VORSCHLAG

Gemäß Artikel 116 Absatz 6 des Gesetzes über die elektronische Kommunikation (UL RS Nr. 130/22 und 18/23 – ZDU-1O) erlässt die Agentur für Kommunikationsnetze und -dienste der Republik Slowenien unter Berücksichtigung des Informationsverfahrens gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1) Folgendes:

ALLGEMEINES GESETZ
über zusätzliche Sicherheitsanforderungen und -beschränkungen

Artikel 1
(Inhalt des allgemeinen Gesetzes)

Dieses allgemeine Gesetz enthält:

1. Leitlinien für Betreiber von Mobilfunknetzen (im Folgenden „Betreiber“), die diese Netze kritischen Einrichtungen zur Verfügung stellen, die Betreiber kritischer Infrastrukturen in anderen Bereichen der Regulierung kritischer Infrastrukturen, wie im Gesetz über den Bereich der kritischen Infrastruktur (im Folgenden „Betreiber kritischer Infrastrukturen“) festgelegt, Anbieter wesentlicher Dienste im Sinne des Gesetzes über die Informationssicherheit (im Folgenden „Anbieter wesentlicher Dienste“), staatliche Verwaltungsbehörden gemäß dem Gesetz über die Informationssicherheit (im Folgenden „staatliche Verwaltungsbehörden“) oder Träger wichtiger Teile des Sicherheitssystems des Landes sind; und
2. kritische Netzelemente und zugehörige Informationssysteme mit ihren in Artikel 116 Absatz 6 des Gesetzes über die elektronische Kommunikation (UL RS Nr. 130/22 und 18/23 – ZDU-1O; im Folgenden „Gesetz“) genannten Funktionen, wie im Anhang aufgeführt, der integraler Bestandteil dieses allgemeinen Gesetzes ist und in Zusammenarbeit mit der für Informationssicherheit zuständigen Behörde ausgearbeitet wird.

Artikel 2
(Begriffsbestimmungen)

(1) Die in diesem allgemeinen Gesetz verwendeten Begriffe bedeuten:

1. Eine Lieferkette ist das gesamte System von Prozessen, Personen, Organisation und Vertrieb, die an Design, Produktion, Lagerung, Vertrieb und Lieferung sowie an der Installation und Wartung von Komponenten kritischer Netzelemente im Netz des Betreibers oder beim Cloud-Dienstleister, der solche Dienste für den Betreiber bereitstellt, beteiligt sind.

2. Kritische Netzelemente sind die Elemente des Netzes, Funktionen, Dienste und unterstützenden Informationssysteme in physischer oder virtualisierter Form oder in Form von Software beim Betreiber oder beim Cloud-Dienstleister, wie im Anhang zu diesem allgemeinen Gesetz aufgeführt.

3. Kritische Einrichtungen sind Betreiber kritischer Infrastrukturen in anderen Bereichen der Regulierung kritischer Infrastrukturen, die gemäß dem Gesetz über den Bereich der kritischen Infrastruktur bestimmt werden, und Anbieter wesentlicher Dienste gemäß dem Gesetz über die Informationssicherheit, staatliche Verwaltungsbehörden gemäß dem Gesetz über die Informationssicherheit und Träger wichtiger Teile des Sicherheitssystems des Landes.

(2) Andere Begriffe, die in diesem allgemeinen Gesetz verwendet werden, haben die gleiche Bedeutung wie im Gesetz und im Allgemeinen Gesetz über die Sicherheit von Netzen, Diensten und Daten.

