PROPOSAL

Pursuant to Article 116(6) of the Electronic Communications Act (UL RS Nos 130/22 and 18/23 – ZDU-1O), the Agency for Communication Networks and Services of the Republic of Slovenia, taking into account the information procedure in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1), issues the following

GENERAL ACT
on additional security requirements and restrictions

Article 1
(Content of the general act)

This general act provides:

1. guidelines to be followed by mobile communications network operators (hereinafter referred to as 'operators') who provide these networks to critical entities that are managers of critical infrastructure in other areas of critical infrastructure regulation, as specified in the law governing the area of critical infrastructure (hereinafter referred to as 'critical infrastructure managers'), providers of essential services as determined by the law governing information security (hereinafter referred to as 'providers of essential services'), state administration bodies as determined by the law governing information security (hereinafter referred to as 'state administration bodies') or carriers of key parts of the country's security system; and
2. critical elements of the network and associated information systems with their functionalities referred to in Article 116(6) of the Electronic Communications Act (UL RS Nos 130/22 and 18/23 – ZDU-1O; hereinafter referred to as 'Act'), as set out in the annex, which forms an integral part of this general act and is drawn up in cooperation with the body responsible for information security.

Article 2
(Meaning of terms)

(1) The terms used in this general act mean:

1. A supply chain is the entire system of processes, people, organization and distribution involved in the design, production, storage, distribution and supply, as well as the installation and maintenance of components of critical network elements installed in the operator's network or at the cloud service provider providing such services to the operator.

2. Critical elements of the network are those network elements, functions, services and supporting information systems in physical, software or virtualised form at the operator or at the cloud service provider, as listed in the annex to this general act.

3. Critical entities are critical infrastructure managers in other areas of critical infrastructure regulation determined in accordance with the law governing the field of

critical infrastructure, providers of essential services as determined by the law governing information security, state administration bodies as determined by the law governing information security and carriers of key parts of the country's security system.

(2) Other terms used in this general act have the same meaning as defined by the Act and the General Act on the Security of Networks, Services and Data.

Article 3
(General guidelines)

(1) Operators in the supply chain of components of critical network elements and third-level support services for these components shall take into account at least the following guidelines throughout the entire life cycle of these components:

1. for an individual manufacturer or supplier and for a third-level support service provider due to relationships and agreements with them, they shall carry out a risk assessment in terms of supply and potential impacts by third-party natural or legal persons under public or private law (hereinafter referred to as 'third parties'), compatibility with equipment from other manufacturers, product quality and safety and potential negative impacts on the operation of the operator's services and critical entities;
2. that security is built-in and implemented already in the design and that contracts include deadlines for the elimination of perceived vulnerabilities;
3. that key security features (availability, confidentiality, integrity and authenticity) are ensured throughout the entire life cycle of their use,
4. that security and their uninterrupted supply are guaranteed and it is confirmed that it supports high security features in accordance with internationally recognized standards (3GPP) and European technical standards (ETSI);
5. that the guidelines referred to in points 2 to 4 of this paragraph are verifiable in the contractual documentation with the manufacturer or with the supplier;
6. for each manufacturer or supplier, the risks associated with the rights of use of the key technologies, which are necessary for the manufacture and use of the equipment and the risks related to the supply of equipment, spare parts or third-level support services, are also assessed and taken into account;
7. that the components used do not have unresolved known critical or actively exploited vulnerabilities;
8. avoiding a single manufacturer or supplier, where this is technically feasible and economically sustainable, with the aim of reducing dependence and increasing resilience in the event of critical component vulnerabilities, catastrophic network failure or a threat to the security of networks and services of critical entities by third natural or legal entities governed by public or private law.

(2) When supplying information and communication equipment, systems and services, operators shall fully comply with the guidelines of the European Union Agency for Cybersecurity (hereinafter referred to as 'ENISA') and valid regulations of the European Union regarding basic security requirements when procuring secure ICT products and services. The Agency shall publish on its website links to current ENISA documents and EU regulations in the aforementioned area and keep them up to date.

