FEDERAL LAW GAZETTE

FOR THE REPUBLIC OF AUSTRIA

Year 2020 **Issued July 3, 2020** **Part II**

301. Ordinance: 2020 Telecommunications Networks Security Ordinance (TK-NSiV 2020)

301. Ordinance of the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR-GmbH) concerning obligations for operators of electronic communications networks and providers of electronic communications services relating to minimum security requirements in the context of 5G networks as well as reporting obligations in the event of security incidents – Telecommunications Networks Security Ordinance 2020 (TK-NSiV 2020)

The provisions specified below are hereby enacted based on Art. 16a Par. 9 of the Federal Act enacting the Telecommunications Act (2003 Telecommunications Act—TKG 2003), FLG I No. 70/2003 as amended by FLG I No. 23/2020 and by mutual agreement with the Federal Minister of Agriculture, Regions and Tourism, and the Federal Minister of the Interior:

Purpose and scope

Article 1 (1) This Ordinance sets out reporting obligations for operators of electronic communications networks and providers of electronic communications services in the event of such security incidents involving electronic communications networks and services that have led to a substantial impact on network operations or service provision, as well as the actions to be taken by the regulatory authority in the event of such security incidents. The Ordinance also sets out general conditions for the submission of notifications in relation to security incidents without a substantial impact on network operations or service provision.

(2) In addition, requirements are also defined for the minimum security measures to be implemented by operators of electronic communications networks and providers of electronic communications services in order to ensure an appropriate level of control over risks affecting electronic communications networks and services, and to maintain the appropriate level of security in order to do so, considering in particular the security of 5G networks.

(3) This Ordinance is binding on all public communications networks operated on Austrian territory with the exception of broadcasting networks and on all public electronic communications services offered on Austrian territory with the exception of transmission services in broadcast networks.

Definitions

Article 2 Meaning of terms used in this Ordinance

1. ‘Security of networks and services’: the capability of communications networks and services to counteract incidents with a certain level of confidence, where such incidents impair the availability, authenticity, integrity or trustworthiness of those networks and services, the stored, transmitted or processed data, or any related services that are offered or which are accessible via those communications networks or services.
2. ‘Malicious attack’: a process by which an individual or a program wilfully and without authorisation gains logical or physical access or an opportunity for access to a network or its components, to a system, to an application, to data or to other IT resources, or that wilfully impairs the functioning of the attacked network or service.
3. ‘Human error’: negligence (e.g. the misconfiguration or faulty deployment of network components, platforms, applications [software], data backups and databases, the erroneous application of procedures to processes in the context of configuration management, change

management, identity/access control workflows as well as incorrect decisions taken by management).

4. 'Natural event': a naturally occurring event that impacts communications infrastructure, such as bad weather (storm, heavy snowfall, heat wave), earthquake, epidemic disease, flooding, fire, landslide, volcanic eruption or environmental changes caused by solar activity.
5. 'System error': hardware errors, software errors and errors in operating instructions, procedures or internal codes.
6. 'Third-party error': a process that is outside the direct control of the operator (such as an incident at an outsourcing partner or at an organisation within the supply chain).
7. 'Security incident': an event having a detrimental effect on the security of communications networks or services.
8. 'Promptly': without undue delay.
9. '5G network': a fifth-generation mobile telecommunications network in which the corresponding network infrastructure components are based on international technical standards for mobile and wireless communications, and which display advanced performance characteristics such as very high data speeds and capacities, low-latency communications, ultra-high reliability or support for a large number of connected devices. Elements of 5G network infrastructure may also include some legacy components that are based on earlier generations of mobile and wireless communications technology (such as 4G or 3G).

Reporting obligations

Article 3 (1) In the event of security incidents that have led to—or continue to have—a significant impact on the security of electronic communications networks or services, operators of electronic communications networks and providers of electronic communications services shall inform the regulatory authority promptly as soon as they become aware of the incident. In terms of content, details must be submitted as set out in Nos. 1 to 14 and in an electronic format as specified by the regulatory authority ('initial report'). The regulatory authority must be notified promptly once the affected services have been restored. Furthermore, the following information must be submitted to the regulatory authority in the electronic format specified by the authority within a maximum of 24 hours after restoration of the affected services ('follow-up report'):