Artikel 3
(Allgemeine Leitlinien)

(1) Die Betreiber in der Lieferkette von Komponenten kritischer Netzelemente und Third-Level-Support für diese Komponenten berücksichtigen mindestens die folgenden Leitlinien während des gesamten Lebenszyklus dieser Komponenten:

1. für einen einzelnen Hersteller oder Lieferanten und für einen Anbieter von Third-Level-Support aufgrund von Beziehungen und Vereinbarungen mit ihnen muss eine Risikobewertung in Bezug auf die Lieferung und mögliche Auswirkungen von Dritten, seien es natürliche oder juristische, öffentliche oder private Personen (im Folgenden „Dritte“), Kompatibilität mit Geräten anderer Hersteller, Produktqualität und -sicherheit sowie potenzielle negative Auswirkungen auf den Betrieb der Dienste des Betreibers und kritischer Einrichtungen durchgeführt werden;
2. dass die Sicherheit bereits im Entwurf integriert und umgesetzt wird und dass die Verträge Fristen für die Beseitigung wahrgenommener Schwachstellen enthalten;
3. dass wichtige Sicherheitsmerkmale (Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität) während des gesamten Lebenszyklus ihrer Nutzung gewährleistet sind,
4. dass die Sicherheit und ihre unterbrechungsfreie Versorgung gewährleistet sind dass sie gemäß international anerkannten Normen (3GPP) und europäischen technischen Normen (ETSI) zertifiziert sind;
5. dass die in den Nummern 2 bis 4 dieses Absatzes genannten Leitlinien in den Vertragsunterlagen mit dem Hersteller oder dem Lieferanten nachprüfbar sind;
6. für jeden Hersteller oder Anbieter werden auch die Risiken im Zusammenhang mit den Nutzungsrechten der Schlüsseltechnologien, die für die Herstellung und Nutzung der Ausrüstung erforderlich sind, und die Risiken im Zusammenhang mit der Lieferung von Ausrüstung, Ersatzteilen oder Third-Level-Support bewertet und berücksichtigt;
7. dass die verwendeten Komponenten keine bekannten kritischen Schwachstellen aufweisen, die noch nicht behoben wurden oder die aktiv ausgenutzt werden;
8. Vermeidung eines einzigen Herstellers oder Lieferanten, sofern dies technisch machbar und wirtschaftlich tragbar ist, mit dem Ziel, die Abhängigkeit zu verringern und die Widerstandsfähigkeit bei Schwachstellen kritischer Komponenten, katastrophalen Netzausfällen oder einer Bedrohung der Sicherheit von Netzen und Diensten kritischer Einrichtungen durch Dritte, seien es natürliche oder juristische, öffentliche oder private Personen, zu erhöhen.

(2) Bei der Bereitstellung von Informations- und Kommunikationsgeräten, -systemen und -diensten müssen die Betreiber die Leitlinien der Agentur der Europäischen Union für Cybersicherheit (im Folgenden „ENISA“) und die geltenden Vorschriften der Europäischen Union über grundlegende Sicherheitsanforderungen bei der Beschaffung sicherer IKT-Produkte und -Dienste uneingeschränkt einhalten. Die Agentur veröffentlicht auf ihrer Website Links zu aktuellen ENISA-Dokumenten und EU-Vorschriften in dem oben genannten Bereich und hält sie auf dem neuesten Stand.

(3) Bei der Lieferung von Komponenten kritischer Netzelemente oder der Nutzung von Cloud-Diensten sind vorrangig Komponenten von solchen Herstellern oder Lieferanten oder Dienste von Cloud-Diensteanbietern zu wählen, die von Konformitätsbewertungsstellen, die akkreditiert und erforderlichenfalls auf der Grundlage von Artikel 60 Absatz 3 der 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 die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (im Folgenden „Verordnung“) für die Ausstellung europäischer Cybersicherheitszertifikate auf einem bestimmten Sicherheitsniveau zertifiziert wurden, wie in Artikel 52 der Verordnung festgelegt.

(4) Für die Zwecke des vorstehenden Absatzes überprüft der Betreiber eine von der ENISA gemäß Artikel 55 der Verordnung eingerichtete spezielle Website, die die Öffentlichkeit über europäische Cybersicherheitszertifizierungssysteme, europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen informieren soll, einschließlich Informationen über nicht mehr gültige oder widerrufene europäische Cybersicherheitszertifizierungssysteme und abgelaufene europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen, sowie eine Sammlung von Links zu Cybersicherheitsinformationen.

