsichts- und Zertifizierungstätigkeiten entsprochen werden.

Abs. 3:

Art. 56 Abs. 8 CSA sieht vor, dass der Inhaber eines europäischen Cybersicherheitszertifikats bestimmte in Art. 57 Abs. 7 CSA genannte Behörden oder Stellen über etwaige später festgestellte Sicherheitslücken oder Unregelmäßigkeiten hinsichtlich der Sicherheit des zertifizierten IKT-Produkts, -Dienstes oder -Prozesses, die sich auf die mit der Zertifizierung verbundenen Anforderungen auswirken könnten, zu informieren hat. Die Behörden oder Stellen haben diese Informationen ihrerseits unverzüglich an die nationale Behörde für die Cybersicherheitszertifizierung weiterzuleiten. In Abs. 3 soll nunmehr vorgesehen werden, dass der Bundeskanzler diese Informationen an den IKDOK zu melden hat. Der IKDOK wurde durch § 7 Abs. 1 des Netz- und Informationssystemsicherheitsgesetzes (NISG), BGBl. I Nr. 111/2018, eingerichtet und ist eine interministerielle Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen bestehend aus Vertretern des Bundeskanzlers, des Bundesministers für Inneres, des Bundesministers für Landesverteidigung und des Bundesministers für europäische und internationale Angelegenheiten. Durch die Weiterleitungspflicht soll das im IKDOK zu erörternde und zu aktualisierende Lagebild um das Wissen über entsprechende Sicherheitslücken oder Unregelmäßigkeiten in zertifizierten IKT-Produkten, -Diensten oder –Prozessen angereichert werden.

Abs. 4:

Durch Abs. 4 soll sichergestellt werden, dass die Zuständigkeiten anderer Marktüberwachungsbehörden von der Zuständigkeit des Bundeskanzlers als nationale Behörde für die Cybersicherheitszertifizierung unberührt bleiben. Dem Bundeskanzler obliegt gemäß Art. 58 Abs. 7 Buchstabe a CSA in Zusammenarbeit mit diesen anderen zuständigen Marktüberwachungsbehörden die Überwachung und Durchsetzung der Vorschriften im Rahmen der europäischen Schemata für die Cybersicherheitszertifizierung im Hinblick auf die Beobachtung der Übereinstimmung der IKT-Produkte, -Dienste und -Prozesse mit den Anforderungen der in ihrem jeweiligen Hoheitsgebiet ausgestellten europäischen Cybersicherheitszertifikate.

Erläuterung zur Durchführung von Art. 60 Abs. 3 CSA:

Die Befugnis des Bundeskanzlers gemäß Art. 60 Abs. 3 CSA, nur solchen Konformitätsbewertungsstellen, welche die in einem Schema gemäß Art. 54 Abs. 1 Buchstabe f CSA festgelegten spezifischen oder zusätzlichen Anforderungen einhalten, die Befugnis zu erteilen, Aufgaben im Rahmen dieses Schemas wahrzunehmen, soll mit Bescheid erteilt werden. Liegen die Anforderungen nicht (mehr) vor, soll das Ansuchen mit Bescheid abgewiesen oder die bereits ausgestellte Ermächtigung aberkannt werden. Die Bearbeitung soll durch die Organisationseinheit im Bundeskanzleramt erfolgen, der die Aufsichtstätigkeiten obliegen (vgl. § 3 Abs. 2).

Erläuterung zur Durchführung von Art. 63 CSA:

Was die Bearbeitung von Beschwerden nach Art. 63 CSA betrifft, so soll die Organisationseinheit, der die Aufsichtstätigkeiten obliegen (vgl. § 3 Abs. 2), die Beschwerden von natürlichen und juristischen Personen im Zusammenhang mit § 64 und Art. 56 Abs. 5 Buchstabe a CSA bearbeiten.

Zu § 4 (Befugnisse):

Mit § 4 sollen die in Art. 58 Abs. 8 CSA aufgezählten Befugnisse ausdrücklich dem Bundeskanzler zugewiesen werden. Bei den in Art. 58 Abs. 8 CSA genannten Befugnissen handelt es sich um eine demonstrative Aufzählung. Die Befugnisse werden dort konkretisiert, wo der CSA dies vorsieht, insbesondere, wenn er die Ausübung von Befugnissen im „Einklang mit dem nationalen Recht“ vorgibt.