(3) When supplying components of critical network elements or using cloud services, priority shall be given to choosing components from those manufacturers or suppliers or services from cloud service providers that have been certified by conformity assessment bodies that have been accredited and, if necessary, authorized on the basis of Article 60(3) of the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (hereinafter referred to as 'Regulation') for the issuance of European cybersecurity certificates at certain assurance level, as determined by Article 52 of the Regulation.

(4) For the purpose of the previous paragraph, the operator shall check a special website, established by ENISA in accordance with Article 55 of the Regulation, intended to inform the public about European cybersecurity certification schemes, European cybersecurity certificates and EU declarations of conformity, including information regarding with European cybersecurity certification schemes that are no longer valid or revoked and expired European cybersecurity certificates and EU declarations of conformity, and a repository of links to cybersecurity information.

Article 4
(Risk assessment)

(1) When determining the risk of the component manufacturer or supplier and the third-level service provider for critical elements of the network, the operator takes into account the following risk aspects, which it evaluates.

(2) In the valuation referred to in the preceding paragraph, the operator shall assess and take into account at least:

1. overall quality (including safety aspects) and reliability;
2. level of use of open standards and interfaces that prevent dependence and lock-in to the products of a particular manufacturer or supplier;
3. compliance with recognized international and European technical standards (3GPP, ETSI) and European Union regulations and default security settings in accordance with professional recommendations (GSMA Association);
4. level of compatibility with third-party equipment and network functions;
5. ability to provide upgrades and customizations;
6. vulnerability management process, their disclosure and up-to-date process with updates and fixes;
7. availability and transparency of documentation regarding:
   - key functions and information about security and other features of the component and possible settings, and
   - software used, including open source code (Bill Of Materials – SBOM);
8. level of dependence on third-level support services in the management and maintenance of equipment, if the operator does not perform these services alone with its employees;
9. preliminary assessment of the conformity of equipment or an entity that would provide a third-level support service by bodies accredited in the European Union according to European cybersecurity certification schemes, whereby the accredited bodies are published in the Official Journal of the European Union.

(3) The operator shall document the risk factors and the results of the risk evaluation for each selected manufacturer or supplier or third-level service provider referred to in paragraphs 2 and 3 of this article and shall update this regularly.

Article 5
(General guidelines on the operation of critical network elements)

(1) The components of the critical network elements, their operation and default settings shall not contain technical characteristics that could negatively affect the security or the operation of critical entities, inter alia due to sabotage, espionage, theft of intellectual property or terrorism.

(2) The critical network elements are generally located in the Republic of Slovenia or, taking into account all security risks and ensuring a high level of security measures, and if this is not specified otherwise by applicable regulations, in the European Union. The operator shall inform the Agency for Communication Networks and Services of the Republic of Slovenia (hereinafter referred to as 'the Agency') and the body responsible for information security about their intended relocation at least 30 days before the relocation outside the European Union.

(3) Third-level support services for critical elements of the network are generally performed in the Republic of Slovenia or, taking into account all security risks and ensuring a high level of security measures, and if this is not specified otherwise by applicable regulations, in the European Union. The operator shall notify the Agency and the body responsible for information security of the intended relocation of their third-level support services at least 30 days before the relocation outside the European Union countries.

(4) The implementation of third-level support services shall not jeopardise the security or operation of the services of critical entities or national security.

(5) The operator shall establish and regularly implement the process of identifying critical network elements. This must be carried out at least once a year or when components of critical network elements are procured.

(6) If an individual component only partially represents a critical network element, it shall be considered as part of a critical network element.

(7) The operator shall maintain an up-to-date a list of all components of critical network elements, their functions, locations, administrators and managers, their third-level support service providers and their manufacturers or suppliers. Upon request, the list shall be made available to the Agency and a body responsible for information security.