Artikel 4
(Risikobewertung)

(1) Der Betreiber berücksichtigt die folgenden Risikoaspekte, wenn er das Risiko eines Herstellers oder Lieferanten von Komponenten und eines Anbieters von Third-Level-Support für kritische Netzelemente bewertet und bestimmt.

(2) Bei der Bewertung gemäß dem vorstehenden Absatz bewertet und berücksichtigt der Betreiber mindestens Folgendes:

1. Gesamtqualität (einschließlich Sicherheitsaspekte) und Zuverlässigkeit;
2. Umfang der Verwendung offener Standards und Schnittstellen, die Abhängigkeit und die Bindung an Produkte eines bestimmten Herstellers oder Lieferanten („Lock-in-Effekt“) verhindern;
3. Einhaltung anerkannter internationaler und europäischer technischer Normen (3GPP, ETSI) und EU-Vorschriften sowie Standardsicherheitseinstellungen gemäß den Branchenempfehlungen (GSMA Association);
4. Grad der Kompatibilität mit Fremdgeräten und Netzfunktionen;
5. Fähigkeit zur Bereitstellung von Upgrades und Anpassungen;
6. Verwaltung und Offenlegung von Schwachstellen sowie die Aktualität von Updates und Fehlerbehebungen;
7. Verfügbarkeit und Transparenz der Dokumentation in Bezug auf:

- Schlüsselfunktionen und Informationen über die Sicherheit und andere Merkmale der Komponente und mögliche Einstellungen sowie
- verwendete Software, einschließlich Open Source Code (Software Bill Of Materials – SBOM);

8. Grad der Abhängigkeit von Third-Level-Support bei der Verwaltung und Wartung von Geräten, wenn der Betreiber diese Dienste nicht allein mit seinen Angestellten erbringt;
9. vorläufige Bewertung der Konformität von Geräten oder Einrichtungen, die Third-Level-Support von in der Europäischen Union nach europäischen Systemen für die Cybersicherheitszertifizierung akkreditierten Stellen erbringen würden, wobei die akkreditierten Stellen im *Amtsblatt der Europäischen Union* veröffentlicht werden.

(3) Der Betreiber dokumentiert die Risikofaktoren und die Ergebnisse der Risikobewertung für jeden in den Absätzen 2 und 3 dieses Artikels genannten ausgewählten Hersteller oder Anbieter von Third-Level-Support und aktualisiert diese regelmäßig.

Artikel 5
(Allgemeine Leitlinien für den Betrieb kritischer Netzelemente)

(1) Die Komponenten der kritischen Netzelemente, ihre Betriebs- und Standardeinstellungen dürfen keine technischen Merkmale enthalten, die sich negativ auf die Sicherheit oder den Betrieb kritischer Einrichtungen auswirken könnten, unter anderem aufgrund von Sabotage, Spionage, Diebstahl von geistigem Eigentum oder Terrorismus.

(2) Die kritischen Netzelemente befinden sich in der Regel in der Republik Slowenien oder, unter Berücksichtigung aller Sicherheitsrisiken und Gewährleistung eines hohen Sicherheitsniveaus, in der Europäischen Union, sofern dies in den geltenden Rechtsvorschriften nicht anders festgelegt ist. Der Betreiber unterrichtet die Agentur für Kommunikationsnetze und -dienste der Republik Slowenien (im Folgenden „Agentur“) und die für Informationssicherheit zuständige Stelle mindestens 30 Tage vor der geplanten Verlagerung in ein Land außerhalb der Europäischen Union.

