# Explanatory notes

**Key aspects of the Ordinance**

TK-NSiV 2020 defines 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. In addition, the Ordinance also sets out the actions to be taken by the regulatory authority in the event of such security incidents. The Ordinance also stipulates general conditions for the submission of notifications in relation to security incidents without a substantial impact on network operations or service provision.

Lastly, the Ordinance defines requirements 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. In terms of the security of 5G networks, several provisions from the corresponding EU legislative package ('EU 5G toolbox') are implemented.

**Article 1 Purpose and scope**

Par. 1: In contrast to Art. 3 No. 6 of the NISG, use of the term 'security incident' here conforms to Art. 2 No. 42 of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

Par. 3: The Austrian Communications Authority (KommAustria) is assigned responsibility for broadcast networks and for transmission services in broadcast networks.

**Article 2 Definitions**

No. 1: Since the term 'security of networks and services' had not been included in the definitions in TKG 2003, a corresponding, EECC-compliant definition was included.

No. 2: 'Malicious attack' was defined so as to include the possibility of a deliberate impairment to the functioning of the network or service attacked and to extend the term to cover DDoS attacks as well. A deliberate impairment of this kind covers attacks launched from both outside and inside a business.

No. 4: The example of an 'epidemic disease' enclosed in parentheses also encompasses pandemics.

No. 6: Since a specific hazard arising from interconnection partners is not evident in comparison with dependencies on other third-party relationships, there appears no need to list this group separately as an example for 'third-party error'.

No. 8: 'Promptly' means 'without undue delay', whereby the reporting obligations are not at all restricted to an operator's normal hours of business. These reporting obligations arise as soon as it becomes clear that the incident will have significant impact. In case of doubt, reporting obligations shall be assumed to apply.

No. 9: Number 9 adopts a definition of the term '5G network' that corresponds to the definition given in Point (a) of Commission Recommendation (EU) 2019/534 of 26 March 2019, 'Cybersecurity of 5G networks'. For reasons of consistency with this Recommendation, the parenthetical '4G or 3G' has been maintained, contrary to the wishes of some consultation participants. A request made in the consultation procedure to restrict the term '5G network' to '5G standalone' is not in line with the Recommendation mentioned.

The inclusion of additional definitions did not appear pertinent. This is not helpful in the case of some terms that form part of existing legal definitions taken from Directive 2018/1972/EU (for 'event', cf. Art. 2 No. 42, for 'certain level of confidence', cf. Art. 2 No. 21). The term 'service category' is self-explanatory and is used only in Art. 3. The term 'promptly' needs no explanation in the given context.

**Article 3 Reporting obligations**

The requested, explicit extension of reporting obligations to OTT providers is to be achieved by the transposition of the relevant provisions from Directive 2018/1972/EU into national law. A restriction of reporting obligations to public communications networks or granting an exemption to M2M services would exclude subscribers to non-public communications networks and users of M2M applications from the protection granted by the network security provisions, and there is no discernible justification for doing so.

A duplication of reporting duties, to the data protection authority and RTR GmbH, has been criticised as potentially arising based on the definition of terms in Art. 2 No. 1, according to which the 'security of networks and services' also covers the confidentiality of the stored, transferred or processed data. To clarify in response: a breach of the protection of personal data according to Art. 2 Par. 2 of Regulation 2013/611/EU must be reported solely to the data protection authority. If the data subject ascertains that the personal data breach can be ascribed to deficiencies in relation to the security of communications networks and services, then reporting to the regulatory authority will also be required if a substantial impact is present as defined by Art. 3 Par. 2 (if threshold values are exceeded).

The option for citing a warning notice submitted earlier concerning the exact same security incident was raised in the consultation procedure: this simplifies assignment and serves to document the fact that the reporting party has fulfilled their obligation to report the security incident promptly.

Par. 1: Details of the information to be submitted by operators of public communications networks or providers of public communications services are derived from the document adopted by the Member States of the European Union in consultation with ENISA entitled 'Technical Guideline on Reporting Incidents', version 2.1, October 2014. The document is available from the regulatory authority for examination and is also generally accessible on the authority's website at http://www.rtr.at/de/tk/Netzsicherheit/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf.

Par. 1 No. 1: If the exact start time of the incident cannot be determined, then the point in time when the affected party first became aware of the incident can also be indicated. Suggestions to include a maximum grace period of 24 hours for the initial report and three working days for the follow-up report were declined as they both lessen the incentive to report incidents as quickly as possible.