1. Date and time when the incident started;
2. Cause of the incident, according to one of the following categories: natural event, human error, malicious attack, systemerror or third-party error;
3. Operating equipment affected (e.g. mobile base station, network node, home subscriber server, international data transmission link);
4. Service affected (by category: fixed network telephony, mobile telephony, fixed internet access, mobile internet access) and the underlying technology;
5. Number of subscribers affected in the respective service category:
   a. For fixed network telephony, the number of connections affected;
   b. For mobile telephony, the number of activated SIM cards affected;
   c. For fixed internet access, the number of connections affected;
   b. For mobile internet access, the number of activated SIM cards affected;
6. Impact on the reachability of emergency telephone numbers (emergency numbers affected, number of subscribers affected in each service category);
7. Total number of subscribers affected in all service categories;
8. Measures taken to resolve the incident and to restore the service;
9. Post-incident follow-up (minimising risk in future incidents, estimation of the efficiency of the measures taken);
10. Long-term 'lessons learned' from the incident;
11. Time required for restoration, from the start of the incident to restoration of the affected service;
12. Interconnections affected, in terms of interconnection partners and sites affected;
13. Brief description and analysis of the incident;
14. Details of any communications made or planned to be made to the public (where relevant).

The initial and follow-up reports must be submitted using the regulatory authority's reporting portal. In the initial and follow-up reports, the reporting party must cite any warning notice previously issued by

that party in accordance with Art. 4. In the event of the regulatory authority's reporting portal being unavailable, reports of security incidents with substantial impact can be submitted in a format other than the electronic format described in sentence 1 and 2.

(2) A 'substantial impact' is present in the following cases:

1. The incident lasts up to and including one hour, and the number of subscribers affected in the respective service category (Par. 1 No. 5) exceeds 500,000; or
2. The incident lasts over an hour and the number of subscribers affected in the respective service category (Par. 1 No. 5) exceeds 500,000 or 15 percent of the total number of users of this service on Austrian territory; or
3. The incident lasts over two hours and the number of subscribers affected in the respective service category (Par. 1 No. 5) exceeds 250,000 or 10 per cent of the total number of users of this service on Austrian territory; or
4. The incident lasts over four hours and the number of subscribers affected in the respective service category (Par. 1 No. 5) exceeds 150,000 or 5 per cent of the total number of users of this service on Austrian territory; or
5. The incident lasts over six hours and the number of subscribers affected in the respective service category (Par. 1 No. 5) exceeds 100,000 or 2 percent of the total number of users of this service on Austrian territory; or
6. The incident lasts over eight hours and the number of subscribers affected in the respective service category (Par. 1 No. 5) exceeds 50,000 or 1 per cent of the total number of users of this service on Austrian territory; or
7. The incident lasts over 16 hours, and the number of subscribers affected in the respective service category (Par. 1 No. 5) exceeds 10,000; or
8. An emergency telephone number from a communications network for subscribers to an available public telephone service is not reachable or the telephone service is only partially available for subscribers and at least one emergency telephone number is not reachable. A substantial impact also exists if the telephone service for the emergency control centre at which an emergency call terminates is not available for incoming calls, regardless of whether or not the emergency telephone number is reachable.

(3) If disclosure of the incident is in the public interest, operators of communications networks and services shall at the request of the regulatory authority inform the public promptly. The regulatory authority may inform the public directly in the event of imminent danger.

(4) The regulatory authority shall publish on its website the data used to determine the threshold values listed in Par. 2.

(5) The regulatory authority shall forward any report received in accordance with Par. 1 promptly to the Federal Minister of the Interior (Art. 16a Par. 5a TKG 2003, FLG I No. 70/2003 as amended by FLG I No. 23/2020).

Warning notice

Article 4 (1) Without prejudice to Art. 23 of the Federal Act guaranteeing a high level of security in network and information systems (Network and Information System Security Act—NISG, FLG I No. 111/2018), operators of electronic communications networks and providers of electronic communications services may report to the regulatory authority any risks and incidents not subject to the reporting requirements in Art. 3 Par. 1 that they consider to be security-relevant. This warning notice must not contain any personal data about natural persons (excepting that of the reporting party).

(2) The warning notice should include all relevant details concerning the risk or incident and the general technical circumstances as known at the point in time the report is made, and, in particular, the probable or actual cause and the operating equipment affected. Situational details that transpire later concerning the risk or incident shall be included in follow-up reports. The warning notice and follow-up reports shall be submitted via the regulatory authority's reporting portal in the electronic format required for mandatory reports; Art. 3 Par. 1, last sentence applies accordingly. The regulatory authority shall forward the warning notice and the respective report to the competent Computer Emergency Response Team (Art. 23 Par. 2 and Par. 3 NISG) and, where the reporting party consents, to the Federal Minister of the Interior.