(3) Third-Level-Support für kritische Netzelemente wird in der Regel in der Republik Slowenien oder unter Berücksichtigung aller Sicherheitsrisiken und Gewährleistung eines hohen Sicherheitsniveaus in der Europäischen Union erbracht, sofern dies in den geltenden Rechtsvorschriften nicht anders festgelegt ist. Der Betreiber unterrichtet die Agentur und die für die Informationssicherheit zuständige Stelle mindestens 30 Tage vor der geplanten Verlagerung des Third-Level-Supports in ein Land außerhalb der Europäischen Union.

(4) Die Durchführung von Third-Level-Support darf die Sicherheit oder den Betrieb der Dienste kritischer Einrichtungen oder die nationale Sicherheit nicht gefährden.

(5) Der Betreiber führt ein Verfahren zur Ermittlung kritischer Netzelemente ein und führt diese regelmäßig durch. Dies muss mindestens einmal jährlich erfolgen oder wenn Komponenten kritischer Netzelemente beschafft werden.

(6) Stellt eine einzelne Komponente nur teilweise ein kritisches Netzelement dar, so gilt sie als Teil eines kritischen Netzelements.

(7) Der Betreiber führt eine Liste aller Komponenten kritischer Netzelemente, deren Funktionen, Standorte, Administratoren und Manager, der Anbieter von Third-Level-Support und der Hersteller oder Lieferanten auf dem neuesten Stand. Die Liste wird der Agentur und einer für die Informationssicherheit zuständigen Stelle auf Anfrage zur Verfügung gestellt.

Artikel 6
(Sicherheitsmaßnahmen für die Lieferung von Komponenten kritischer Netzelemente)

(1) Der Betreiber muss die gesamte Lieferkette und die damit verbundenen Risiken kennen, einschließlich Subunternehmern einzelner Komponenten kritischer Netzelemente, zu denen auch Verschlüsselungsschlüssel, UICC/eUICC und andere Sicherheitselemente gehören, deren Missbrauch die Sicherheit kritischer Einrichtungen gefährden könnte.

(2) Der Betreiber stellt sicher, dass die Sicherheitsanforderungen zwischen dem Betreiber und den Herstellern oder Lieferanten von Komponenten kritischer Netzelemente oder den Anbietern von Third-Level-Support vertraglich vereinbart und dokumentiert werden und die Hersteller oder Lieferanten verpflichtet sind, die vereinbarten Sicherheitsmaßnahmen in der gesamten Lieferkette einzuhalten.

(3) Um die Ausnutzung von Schwachstellen durch böswillige Akteure rechtzeitig zu verhindern, stellt der Betreiber sicher, dass sich der Hersteller oder Anbieter von Komponenten eines kritischen Netzelements vertraglich verpflichtet, den Betreiber unverzüglich über festgestellte Schwachstellen und über Maßnahmen zur Verringerung der Risiken zu informieren und über Schutz- oder Abhilfemaßnahmen zu beraten, die der Betreiber als Reaktion auf die Bedrohung ergreifen kann.

(4) Der Betreiber überprüft mindestens einmal jährlich die Angemessenheit der Zugangsrechte für kritische Netzelemente oder aktualisiert diese unverzüglich bei Änderungen in der Organisation oder auf der Seite der Anbieter von Third-Level-Support.

(5) Der Betreiber verhindert seine Abhängigkeit von einem einzigen Lieferanten oder Anbieter von Third-Level-Support (d. h. den „Lock-in-Effekt“), sofern dies technisch machbar und wirtschaftlich tragbar ist, mit dem Ziel, die Abhängigkeit zu verringern und die Widerstandsfähigkeit bei Schwachstellen kritischer Komponenten zu erhöhen, auch indem langfristige Verträge mit einem einzigen Hersteller oder Lieferanten oder Anbieter von Third-Level-Support vermieden werden oder die Möglichkeit besteht, diese zu ändern, um Unterbrechungen in der Erbringung von Dienstleistungen für kritische Einrichtungen so gering wie möglich zu halten.