Erläuterung zur Durchführung von Art. 58 Abs. 8 Buchstabe a CSA:

Die Befugnisse gemäß Art. 58 Abs. 8 Buchstaben a und b CSA bedürfen keiner Durchführung. Art. 58 Abs. 8 Buchstabe a CSA normiert ein Auskunftsrecht der nationalen Behörde für die Cybersicherheitszertifizierung gegenüber den Konformitätsbewertungsstellen, den Inhabern europäischer Cybersicherheitszertifikate und den Ausstellern von EU-Konformitätserklärungen, wobei unter sämtlichen Auskünften sowohl mündliche als auch schriftliche Auskünfte zu verstehen sein dürfen. Wer dem Auskunftsverlangen nicht oder nicht vollständig nachkommt, begeht eine Verwaltungsstrafe gemäß § 7 Abs. 1 Z 1.

Erläuterung zur Durchführung von Art. 58 Abs. 8 Buchstabe b CSA:

Gemäß Art. 58 Abs. 8 Buchstabe b CSA ist die nationale Behörde für die Cybersicherheitszertifizierung befugt, Untersuchungen in Form von Rechnungsprüfungen bei den Konformitätsbewertungsstellen, den Inhabern europäischer Cybersicherheitszertifikate und den Ausstellern von EU-Konformitätserklärungen durchzuführen. Die Untersuchungen müssen geeignet sein, die Einhaltung der Bestimmungen eines Schemas bzw. des CSA zu überprüfen. Der Begriff der Rechnungsprüfung dürfte im Kontext der Zertifizierung weit – in die Richtung Auditierung – zu verstehen sein, wie dies auch in der englischen und französischen Version („audits“) der Fall ist. Wer dem Untersuchungsverlangen nicht vollständig nachkommt, begeht eine Verwaltungsstrafe gemäß § 7 Abs. 1 Z 2.

Abs. 2 Z 1:

Abs. 2 Z 1 führt den weit formulierten Art. 58 Abs. 8 Buchstabe c CSA durch. Gemäß Art. 58 Abs. 8 Buchstabe c CSA kann die nationale Behörde für die Cybersicherheitszertifizierung geeignete Maßnahmen ergreifen, um sicherzustellen, dass die Konformitätsbewertungsstellen, die Inhaber von europäischen Cybersicherheitszertifikaten und die Aussteller von EU-Konformitätserklärungen den Anforderungen des CSA oder eines europäischen Schemas für die Cybersicherheitszertifizierung genügen. Abs. 2 Z 1 soll im Hinblick auf das Bestimmtheitsgebot diese sehr allgemeine Befugnis der nationalen Behörde für die Cybersicherheitszertifizierung in Form von konkreten Einzelbefugnissen durchführen.

Abs. 2 Z 1 lit. a:

Nach Abs. 2 Z 1 lit. a wird ein Einsichtsrecht des Bundeskanzlers in die nach dem CSA oder einem Schema durch Konformitätsbewertungsstellen, Inhaber europäischer Cybersicherheitszertifikate und

Aussteller von EU-Konformitätserklärungen zu führenden Aufzeichnungen vorgesehen. Das Einsichtsrecht ist notwendig, damit der Bundeskanzler auch die in Abs. 2 Z 1 lit. c mögliche Befugnis wahrnehmen kann. Die Einsicht in die zu führenden Aufzeichnungen wird insbesondere im Wege der schriftlichen Auskünfte gemäß Art. 58 Abs. 8 Buchstabe a CSA, in Form von Rechnungsprüfungen gemäß Art. 58 Abs. 8 Buchstabe b CSA und im Zuge der Betretung der Räumlichkeiten gemäß Abs. 2 Z 2 ermöglicht. Vom Einsichtsrecht unbeschadet bleiben Informationspflichten an die nationale Behörde für die Cybersicherheitszertifizierung, wie etwa die Verpflichtung gemäß Art. 53 Abs. 3 CSA.

Abs. 2 Z 1 lit. b:

Nach Abs. 2 Z 1 lit. b ist der Bundeskanzler befugt, gegenüber Konformitätsbewertungsstellen, Inhabern europäischer Cybersicherheitszertifikate und Ausstellern von EU-Konformitätserklärungen (Handlungs-)Empfehlungen auszusprechen, wenn diese den Anforderungen nach dem CSA oder einem Schema nicht entsprechen. Der Bundeskanzler kann, soweit dies erforderlich ist, auch einen Nachweis für die Befolgung der Empfehlung verlangen. Dafür ist eine angemessene Frist zu setzen. Wird den Empfehlungen nicht innerhalb dieser Frist nachgekommen, so ist deren Befolgung bescheidmäßig und unter Androhung einer Sanktion (siehe auch § 7 Abs. 1 Z 4) anzuordnen. Die Befugnis nach Abs. 2 Z 1 lit. b stellt eine besonders geeignete Maßnahme im Sinne des Art. 58 Abs. 8 Buchstabe c CSA dar. Durch diese Befugnis kann auch Art. 58 Abs. 8 Buchstabe f CSA durchgeführt werden, nach welchem eine Anordnung der Behörde zur unverzüglichen Beendigung von Verstößen gegen die im CSA festgelegten Verpflichtungen vorgesehen werden kann.

