June 5th 2020

RUNDFUNK UND TELEKOM REGULIERUNGS-GMBH
Mariahilfer Straße 77-79
A-1060 Wien,

Submitted via e-mail to konsultationen@rtr.at

Peter Wukowits / Robert Koenig
CSO Nokia AT / Legal Counsel AT

peter.wukowits@nokia.com
robert.koenig@nokia.com

**Public Consultation to RTR ordinance about obligations for operators with regards to minimum security measures for 5G networks (Telekom-Netzsicherheitsverordnung 2020 – "TK-NSiV" 2020)**

Dear Ladies and Gentlemen,
Dear Mr. Reichinger

Thank you for informing us about the RTR ordinance TK-NSiV and giving us the opportunity to comment on the draft which we gladly provide as follows:

Collaboration with regulatory authorities in Europe is essential so that network security is ensured not only at national level, but also at international level.

It is positive that the ordinance is referring to European recommendations and the European Union (EU) toolbox of risk mitigating measures. This will allow for an internationally harmonized approach to 5G networks security.

Also positive is the common understanding that effective network security requires a holistic approach, based on a thorough risk assessment of all network elements and stakeholders, that applies both technical and non-technical measures. Technical measures are based on standards (3GPP, ETSI), but need to comprise also non-standardized tools (e.g. monitoring and anomaly detection) and best practices (e.g. networking zoning). Especially the 3GPP standards addressed in the ordinance are defining comprehensive security requirements and test cases to ensure that security is built into network elements. Technical assurance schemes can ensure compliance

**Nokia Solutions and Networks Österreich GmbH**
Leonard Bernsteinstraße 10
1220 Wien
Österreich

and may additionally address product lifecycle aspects to ensure that the network remains secure. Nokia supports and proposes the use of a harmonized approach with regards to the Security assurance schemes such as GSMA NESAS, which could help the operators to provide the requested conformity declaration.

Many new use cases such as industrial automation and control or mission-critical public safety networks will all be powered by 5G. Therefore, ensuring the integrity and availability of those networks and protecting them from the ever-growing number and sophistication of cyber-attacks will be more important than ever. Therefore, Nokia supports the 5G Toolbox recommendation of the European Commission (EC) and the initiative of the RTR drafting such ordinance. However, Nokia identified some aspects which should be clarified or amended.

Given the shared common understanding regarding the need for a holistic approach to 5G networks' security, the resulting regulatory framework should also encompass the strategic measures defined in the EU Commission's 5G Toolbox (*inter alia* the creation and definition of a suppliers' risk profiles as identified in the EB (explanatory remarks) to section 6 TK-NSiV). Nokia has understood that these topics will be addressed in the coming amendment of the Austrian Telecommunications Act. Strong prior alignment between the separate regulatory processes would bring consistency and harmonization.

Already today, networks, network and security operation centers (NOC and SOC) as well as supply chains, in particular software supply chains adopting a DevOps approach with continuous integration and continuous delivery, operate across national borders. Taking both this transnational aspect, as well as the cruciality of 5G networks' security mentioned above, the need for similar dispositions in the different European national regulatory frameworks seems essential. As such, an alignment between all EU member states on a common implementation of the 5G Toolbox would increase the overall security of these networks. Nokia would welcome and gladly take part in any initiative taken by the RTR that would lead to such alignment.

With regards to certain terms employed in the ordinance, the following could use some clarification and/or more precise definition:

- Related to section 2 no 2 TK-NSiV: the definition of malicious attacks clearly covers outsider attacks. For clarity, Nokia recommends addressing more explicitly if/that the definition shall also cover malicious insider attacks. Referring explicitly to insider attacks in the definition would allow for insider attacks to be properly reported and documented.
- Related to section 5. para 1 TK-NSiV: regarding both the” adequate security level” (“eines angemessenen Sicherheitsniveaus”) and the “adequate measures” to be taken with respect to the existing risks (“angesichts des bestehenden Risikos angemessen ist”) as well as regarding “adequate tool” (“adequate Werkzeuge”) section 6 para 3 no 6 TK-NSiV:  
  To facilitate a holistic and standardized approach for the terms mentioned before, Nokia recommends referring to the respective section in the 5G Toolbox in order to ensure alignment and common risk approach on a European level.
- Related to section 5. para 1 no 3 TK-NSiV: The security of systems and operation centers comprises also the reliability of supply (“Versorgungssicherheit”). What is RTR’s understanding about minimum security measures *e.g.* for the software supply chain and especially for software supply chains that adopt a continuous integration and continuous delivery approach (DevOps)? In which way and to which extent will the security of software developed and delivered in a DevOps mode be ensured?
- Related to section 6. para 2 TK-NSiV: In order to harmonize the data quality required for conformity declarations to be provided by the operators with help from suppliers Nokia recommends using GSMA NESAS report as basis for such data requests.

- Related to section 6. para 2 TK-NSiV which refers to Annex 1: ENISA document: Nokia supports the outlined principles for secure products and verifiable security. Nokia recommends however, to replace the document with a reference to GSMA NESAS (https://www.gsma.com/security/network-equipment-security-assurance-scheme/) and its development and lifecycle security requirements. As GSMA NESAS provides an industry-wide security assurance framework for these requirements, the GSMA NESAS process audit would examine that network equipment vendors have adequately defined processes for secure design, development, implementation as well as product maintenance and apply them in practice.
- Related to section 6. para 3 no 1 TK-NSiV: It appears that the dispositions developed in the ordinance regarding the NOC/SOC (*i.e.* premises to be located within the EU and owned by the operator) would lead to a stricter normative framework than what the EU 5G Toolbox recommends on this matter. As this would add restrictions, for example when it comes to outsourcing possibilities, which would not necessarily enhance the overall security of the networks, Nokia recommends that NOC/SOC should be operated by a trustworthy supplier according to the criteria developed both by the EU 5G toolbox and the EU coordinated risk assessment of the cybersecurity of 5G networks. Moreover, assessing the trustworthiness of actors involved in the operation of networks would help in mitigating the risk of insider threats and therefore help increasing the overall networks' security.
- Related to section 6. para 3 no 2 and no 4 TK-NSiV: What is to be understood by "critical network components" and "sensitive parts of the network"? What is the reference framework used by RTR to identify such criticality and sensitivity of network elements? In order to avoid confusion, Nokia recommends that such terms be defined in the ordinance and suggests referring to the sensitivity framework developed in the EU risk assessment.

- Related to section 6. para 3 no 4 TK-NSiV: What is meant by physical protection of MEC and base stations? Will all base stations need specific physical protections or are cabinets sufficient? Nokia recommends for the RTR to clarify if this relates to the secure environment defined in 3GPP TS 33.501.
- Related to the annexes: the list of standards will very likely evolve over time. Nokia recommends involving operators and suppliers for such evolutions via a consultation process and implementing transition periods before new standards take effect.

Nokia would like to emphasize its availability to support both the RTR and other regulation and legislation bodies in their efforts to establish an aligned security regulation framework for 5G networks.
As Nokia takes gladly part in this important legislation process, please keep us informed about changes to the draft version of the ordinance.

Best regards,
**Nokia Solutions and Networks Österreich GmbH**

Signature:
Name: Peter Wukowits / Robert Koenig
Title: CSO Nokia AT / Legal Counsel AT
Date: 5th June 2020