Article 6
(Security measures for the supply of components of critical network elements)

(1) The operator shall be aware of the entire supply chain and the risks associated with it, including subcontractors of individual components of critical network elements, which

also includes encryption keys, UICC/eUICC and other security elements, the misuse of which could jeopardise the security of critical entities.

(2) The operator shall ensure that the security requirements between the operator and the manufacturers or suppliers of components of critical network elements or its third-level support service providers are contractually agreed and documented and require manufacturers or suppliers to respect the agreed security measures throughout the entire supply chain.

(3) In order to prevent the exploitation of vulnerabilities by malicious actors in a timely manner, the operator shall ensure that the manufacturer or supplier of components of a critical network element contractually undertakes to immediately inform the operator of the detected vulnerability and of measures to reduce risks and advise on protective or remedial measures, which the operator can take in response to the threat.

(4) The operator shall, at least once a year, verify the adequacy of access rights on critical network elements or update them without delay in accordance with changes in the organization or on the side of third-level support service providers.

(5) The operator shall prevent its dependence on an individual supplier or third-level service provider (i.e. 'vendor lock-in'), where this is technically feasible and economically sustainable, with the aim of reducing dependence and increasing resilience in case of critical component vulnerabilities, also by avoiding long-term contracts with individual manufacturers or suppliers or providers of third-level support services, or having the option of changing them with the aim of reducing disruptions in the provision of services to critical entities to the lowest possible level.

Article 7
(Contractual terms with manufacturers, suppliers or third-level support service providers)

In order to ensure a high level of security, the operator shall include at least the following in new contractual terms with manufacturers, suppliers or third-level support service providers:

1. a statement by the manufacturer or the supplier that the component or its default settings have no undocumented backdoors or any negative impact on the operation of critical entities;
2. a commitment of the manufacturer or the supplier or the third-level service provider to protect the data with which they become acquainted during the provision of services or access to them in connection with the provision of the access service;
3. a commitment of the manufacturer or the supplier or the third-level service provider to immediately inform the operator in the event of violations of the protection of communication data or traffic data that affects or could affect the operator or the critical entities referred to in the Article 1, point 1, of this general act;
4. a commitment of the manufacturer or the supplier or the third-level service provider to immediately notify the operator of any security incident and vulnerabilities that could affect the security of the network, associated services or data of the operator;
5. a commitment of the manufacturer or the supplier or the third-level service provider to comply with the security standards and rules set by the operator and to take

appropriate security measures to ensure the security of information systems and networks, and the operator's or critical entity's data;

6. operator's ability to review the environments, procedures, security measures and tools used by the third-level support service provider when accessing the operator's network and data at any time;
7. responsibility of the manufacturer or the supplier or the third-level support services provider for damage that would be caused by identified vulnerabilities or misuse of components of critical network elements, their default setting or during the provision of third-level support services that the manufacturer or the supplier or third-level support provider neglected or deliberately implemented;
8. an obligation to regularly train the personnel of the manufacturer or supplier or third-level support service provider in the field of data security and information systems and networks.

Article 8
(Rules regarding access and use of critical network elements)

(1) When physically or logically accessing the components of critical network elements, their settings, and the operator's data stored, processed or modified in them, the operator shall ensure that:

1. access is strictly limited to persons who have been previously authorised;
2. all works on critical network elements carried out on site or via remote access are controlled by the operator;
3. multi-factor authentication is carried out for users to whom the highest privileges of rights are assigned to access individual components of critical network elements, their settings or the data stored or processed there;
4. each authorised person to whom access is granted has a unique user account and password;
5. only passwords that are changed regularly or immediately in case of detected misuse and contain at least 15 characters and include upper and lower case letters, numbers and special characters, if the software allows this, are used;
6. the concept of zero tolerance or trust is implemented in access where possible;
7. the security of the communication connection from the authorized user to the individual components is protected by the use of encryption, taking into account the latest technological developments and best industrial good practices in the field of information security, or recommended by established institutions in the field of information security;
8. an indelible recording of accesses and access attempts is carried out, which is kept for at least 6 months, including a backup copy, but may also be for a longer period, when the analysis of risk management and the assessment of the acceptable level of risks show that the risks should be adequately managed by keeping the logs for a longer period records;
9. recording and monitoring of all software interventions on components is performed where possible, including configuration changes. Records, including a backup copy of this data, shall be kept for as long as indicated in the previous point;
10. access to individual components and to data stored or processed on them is time-limited and open only for the duration of necessary work.