Abs. 2 Z 1 lit. c:

Nach Abs. 2 Z 1 lit. c kann der Bundeskanzler von Konformitätsbewertungsstellen, Inhabern europäischer Cybersicherheitszertifikate und Ausstellern von EU-Konformitätserklärungen verlangen, dass IKT-Produkte, -Dienste und -Prozesse auf Kosten der Konformitätsbewertungsstellen, Inhabern europäischer Cybersicherheitszertifikate und Ausstellern von EU-Konformitätserklärungen an einem dafür bestimmten Ort und zu einem dafür bestimmten Zeitpunkt zur Prüfung bereitgestellt werden. Mit solchen Prüfungen soll insbesondere die Überprüfung der Einhaltung der Anforderungen an technische Parameter durch IKT-Produkte, -Dienste und -Prozesse möglich sein. Voraussetzung für die Ausübung der Befugnis ist einerseits, dass die Beurteilung, ob IKT-Produkte, -Dienste und -Prozesse dem CSA oder einem Schema entsprechen, nicht ohne weiteres an Ort und Stelle getroffen werden kann. Dies ist zB dann der Fall, wenn eine Untersuchung der IKT-Produkte, -Dienste und -Prozesse nur mit bestimmten Werkzeugen, die physisch nicht an Ort und Stelle gebracht werden können, oder mit Methoden, die nur in bestimmten Prüflaboren angewendet werden können, möglich ist. Voraussetzung für die Ausübung dieser Befugnis ist andererseits, dass die IKT-Produkte, -Dienste und -Prozesse selbst ohne weiteres transportiert werden können. Ohne weiteres ist dabei u.a. so zu verstehen, dass sich der Aufwand des Transports nicht ungebührlich teuer und aufwendig darstellt. Der zu bestimmende Zeitpunkt muss in diesem Zusammenhang auch den Transportweg berücksichtigen. Mit dem zu bestimmenden Ort sind in erster Linie die Örtlichkeiten des Bundeskanzleramtes als Behörde für die Cybersicherheitszertifizierung selbst oder jener von Konformitätsbewertungsstellen oder sonstigen sachkundigen Personen oder Einrichtungen gemeint, die die IKT-Produkte, -Dienste und -Prozesse im Auftrag des Bundeskanzlers prüfen.

Abs. 2 Z 1 lit. d:

Nach Abs. 2 Z 2 lit. d ist der Bundeskanzler befugt, IKT-Produkte, -Dienste und -Prozesse zu besichtigen und in Betrieb zu nehmen sowie vor Ort zu prüfen oder prüfen zu lassen. Hierdurch soll die Einhaltung der Anforderungen an technische Parameter durch IKT-Produkte, -Dienste und -Prozesse auch in einem Echtzeitbetrieb überprüft werden können. Um die in hochtechnischen Fällen allenfalls erforderliche externe Expertise im Zuge dessen gewährleisten zu können, sollen auch vom Bundeskanzler beauftragte sachkundige Personen oder Einrichtungen beigezogen werden können, wobei diese auch technische Prüfhandlungen vornehmen können sollen.

Abs. 2 Z 2:

Abs. 2 Z 2 konkretisiert die Ausübung des der nationalen Behörde für die Cybersicherheitszertifizierung in Art. 58 Abs. 8 Buchstabe d CSA eingeräumte Recht, Zugang zu den Räumlichkeiten von Konformitätsbewertungsstellen und von Inhabern europäischer Cybersicherheitszertifikate zum Zweck der Durchführung von Untersuchungen zu erhalten. Die Ausübung dieser Befugnis hat im Einklang mit den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit zu erfolgen. Die Nachschau ist, außer bei Gefahr im Verzug, nur während der üblichen Geschäfts- oder Betriebsstunden und unter Beiziehung eines informierten Betriebsangehörigen zulässig. Des Weiteren ist bei der Nachschau darauf Bedacht zu nehmen, dass jede nicht unbedingt erforderliche Störung oder Behinderung des Betriebes vermieden wird. Rechte der betroffenen Konformitätsbewertungsstellen und Inhaber europäischer