Artikel 7
(Vertragliche Bedingungen mit Herstellern, Lieferanten oder Anbietern von Third-Level-Support)

Um ein hohes Sicherheitsniveau zu gewährleisten, muss der Betreiber mit Herstellern, Lieferanten oder Anbietern von Third-Level-Support mindestens Folgendes in neuen Vertragsbedingungen aufnehmen:

1. eine Erklärung des Herstellers oder des Lieferanten, dass eine Komponente oder ihre Standardeinstellungen keine undokumentierten Hintertüren oder negative Auswirkungen auf den Betrieb kritischer Einrichtungen haben;
2. eine Verpflichtung des Herstellers oder des Lieferanten oder des Anbieters von Third-Level-Support, die Daten, die sie während der Erbringung von Dienstleistungen erhalten oder zu denen sie Zugang bekommen, zu schützen;
3. eine Verpflichtung des Herstellers oder des Lieferanten oder des Anbieters von Third-Level-Support, den Betreiber im Falle von Verstößen gegen den Schutz von Kommunikationsdaten oder Verkehrsdaten, die den Betreiber oder die in Artikel 1 Nummer 1 dieses allgemeinen Gesetzes genannten kritischen Einrichtungen betreffen oder betreffen könnten, unverzüglich zu informieren;
4. eine Verpflichtung des Herstellers oder des Lieferanten oder des Anbieters von Third-Level-Support, den Betreiber unverzüglich über Sicherheitsvorfälle und Sicherheitslücken, die die Sicherheit des Netzes, der zugehörigen Dienste oder Daten des Betreibers beeinträchtigen könnten, zu informieren;
5. eine Verpflichtung des Herstellers oder des Lieferanten oder des Anbieters von Third-Level-Support, die vom Betreiber festgelegten Sicherheitsstandards und -regeln einzuhalten und geeignete Sicherheitsmaßnahmen zu ergreifen, um die Sicherheit der Informationssysteme und -netze sowie der Daten des Betreibers oder der kritischen Einrichtung zu gewährleisten;
6. die Fähigkeit des Betreibers, die Umgebungen, Verfahren, Sicherheitsmaßnahmen und Werkzeuge zu überprüfen, die der Anbieter von Third-Level-Support beim Zugriff auf das Netz und die Daten des Betreibers verwendet;
7. die Verantwortung des Herstellers oder des Lieferanten oder des Anbieters von Third-Level-Support für Schäden, die durch festgestellte Schwachstellen oder den Missbrauch von Komponenten kritischer Netzelemente, deren Standardeinstellungen oder während der Bereitstellung von Third-Level-Support verursacht werden, die vom Hersteller oder Lieferanten oder Anbieter von Third-Level-Support vernachlässigt oder vorsätzlich herbeigeführt wurden;
8. eine Verpflichtung, das Personal des Herstellers oder Lieferanten oder Anbieters von Third-Level-Support im Bereich der Datensicherheit und Informationssysteme und -netze regelmäßig zu schulen.

Artikel 8

(Regeln für den Zugang zu und die Nutzung von kritischen Netzelementen)

(1) Beim physischen oder logischen Zugriff auf die Komponenten kritischer Netzelemente, deren Einstellungen und die darin gespeicherten, verarbeiteten oder geänderten Daten des Betreibers stellt der Betreiber sicher, dass:

1. der Zugang streng auf Personen, die zuvor autorisiert wurden, beschränkt ist;
2. alle Arbeiten an kritischen Netzelementen, die vor Ort oder per Fernzugriff durchgeführt werden, vom Betreiber kontrolliert werden;
3. für die Benutzer, denen die höchsten Zugriffsrechte gewährt werden, um auf einzelne Komponenten kritischer Netzelemente, deren Einstellungen oder die dort gespeicherten oder verarbeiteten Daten zuzugreifen, eine Multi-Faktor-Authentifizierung durchgeführt wird;
4. jede autorisierte Person, der Zugang gewährt wird, über ein eindeutiges Benutzerkonto und ein Passwort verfügt;