(2) In the case of access to individual components of critical network elements by staff or employees of a third-level support service provider they shall:

1. use only a secure intermediate dedicated workstation (‘jump server’), which shall be subject to regular security checks;
2. install on a dedicated workstation only the absolutely necessary tools, components and active services to access other resources on the network that are absolutely necessary and must be updated with the latest security patches;
3. use secure cryptographic operations and keys on a dedicated workstation, which must be located in the operator's network and is under its sole control;
4. each access is approved and activated by the operator manually and only for the duration of the access;
5. all accesses and activities are physically controlled and recorded by the operator;
6. use two-factor authentication and passwords that are at least 15 characters long and include upper and lower case letters, numbers and special characters, which shall be changed based on assessed risks.

(3) Before the operator transfers the service of managing, maintaining or updating critical network elements or their individual components to a third party, it shall verify and ensure that it has at least the same or better security mechanisms and security management processes in place in comparison to its mechanisms and processes. It shall immediately inform the critical entity concerned, the Agency and the body responsible for information security about the intention to transfer.

(4) The operator shall verify the actual state of the security processes before the start of service provision and thereafter at least once a year. The operator shall maintain records of internal reviews and controls on the provision of third-party support services and keep them for the duration of the provision of the services and for one year after their termination, but no longer than five years.

TRANSITIONAL AND FINAL PROVISION

Article 9
(Transitional provisions)

(1) The operator shall notify the Agency and the body responsible for information security of the existing locations of critical network elements within 30 days of the entry into force of this general act.

(2) The operator shall notify the Agency and the body responsible for information security of the existing locations of third-level support services for critical network elements within 30 days of the entry into force of this general act.

(3) The Agency shall publish for the first time the documents referred to in Article 3(2) of this general act from the date of its entry into force.

Article 10
(Entry into force)

This general act enters into force on the thirtieth day after its publication in the Official Gazette of the Republic of Slovenia, whereby operators may use the equipment and maintain the provision of third-level support services until the expiration of the deadlines specified in Article 312(2) and (3) of the Act.

No _____ mag. Marko Mišmaš

Ljubljana, on _____ director

EVA 2023-3150-0034

PROPOSAL

Annex

List of critical network elements and associated information systems:

Critical network elements	**Functionalities of the network and information systems**
Subscriber management and encryption mechanisms	- Session management (voice and data), - authentication of users and equipment with the network, - management and storage of keys for authorization of subscribers and network components (UICC/eUICC, digital certificates/HSM), - functions for secure authentication, protection of communication integrity (encryption) and storage of user keys, network and management components, - management of access rights.
Interconnection	- Hosting features and interfaces to other networks and services.
Managed network services	- Registration and authorisation of network services, - storage and processing of communication, location and traffic data, - exposure of network and network functions to external applications and services.
Management and orchestration of virtualised network functions (NFV) and network orchestration (MANO), including virtualisation infrastructure	- Management functions of orchestration and configuration of NFV regardless of the type of implementation (VM, container, micro-services), - virtualisation functions for the implementation and use of NFV, - Network Slice Selection Function (NSSF).
Radio access network	- Base stations that support 5G technology or higher.
Management systems and other support systems	- Monitoring the operation and management of the mobile communication network, including the access part (RAN/O-RAN), - systems for detecting security events, anomalies, threats and their management (security functions including SIEM/SOAR).
Legal interception	- Functions of access to the communication content and data on user traffic by the competent authority.