Cybersicherheitszertifikate, wie zB Geschäfts- und Betriebsgeheimnisse, und Rechte Dritter, wie zB Datenschutzrechte sowie auch der Betrieb, also etwa der Betriebsablauf und Sicherheitsregeln (wie zB Safety-Anforderungen), sind möglichst zu schonen bzw. zu beachten. Um den erforderliche technischen Sachverstand während der Untersuchung zu gewährleisten, kann der Bundeskanzler sachkundige Personen oder Einrichtungen beiziehen. Im Unterschied zu Z 1 lit. c, die durch diese Ziffer unbeschadet bleibt, wird auf Untersuchungen vor Ort Bezug genommen, denn Z 1 lit. c soll insbesondere Fälle abdecken, wo eine ausreichende technische Untersuchung der IKT-Produkte, -Dienste und -Prozesse in den Räumlichkeiten nicht ohne weiteres möglich ist. Aussteller von EU-Konformitätserklärungen sind von Z 2 nicht umfasst. Während Abs. 2 Z 2 lit. d die Befugnis zur Inbetriebnahme und Prüfung der IKT-Produkte, -Dienste und -Prozesse vor Ort regelt, ermöglicht Z 2 den Zugang zu den Räumlichkeiten, wo diese IKT-Produkte, -Dienste und -Prozesse gelegen sind. Auch kann im Rahmen des Rechtes auf Zugang zu den Räumlichkeiten Einsicht in dort befindliche Aufzeichnungen gemäß Abs. 2 Z lit. a genommen werden.

Abs. 2 Z 3:

Abs. 2 Z 3 regelt in Durchführung von Art. 58 Abs. 8 Buchstabe e CSA den Widerruf von Zertifikaten, die den Anforderungen des CSA oder eines Schemas nicht genügen. Der Widerruf von Cybersicherheitszertifikaten folgt dem Prinzip, dass der Bundeskanzler nur jene europäischen Cybersicherheitszertifikate widerrufen kann, welche von ihm selbst oder aber von Konformitätsbewertungsstellen, die von ihm die Zustimmung bzw. Ermächtigung zur Ausstellung von europäischen Cybersicherheitszertifikaten für die Vertrauenswürdigkeitsstufe „hoch“ gemäß Art. 56 Abs. 6 CSA (iVm § 6) erhalten haben, ausgestellt wurden. Darüber hinaus sollen EU-Konformitätserklärungen in Durchführung von Art. 58 Abs. 8 Buchstabe f CSA durch den Bundeskanzler für ungültig erklärt werden können, wenn sie den Anforderungen des CSA oder eines europäischen Schemas für die Cybersicherheitszertifizierung nicht genügen. Diese Möglichkeit zum Widerruf von oben genannten Zertifikaten und zur Ungültigkeitserklärung von EU-Konformitätserklärungen soll auch bestehen, wenn einer Anordnung des Bundeskanzlers gemäß Abs. 2 Z 1 lit. b nicht nachgekommen wurde, um die unverzügliche Beendigung von Verstößen gegen die im CSA festgelegten Verpflichtungen sicherstellen zu können.

Zu § 5 (Datenverarbeitung):

In § 5 werden datenschutzrechtliche Bestimmungen zur Verarbeitung von personenbezogenen Daten im Sinne des Art. 4 Z 1 DSGVO geregelt. Der Bundeskanzler als nationale Behörde für die Cybersicherheitszertifizierung wird in § 5 Abs. 1 explizit ermächtigt, personenbezogene Daten, die zur Wahrnehmung sämtlicher Aufgaben und Befugnisse nach dem CSA sowie damit in Verbindung stehend §§ 3, 4 und 6 erforderlich sind und in Abs. 2 näher bestimmt werden, zu verarbeiten. Beim Verarbeiten von personenbezogenen Daten sind jedenfalls die Grundsätze für die Verarbeitung personenbezogener Daten, wie insbesondere der Grundsatz der Zweckbindung (Art. 5 Abs. 1 Buchstabe b DSGVO), der Datenminimierung (Art. 5 Abs. 1 Buchstabe c DSGVO) und der Verhältnismäßigkeitsgrundsatz zu beachten. Die Datenverarbeitung wird im Rahmen der Aktenverwaltung insbesondere zum Zwecke der Dokumentation und zur Nachvollziehbarkeit der Tätigkeit, beispielsweise bei der Verwendung des ELAK, erfolgen.