5. nur Passwörter verwendet werden, die regelmäßig oder im Falle eines erkannten Missbrauchs sofort geändert werden und mindestens 15 Zeichen enthalten, einschließlich Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, sofern die Software dies zulässt;
6. das beim Zugang soweit möglich das Konzept der Nulltoleranz oder Vertrauenswürdigkeit umgesetzt wird;
7. die Sicherheit der Kommunikationsverbindung zwischen dem autorisierten Benutzer und den einzelnen Komponenten durch Verschlüsselung unter Berücksichtigung der neuesten technologischen Entwicklungen und bewährten industriellen Verfahren im Bereich der Informationssicherheit oder gemäß den Empfehlungen von etablierten Institutionen im Bereich der Informationssicherheit geschützt wird;
8. eine unauslöschliche Aufzeichnung der Zugriffe und Zugriffsversuche erstellt und mindestens 6 Monate lang aufbewahrt wird, einschließlich einer Sicherungskopie; sie kann auch für einen längeren Zeitraum aufbewahrt werden, wenn eine Risikomanagementanalyse und eine Bewertung des annehmbaren Risikos ergeben, dass die Risiken durch eine längere Aufbewahrung der Aufzeichnungen angemessen beherrscht würden;
9. alle Softwareinterventionen an Komponenten, soweit möglich, einschließlich von Konfigurationsänderungen, erfasst und überwacht werden. Die Aufzeichnungen, einschließlich einer Sicherungskopie dieser Daten, werden so lange aufbewahrt, wie in der vorstehenden Nummer angegeben;
10. der Zugriff auf einzelne Komponenten und auf ihnen gespeicherte oder verarbeitete Daten ist zeitlich begrenzt und nur für die Dauer der erforderlichen Arbeit freigegeben.

(2) Im Falle des Zugriffs auf einzelne Komponenten kritischer Netzelemente durch Personal oder Angestellte eines Anbieters von Third-Level-Support. gilt Folgendes:

1. es darf nur ein sicherer, dedizierter Rechner („Jump-Server“) verwendet werden, der regelmäßig Sicherheitskontrollen unterzogen wird;
2. auf einem dedizierten Rechner dürfen nur die Tools, Komponenten und aktiven Dienste, die absolut notwendig sind, um auf andere Ressourcen im Netz zuzugreifen, installiert werden und müssen mit den neuesten Sicherheitspatches aktualisiert werden;
3. sichere kryptografische Operationen und Schlüssel müssen an einem dedizierten Rechner verwendet werden, der sich im Netz des Betreibers befinden muss und unter seiner alleinigen Kontrolle steht;
4. jeder Zugriff wird vom Betreiber manuell und nur für die Dauer des Zugriffs genehmigt und aktiviert;
5. alle Zugriffe und Aktivitäten werden vom Betreiber physisch kontrolliert und aufgezeichnet;
6. es müssen Zwei-Faktor-Authentifizierung und Passwörter, die mindestens 15 Zeichen lang sind und Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten, verwendet und auf der Grundlage der bewerteten Risiken geändert werden.

(3) Bevor der Betreiber den Dienst zur Verwaltung, Wartung oder Aktualisierung kritischer Netzelemente oder einzelner Komponenten an einen Dritten überträgt, muss er überprüfen und sicherstellen, dass dieser Dritte über Sicherheitsmechanismen und Sicherheitsmanagementprozesse verfügt, die mindestens genauso gut oder besser sind als die Mechanismen und Prozesse des Betreibers. Er informiert die betreffende kritische Einrichtung, die Agentur und die für die Informationssicherheit zuständige Stelle unverzüglich über die Absicht der Übertragung.

(4) Der Betreiber überprüft den tatsächlichen Stand der Sicherheitsprozesse vor Beginn der Dienstleistungserbringung und danach mindestens einmal jährlich. Der Betreiber führt Aufzeichnungen über interne Überprüfungen und Kontrollen über die Erbringung von Third-Level-Support und wahrt diese für die Dauer der Erbringung der Dienste und für ein Jahr nach ihrer Beendigung, jedoch nicht länger als fünf Jahre auf.