Par. 1 No. 3: cf. ENISA guideline 'Threats and Assets', https://www.rtr.at/de/tk/Netzsicherheit/Article_13a_ENISA_Technical_Guideline_On_Threats_And_Assets.pdf, version 1.2, August 2015.

Par. 1 No. 5: For mobile telephony and mobile internet access, the number of subscribers affected in each service category also includes eSIMs alongside activated SIM cards. Where services are provided to a SIM card or eSIM that belongs to more than one service category (mobile telephony or mobile internet access), the number of SIM cards affected including eSIMs shall be specified for each of the service categories in points (b) and (d). Where services are provided via a fixed-line network and belong to both the 'fixed-line telephony' and 'fixed internet access' service categories, the number shall be specified for each of the service categories in points (a) and (c). Where internet access services are provided using a combination of fixed and mobile internet access ('hybrid' products), the number shall be specified using the service categories in points (c) and (d) based on the respective category affected.

Par. 1 No. 5 Points (b) and (d): If the exact number cannot be determined, then the number can be estimated based on the average number of users of the affected cell, based on historical values.

Par. 2: The subscribers affected in each service category include only those subscribers who can be ascribed to the provider of the communication service affected.

Par. 4: When determining the total number of users of a service on Austrian territory, the operator can make use of the data published by the regulatory authority at https://www.rtr.at/en/tk/MitteilungVorflle.

**Article 4 Warning notice**

The provisions for the warning notice and follow-up reports relating to risks or incidents not subject to the reporting obligations defined in Art. 3 Par. 1 are modelled on those in Art. 19 Par. 3 and Art. 23 of the NISG and contain the related general conditions. A request was made in the consultation procedure to delete the requirement for the consolidated forwarding of the warning notice and follow-up reports by the responsible CERT to the Federal Minister of the Interior; while this was accepted, note that the forwarding of this information is nonetheless required anyway based on Art. 23 Par. 2 in conjunction with Par. 3 of the NISG.

**Article 5 Minimum security measures**

Par. 1: The areas for which security measures shall be provided by operators of public communications networks or providers of public communications services are derived from the document adopted by the Member States of the European Union in consultation with ENISA entitled 'Technical Guideline on Security Measures', version 2.0, October 2014. The document is available from the regulatory authority for examination and is also generally accessible on the authority's website at https://www.rtr.at/de/tk/Netzsicherheit/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf. These security measures include the specification of an information security policy. This

policy is to be understood as a guideline approved by the executive of an organisation that sets out the organisation's approach to achieving its information security goals. An information security policy should address requirements that are derived from business strategy, legislation and agreements, as well as the current and foreseeable threats to information security. The information security policy should contain the following details:

a) Definition of information security, goals and principles by which the organisation is guided in all of its efforts to achieve information security;

b) Assignment of general and specific responsibilities in information security management to defined roles;

c) Processes for handling non-conformities and exceptions.

At a subordinate level, the information security policy should be supported by topic-specific policies that provide details of implementation for the security measures and which are typically structured so that they address the needs of certain target groups within the organisation or cover certain topics (cf. ISO/IEC 27002:2013, 5.1.1).

The necessity for guaranteeing the security of supply in relation to software was raised specifically during the consultation. In response to this, it should be noted that this topic is covered by Art. 5 Par. 1 No. 3 (general security of supply) and No. 4 (change management, which also encompasses software patches).

A request for a maximum implementation period (six months or a year) for fulfilling these minimum security measures after the entry into force of this Ordinance was declined. As regards the obligation to implement these minimum security measures, the applicable legislation has been in place for many years and remains unchanged. Templates for creating documents in which these kinds of minimum security measures can be recorded are available at no charge (cf. e.g. https://www.ispa.at/wissenspool/vorlagen/ispa-mustersicherheitskonzept.html)

**Article 6 Security requirements for 5G networks**

Article 6 transposes Commission Recommendation (EU) 2019/534 of 26 March 2019 on the cybersecurity of 5G networks and includes provisions supplementing the security measures to be implemented by operators of public communications networks or providers of public communications services. These provisions account for the set of recommendations summarised at EU level following the completion of a corresponding risk assessment ('EU toolbox', cf. document CG 01/2020 from the NIS Cooperation Group, 'Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures', https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures) as well as the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Secure 5G deployment in the EU – Implementing the EU toolbox' (COM(2020) 50 final of 29 January 2020), and are intended to ensure that appropriate responses can be made to the higher security risks associated with the operation of 5G networks.