Zu § 6 (Allgemeine Ermächtigung zur Ausstellung von Cybersicherheitszertifikaten):

Ein europäisches Schema für die Cybersicherheitszertifizierung kann für IKT-Produkte, -Dienste und -Prozesse eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ und/oder „hoch“ angeben (Art. 52 Abs. 1 erster Satz CSA). Die Vertrauenswürdigkeitsstufe bezeichnet dabei die Grundlage für das Vertrauen (zB von Verbraucher:innen oder Unternehmen) darin, dass ein IKT-Produkt, -Dienst oder -Prozess den Sicherheitsanforderungen eines europäischen Schemas für die Cybersicherheitszertifizierung genügt. Sie gibt an, auf welchem Niveau das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess bei der Bewertung eingestuft wurde (Art 4 Nr. 21 CSA). Aus der Vertrauenswürdigkeitsstufe ergibt sich die entsprechende Strenge und Gründlichkeit für die Bewertung des IKT-Produkts, -Dienstes oder –Prozesses. Die Wahl der Vertrauenswürdigkeitsstufe wiederum ergibt sich aus einem risikobasierten Ansatz, der von dem mit der beabsichtigten Verwendung eines IKT-Produkts, -Dienstes oder -Prozesses verbundenen Risiko im Hinblick auf die Wahrscheinlichkeit und die Auswirkungen eines Sicherheitsvorfalls ausgeht (Art. 52 Abs. 1 zweiter Satz CSA). Für die Vertrauenswürdigkeitsstufe „hoch“ sind entsprechend strenge Sicherheitsanforderungen vorzusehen und eine entsprechend gründliche Bewertung vorzunehmen, die darauf ausgerichtet ist, das Risiko von Cyberangriffen, die dem neuesten Stand der Technik entsprechen und durch Akteure mit umfangreichen Fähigkeiten und Ressourcen ausgeführt werden, möglichst gering zu halten (Art. 52 Abs. 7 CSA). Die Bewertung von IKT-Produkten, -Diensten und –Prozessen für die Vertrauenswürdigkeitsstufe „hoch“

erfordert daher ein entsprechend hohes Maß an Fachwissen und Fähigkeiten des Personals und entsprechend taugliche Prüfwerkzeuge.

Art. 56 Abs. 6 CSA gibt im Hinblick auf die Cybersicherheitszertifizierung für die Vertrauenswürdigkeitsstufe „hoch“ vor, dass das europäische Cybersicherheitszertifikat grundsätzlich nur von einer nationalen Behörde für die Cybersicherheitszertifizierung ausgestellt werden darf. Konformitätsbewertungsstellen dürfen Cybersicherheitszertifikate für die Vertrauenswürdigkeitsstufe „hoch“ nur ausstellen, wenn die nationale Behörde für die Cybersicherheitszertifizierung zuvor für jedes einzelne Cybersicherheitszertifikat ihre Zustimmung erteilt hat (Art. 56 Abs. 6 Buchstabe a CSA) oder ihnen die Aufgabe zuvor allgemein übertragen hat (Art. 56 Abs. 6 Buchstabe b CSA).

Mit § 6 wird Art. 56 Abs. 6 CSA dahingehend durchgeführt, dass von der Möglichkeit des Art. 56 Abs. 6 Buchstabe b CSA Gebrauch gemacht und der Bundeskanzler ermächtigt wird, 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 zu übertragen. Der Bundeskanzler kann eine solche allgemeine Ermächtigung auf Antrag einer Konformitätsbewertungsstelle durch Bescheid erteilen. Da die Ausstellung von Cybersicherheitszertifikaten für die Vertrauenswürdigkeitsstufe „hoch“ als Regelfall den nationalen Behörden für die Cybersicherheitszertifizierung vorbehalten ist, ist davon auszugehen, dass es sich bei der Erteilung der allgemeinen Ermächtigung der Konformitätsbewertungsstelle um eine Beleihung handelt.

Der CSA definiert keine näheren Kriterien, auf deren Grundlage eine nationale Behörde für die Cybersicherheitszertifizierung eine allgemeine Ermächtigung an eine Konformitätsbewertungsstelle gemäß Art. 56 Abs. 6 Buchstabe b CSA erteilen kann, weshalb (infolge des Transpositionsverbots) die allgemeinen Kriterien des CSA für Konformitätsbewertungsstellen als ausreichend erachtet werden müssen. Das heißt die betreffende Konformitätsbewertungsstelle muss (lediglich) akkreditiert und gegebenenfalls gemäß Art. 60 Abs. 3 CSA autorisiert sein.