Minimum security measures

Article 5 (1) To guarantee an appropriate level of security and in the interests of preventing security incidents, operators of electronic communications networks and providers of electronic communications services shall define, implement and document relevant measures in accordance with TKG 2003 Art. 16a Par. 1 and shall draw up an Information Security Policy. Those measures should ensure a level of security for networks and services that is considered appropriate in light of the extant risk. Those measures and the Information Security Policy in particular shall meet the latest technical standards and cover the following areas:

1. Governance and risk management (risk management system, security roles and responsibilities, relationships with third parties);
2. Personnel and people security (background checks, security expertise and training, staff changes, disciplinary action in the event of a breach);
3. Security of systems and business premises (physical security, peripheral security, security of materials, security of supply, physical access control, information security);
4. Operational management (operating procedures, change management, handling of operating equipment);
5. Fault management (procedures, detection, response, escalation, reporting);
6. Business continuity management (service availability and continuity of provision, contingency planning, and disaster recovery planning);
7. Monitoring, auditing, testing (monitoring/logging, drills with deputy executives and emergency drills, system tests, security appraisal, compliance monitoring and auditing procedures);

(2) Operators of electronic communications networks and providers of electronic communications services shall keep records of measures as required by Par. 1. At the request of the regulatory authority, they shall submit to the authority in a standard electronic format details of the audits of their network/service security, as well as the security measures they have implemented and documented as required by Par. 1, together with their Information Security Policy.

Security requirements for 5G networks

Article 6 (1) To guarantee an appropriate level of security for 5G networks, operators of such networks with more than 100,000 subscribers in total in all of the mobile telecommunications networks they operate shall furnish the regulatory authority with proof of an extant information security management system conforming to a relevant, recognised standard by submitting the respective audit reports, initially by 31 December 2021 and then at regular intervals not exceeding three years. The specification and implementation of information security measures both of a general nature and specific to telecommunications networks shall also conform to relevant and recognised standards. Justification shall be given for each non-conformity to a provision in these standards.

(2) Operators of 5G networks with more than 100,000 subscribers in total in all of the mobile telecommunications networks they operate shall also furnish the regulatory authority with proof of the fulfilment of the standards listed in Appendix 1 by submitting an Operator Declaration Of Conformity, initially by 30 June 2021 and then at regular intervals not exceeding three years. Justification shall be given for each non-conformity to an optional provision in the standards listed in the Appendix.

(3) At the request of the regulatory authority, operators of 5G networks with more than 100,000 subscribers in total in all of the mobile telecommunications networks they operate shall also furnish the regulatory authority with proof of compliance with the following requirements:

1. Operation of a Network Operations Centre (NOC) and a Security Operations Centre (SOC) on their own premises within the European Union;
2. Effective monitoring by the NOC/SOC of all critical network components and sensitive parts of 5G networks, in order to detect anomalies, and to identify and mitigate threats;
3. Protection of management traffic in communications networks or services, in order to prevent unauthorised changes to network or service components;
4. Physical protection of critical network components and sensitive parts of 5G networks, using a risk-based approach for multi-access edge computing (MEC) and base stations;
5. Restriction of access to authorised and qualified personnel who have successfully passed background checks; access by third parties shall be restricted and monitored to an appropriate extent using systems meeting the latest technical standards;

6. Use of tools and processes that are capable of ensuring software integrity on any update or application of a security patch, as well as reliable identification and end-to-end documentation of changes and patch statuses;
7. A multi-vendor strategy that accounts for the technical limitations and interoperability requirements affecting the various parts of a 5G network.

(4) Lastly, operators of 5G networks with more than 100,000 subscribers in total in all of the mobile telecommunications networks they operate shall furnish the regulatory authority with a summary of the functions and manufacturers of the security-relevant components deployed to operate the 5G network as specified in Appendix 2 as well as any other components deployed, submitting the summary biannually as of the end of Q1 and Q3 by 30 April and 31 October of the same year, respectively, or in response to a justified request by the regulatory authority. Details of the functions and manufacturers shall be given in the electronic format specified by the regulatory authority. The regulatory authority is entitled to store and process for the service life of the components the data provided in this context.

Final provisions

Article 7 (1) Designations used for individuals in this Ordinance apply equally to all genders.

Steinmaurer