Some consultation participants requested the extension of requirements for 5G networks to open-access networks, networks run by interconnection partners and internet exchange nodes, and other actors with usage rights to 5G spectrum, who wish to use infrastructure by means of network slicing or multi-access edge computing. This is not only problematic—internet exchange nodes are subject to the NISG, for example, and are not governed by the TKG or this Ordinance since telecommunications services are not provided—but also unnecessary on account of the low number of subscribers involved.

Par. 1: Since the security measures to be implemented by operators must guarantee a certain level of security that is suitable for controlling risks, and these risks, in turn, depend on the probability of occurrence and the potential consequences of a security incident, it is justified to consider the number of subscribers when assessing the degree of risk. Comparable regulations, such as Art. 10 Par. 1 No. 2 Point (a) of the Network and Information Security System Ordinance (NISV), FLG II No. II 215/2019 utilise a figure of 88,000 subscribers to communications services in the context of operating DNS services as key services within the 'digital infrastructure' sector. It is therefore justified that a forward-looking assessment of the higher level of risk involved in operating 5G networks also considers the growth in subscriber numbers until the first point in time that proof is submitted and therefore assumes a correspondingly higher value.

To respond to this higher level of risk, a functional information security management system as well as information security measures both specific to telecommunications and of a general nature are required. Proof of this functional information security management system can be furnished by submitting an audit report verifying compliance with the requirements of 'ÖVE/ÖNORM EN ISO/IEC 27001:2017, Information technology — Security techniques — Information security management systems —

Requirements (ISO/IEC 27001:2013 + Cor 1:2014 + Cor 2:2015)'. The specification and implementation of general information security measures can be documented using a statement of applicability as stated in ISO 27001, Clause 6.1.3 Point (d). The specification and implementation of information security measures specific to telecommunications services can be documented using a declaration modelled on the security measure specification and implementation given in 'ÖVE/ÖNORM EN ISO/IEC 27011:2020, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organisations'.

Instead of the standards mentioned above, standards viewed as equivalent by the regulatory authority may also be used, such as the 200-1, 200-2 and 200-3 standards from the German Federal Office for Information Security in conjunction with ITU-T Rec. X.1051. The issue of self-audits was raised during the consultation process. To clarify: the preparation of audit reports in this context must be entrusted at all times to accredited testing laboratories or qualified bodies as defined by Art. 3 No. 11 of the NISG. The deadline stated for the first submission of proof is intended to allow operators who do not yet conform to the standards the time needed to establish the necessary prerequisites for certification and to complete the certification process. The three-year period for repeat audits corresponds to typical audit cycles.

Par. 2: As a result of the EU 5G toolbox, operators of 5G networks with over 100,000 subscribers shall also implement the security measures envisaged in the relevant 3GPP and ETSI technology standards listed in the Appendix (cf. https://www.3gpp.org/DynaReport/33-series.htm), as well as the 'virtualisation good practices' defined by ENISA, and document the same by means of a declaration of conformity from the operator. All of the documents listed in Appendix 1 are publicly available. The requirement made in the EU 5G toolbox to additionally ensure the implementation of optional parts of the 3GPP technology standards in an appropriate manner is reflected in the requirement for the operator to justify deviations relating to the optional parts by (e.g.) implementing comparable security measure that achieve the exact same security goal. The suggestion raised in the consultation procedure to replace the specified ETS-GS-NFV-SEC standards with the ENISA document 'Security aspects of virtualisation' (cf. https://www.enisa.europa.eu/publications/security-aspects-of-virtualization/at_download/fullReport, 10 February 2017) was accepted. The necessity to comply with the above-mentioned ENISA document and particularly the provisions from chapter 3 of that document, entitled 'Virtualisation good practices', instead of the ETSI Network Function Virtualisation standards (NFV, cf. https://www.etsi.org/standards#page=1&search=&title=1&etsiNumber=1&content=1&version=0&onApproval=0&published=1&historical=0&startDate=&endDate=&harmonized=0&keyword=&TB=799&stdType=&frequency=&mandate=&collection=&sort=1) as previously specified results from the fact that the complexity introduced by virtualisation also involves a higher level of risk, as well as from the requirement in the EU 5G toolbox for 5G operators to follow good practice in relation to NFV. The necessity to comply with the requirements listed in the ENISA document 'Indispensable baseline security requirements for the procurement of secure ICT products and services' (cf. https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services) is in response to the EU 5G toolbox requirement for specific security standards to be maintained in the procurement process for ICT components and services. In the consultation process, it was suggested that an implementation of the provisions of the 'indispensable baseline security requirements for the procurement of secure ICT products and services' mentioned above might be required only for awards made after 30 June 2021. This is not correct: by the stated date, a corresponding declaration of conformity must in fact be submitted that provides proof of compliance with the ENISA ICT Baseline Security Requirements.