Zu § 7 (Verwaltungsstrafbestimmungen):

Abs. 1:

Abs. 1 enthält Verwaltungsstrafbestimmungen in Bezug auf die Verletzung von Bestimmungen in Zusammenhang mit der Cybersicherheitszertifizierung. Gemäß Art. 65 CSA haben die Mitgliedstaaten Vorschriften über Sanktionen zu erlassen, die bei Verstößen gegen Titel III CSA und bei Verstößen gegen die europäischen Schemata für die Cybersicherheitszertifizierung zu verhängen sind. Die zu ahndenden Verwaltungsübertretungen stellen in Durchführung des Art. 65 CSA insbesondere Verstöße gegen Mitwirkungspflichten von juristischen und natürlichen Personen im Rahmen der Überprüfung von Anforderungen europäischer Cybersicherheitszertifikate auf Basis von § 4 iVm Art. 58 Abs. 8 CSA dar (Abs. 2 Z 1 bis 7). Die Strafhöhe orientiert sich an § 26 Abs. 1 NISG.

Hinsichtlich der in Abs. 1 Z 4 angesprochenen Anordnungen des Bundeskanzlers sollen insbesondere Fälle sanktioniert werden, in denen Konformitätsbewertungsstellen, Inhaber europäischer Cybersicherheitszertifikate und Aussteller von EU-Konformitätserklärungen einer Anordnung nicht, nicht richtig, nicht vollständig oder nicht binnen der gesetzten Frist nachkommen.

Abs. 1 Z 8 soll insbesondere der Vollziehung der europäischen Vorgaben zu Konformitätsbewertungsstellen, die im Anwendungsbereich des Art. 56 Abs. 6 und Art. 60 Abs. 3 CSA tätig werden, dienen. Die Sanktionierungsmöglichkeit muss bestehen, um die Tätigkeit von Konformitätsbewertungsstellen ohne die erforderliche Ermächtigung des Bundeskanzlers gemäß § 31 iVm Art. 56 Abs. 6 Buchstabe b CSA oder die erteilte Befugnis des Bundeskanzlers gemäß Art. 60 Abs. 3 CSA zu unterbinden. Dies gilt sowohl für nicht erteilte, als auch durch den Bundeskanzler widerrufene Ermächtigungen und Befugnisse.

Abs. 2:

Die Verwaltungsstrafen sollen von den Bezirksverwaltungsbehörden verhängt werden. Für die Erstellung des Jahresberichts gemäß Art. 57 Abs. 7 lit. g CSA sollen die Bezirksverwaltungsbehörden den Bundeskanzler unverzüglich über jede rechtskräftige Bestrafung nach Abs. 1 Z 1 bis 8 unter Angabe der Verwaltungsübertretung und der Höhe der verhängten Geldstrafe informieren.

Abs. 3:

Werden verschiedene strafbare Handlungen durch eine Tat verwirklicht, dann sind diese mit dem Doppelbestrafungsverbot gemäß Art. 4 7. ZPMRK nur dann vereinbar, wenn die strafbaren Handlungen nicht dieselben wesentlichen Elemente aufweisen (EGMR, Franz Fischer, 29.5.2001, 37.950/97). Dementsprechend liegt eine Verwaltungsübertretung gemäß Abs. 1 und 2 nur dann vor, wenn die Tat

nicht den Tatbestand einer in die Zuständigkeit der ordentlichen Gerichte fallenden strafbaren Handlung bildet oder nicht nach anderen Verwaltungsstrafbestimmungen mit einer strengeren Strafe bedroht ist.

Abs. 7:

Unter Berücksichtigung des Doppelstrafverbots und in Orientierung an § 30 Abs. 3 DSG kann von der Bestrafung eines Verantwortlichen gemäß § 9 VStG abgesehen werden, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wird.

Zu §§ 8 bis 11 (Schlussbestimmungen)

In den Schlussbestimmungen werden Regelungen in Hinblick auf die Verwendung personenbezogener Bezeichnungen, Verweisungen auf andere Bundesgesetze, die Vollziehung und das Inkrafttreten dieses Bundesgesetzes getroffen. Dieses Bundesgesetz soll mit xx. xxx 2024 in Kraft treten.