ÜBERGANGS-UND SCHLUSSBESTIMMUNGEN

Artikel 9
(Übergangsbestimmungen)

(1) Der Betreiber unterrichtet die Agentur und die für die Informationssicherheit zuständige Stelle innerhalb von 30 Tagen nach Inkrafttreten dieses allgemeinen Gesetzes über die bestehenden Standorte kritischer Netzelemente.

(2) Der Betreiber unterrichtet die Agentur und die für die Informationssicherheit zuständige Stelle innerhalb von 30 Tagen nach Inkrafttreten dieses allgemeinen Gesetzes über die bestehenden Standorte von Third-Level-Support für kritische Netzelemente.

(3) Die Agentur veröffentlicht die in Artikel 3 Absatz 2 dieses allgemeinen Gesetzes genannten Dokumente erstmals ab dem Tag seines Inkrafttretens.

Artikel 10
(Inkrafttreten)

Dieses allgemeine Gesetz tritt am dreißigsten Tag nach seiner Veröffentlichung im Amtsblatt der Republik Slowenien in Kraft, wonach die Betreiber die Ausrüstung nutzen und die Erbringung von Third-Level-Support bis zum Ablauf der in Artikel 312 Absätze 2 und 3 des Gesetzes genannten Fristen aufrechterhalten können.

Nr. ___ mag. Marko Mišmaš

Ljubljana, den ___ Direktor

EVA 2023-3150-0034

VORSCHLAG

Anhang

Liste kritischer Netzelemente und zugehöriger Informationssysteme:

Kritische Netzelemente	**Funktionalitäten des Netzes und der Informationssysteme**
Teilnehmerverwaltung und Verschlüsselungsmechanismen	- Sitzungsmanagement (Sprache und Daten), - Authentifizierung von Benutzern und Geräten gegenüber dem Netz, - Verwaltung und Speicherung von Schlüsseln zur Autorisierung von Teilnehmern und Netzkomponenten (UICC/eUICC, digitale Zertifikate/HSM), - Funktionen zur sicheren Authentifizierung, zum Schutz der Kommunikationsintegrität (Verschlüsselung) und zur Speicherung von Benutzerschlüsseln, Netz- und Verwaltungskomponenten, - Verwaltung von Zugriffsrechten.
Zusammenschaltung	- Hosting-Funktionen und Schnittstellen zu anderen Netzen und Diensten.
Verwaltete Netzdienste	- Registrierung und Autorisierung von Netzdiensten, - Speicherung und Verarbeitung von Kommunikations-, Standort- und Verkehrsdaten, - Exposition des Netzes und der Netzfunktionen gegenüber externen Anwendungen und Diensten.
Verwaltung und Orchestrierung von virtualisierten Netzfunktionen (NFV) und Netzorchestrierung (MANO), einschließlich Virtualisierungsinfrastruktur	- Managementfunktionen der Orchestrierung und Konfiguration von NFV unabhängig von der Art der Implementierung (VM, Container, Micro-Services), - Virtualisierungsfunktionen für die Implementierung und Nutzung von NFV, - Netzwerk-Slice-Auswahlfunktion (NSSF)
Funkzugangsnetz	- Basisstationen, die 5G-Technologie oder höher unterstützen.
Verwaltungssysteme und andere Unterstützungssysteme	- Überwachung des Betriebs und der Verwaltung des Mobilfunknetzes, einschließlich des Zugangsteils (RAN/O-RAN), - Systeme zur Erkennung von Sicherheitsereignissen, Anomalien, Bedrohungen und deren Verwaltung (Sicherheitsfunktionen einschließlich SIEM/SOAR).
Rechtmäßige Überwachung	- Funktionen für den Zugang der zuständigen

	Behörde zu den Kommunikationsinhalten und Daten über den Nutzerverkehr.