Par. 3: The security measures listed correspond to additional security measures in the EU 5G toolbox that are not derived from the requirements in Par. 1 and Par. 2.

For example, operation of the Network Operation Centre and Security Operation Centre on one's own premises (i.e. premises under the control of the 5G network operator, such as rented data centres but not premises owned by external service providers) as well as the effective monitoring of critical network components and sensitive parts of the 5G network is designed to ensure that anomalies are detected and threats (e.g. arising from compromised end devices, incl. IoT components) are identified and prevented. For these reasons, and because of the need to comply with the provisions of the EU 5G toolbox, the weakening of the requirement to operate an NOC and SOC on one's premises sought after by many consultation participants—by deleting the word 'own', for example—could not be accommodated. To clarify, however: the NOC and SOC can be housed in a single room under the control of the 5G network operator, and can be operated from this same room.

The protection of management traffic in communications networks or services is designed to prevent unauthorised changes to network or service components.

The physical protection of critical network components and sensitive parts of 5G networks, using a risk-based approach, shall also encompass network components outside the core network, such as base stations, which communicate with one another to achieve low latencies ('multi-access edge computing'). In the consultation process, it was criticised that the expressions 'critical network components' and 'sensitive parts' as used in Art. 6 Par. 1 Nos. 2 and 6 had not been defined. In response, the level of risk arising from the criticality of network components and sensitive parts of the network is not static but must be re-assessed continuously based on the current situation. It is therefore not possible to conclusively define these terms.

A multi-vendor strategy consists of the strategic evaluation of the 5G network operator in terms of the options for selecting an operator from a minimum of two suppliers of infrastructure components for a 5G network as defined in Art. 2 No. 9, while accounting for the latest technical standards and acknowledging the corresponding recommendations made by the European Union. This is intended to reveal dependencies on a single supplier (or suppliers with a similar risk profile) and highlight dependencies leading to a higher level of risk, which should be avoided where possible. In response to the criticism that was raised numerous times in the consultation process, the wording was altered to clarify that the operator of a 5G network must provide evidence of having properly addressed the issue of avoiding dependency on a single supplier.

Supplier risk profiles can be evaluated based on a range of separate factors, including the probability of influence being exerted by non-EU countries, the supplier's delivery reliability and the overall quality of the supplier's products and security practices. RTR GmbH saw the need to include a separate legal basis here, however. In the consultation process, it was suggested that relevant provisions of the TKG concerning the assessment of risk associated with the selection of certain suppliers should be aligned with other provisions of the EU 5G toolbox implemented through the current Ordinance. In response, it must be noted that the new TKG will not enter into force before the end of 2020, while the transposition of the EU 5G toolbox is expected already in summer of this year, thereby excluding any additional alignment processes.

Par. 4: Security-relevant components that are deployed for the operation of the 5G network are listed—grouped and by function—in Appendix 2. In response to the concerns that submitting a list of functions to comply with Par. 4 allegedly involves security risks, it is noted that the provision has been revised several times and watered down significantly in terms of its stringency as a result of related comments and complaints received from operators. The criticism raised again in the consultation procedure represents in part a repetition of suggestions made earlier, which does not seem expedient. The increased level of abstraction achieved by merely indicating functions and manufacturers makes this information much less useful for outsiders. Beyond that, it needs to be noted that RTR GmbH has been managing sensitive data from operators for several decades and can draw on all of the organisational tools it needs for this purpose—not only to ensure that information is transmitted in an encrypted format via the regulator's submission portal but also to guarantee the secure storage of this information at all times. It has recently been argued that submitting an overall list at the start of the year, followed by details of changes at six-month intervals, is better in terms of data protection. In response, it is noted that the exact opposite was asserted in previous discussions: namely, that it would be simpler for the operator to generate an overall list than a change list every six months. In reply to the suggestion that manufacturers should be required to submit a corresponding list, consultation participants are reminded that the regulatory authority is empowered to request information only in relation to the security of networks and services and therefore only from operators of communications networks and providers of communications services.