DORDA

Clarity.

WHITEPAPER ON THE AUSTRIAN PATH TO 5G CYBERSECURITY

A. IN A NUTSHELL

5G technology enables greater speed and innovation. Connected mobility, smart homes and IoT are just a few examples of business models and the impact this technology has on our society. At the same time, further interconnectivity and integration of systems also increase the risk of cyberattacks. Telecom providers and suppliers of 5G network components are thus responsible to establish a high level of security to protect users and systems. To ensure a coordinated approach on an adequate security level in the EU, the EU Commission and member states have agreed on the EU Toolbox on 5G Cybersecurity ("**EU Toolbox**"). The recommendation contains a catalogue of technical and strategic measures. This shall animate local policy makers to supplement the (binding) data protection and sector-specific laws, such as the Network and Information System Security legislation. In the last few years, this approach caused many controversial discussions in the member states about minimum cybersecurity strategies and engagement of suppliers from non-EEA countries. The Austrian legislator took the following approach to safeguard secure use of 5G on the Austrian market and by the Austrian society:

- ➔ Focus on technical criteria;
- ➔ Reporting obligations to the Austrian Telecommunications Regulatory Authority when implementing 5G equipment for critical functions;
- ➔ Restriction of using equipment and services of providers deemed as "high-risk vendor", whereas
  - the classification of high-risk vendors is done on a case by case-basis;
  - the crucial aspects are technical and security aspects;
  - no general restriction of vendors based on their administrative seat or country of origin applies.
- ➔ Supplementing cybersecurity rules (General Data Protection Regulation, Austrian Data Protection Act, Austrian Network and Information System Security Act, Austrian Ordinance on Network and Information System Security, Austrian Telecommunications Network Security Ordinance 2020) apply.

On first glance, this seems to be a well-balanced approach. Might Austria's framework, thus, be employed as a role model for the highly controversial discussion on reasonable cybersecurity strategies and engagement of suppliers from non-EEA countries in the telecoms sector? It is a fact that the Austrian legislators were very careful in the law-making process and deliberately obtained and reflected stakeholders input from all relevant market participants right from the very beginning. This might be the key to success to the well balanced approach that we may explain in more details for those interested:

B. COMPARISON CHART: EU 5G TOOLBOX VS AUSTRIAN LEGISLATION

1. Landscape and list of cybersecurity related laws/regulations in Austria

1.1. Background

Already back in 2017, the Austrian federal government set the goal of making **Austria a 5G pilot country** by the beginning of 2021 securing a top position for Austria **among the top three in digitization in the EU and top 10 worldwide**. In 2018 a 5G strategy with the goal to accelerate the introduction of 5G mobile technology in Austria by optimizing the framework conditions was issued by the Ministry of Transport, Innovation and Technology. The strategy defines 5G as the infrastructural "key" for the new digital worlds, for Industry 4.0, autonomous mobility, smart cities and smart villages, comprehensive cyber security, state-of-the-art education or the Internet of Things. 5G is identified being advantageous in numerous areas from transport to energy, e-Health, education, and administration. According to Elisabeth Köstinger, the Austrian Minister of Agriculture, Regions and Tourism, the recently published Austrian Infrastructure Report 2022 by the initiative Future Business Austria is a "*clear confirmation that the **roll-out of broadband and 5G infrastructure is of crucial importance for the future of the location, the economy and society***". In April 2021, the Austrian government approved a broadband funding budget of EUR 1.4 billion; by the end of December 2021 another EUR 25 million in funding commitments were released for further expansion of broadband networks.

The rollout of the 5G network is still under construction in Austria, but recent developments show that the Austrian approach (described in more detail below) is a successful concept for making 5G available for the Austrian population.

1.2. Key Players

In the following, we may give you the following overview over the most relevant public agencies responsible for cybersecurity matters in Austria:

The **Austrian RTR** and the **Ministry of Agriculture, Regions and Tourism** as well as the **Ministry of Interior** are the key players shaping Austrian 5G cybersecurity landscape.

Besides, there are a lot more public agencies and institutions engaged with cybersecurity issues:

- The **Cyber Defence Division of the Federal Ministry of Defence** (*Bundesministerium für Landesverteidigung*) sets up cybersecurity strategies, particularly for armed forces.
- The **Cyber Diplomacy** of the Federal Ministry for European and International Affairs discusses strategies on EU and international level.
- CERT.at is the national Computer Emergency Response Team ("**CERT**") acting as the primary point of contact for national cybersecurity incidents. It is the link between other CERTs and Computer Security Incident Response Teams ("**CSIRTs**") for critical infrastructures.

- **GovCERT Austria** is the Government Computer Emergency Response Team for public administration in Austria. The Federal Chancellery (*Bundeskanzleramt*) manages GovCERT Austria in cooperation with CERT.at.
- The **Cyber Security Center** of the Federal Office for the Protection of the Constitution and Counterterrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*) is responsible for incidents relevant to national defence, in particular the protection of critical infrastructures and constitutional institutions.
- The **Office for Strategic Network and Information System Security** is part of Department I/8 in the Federal Chancellery and responsible for matters related to the implementation of the legal obligations under Directive (EU) 2016/1148 ("**NIS Directive**") and the Network and Information System Security Act (*Netz- und Informationssystemsicherheitsgesetz,* "**NISG**").
- The **Austrian Data Protection Authority** (*Österreichische Datenschutzbehörde*, "**DSB**") is responsible for any notified data breaches according to Art 33 GDPR. Thus, the DSB frequently handles cybersecurity related incidents to the extent personal data is concerned. This is frequently the case as regards phishing, ransomware or DDoS attacks.

1.3. List of cybersecurity related laws and regulations

The following laws apply in Austria in the field of 5G cybersecurity. The TK-NSiV and Sec 45 TKG 2021 are, however, the core provisions:

- General Data Protection Regulation ("**GDPR**") and Austrian Data Protection Act (Datenschutzgesetz 2018, "**DSG**"), particularly Art 25 and 32 GDPR setting forth general provisions on privacy by design, privacy by default and adequate technical and organisational measures to protect data subjects' rights;
- Telecommunications Act 2021 (*Telekommunikationsgesetz 2021*, "**TKG 2021**")
- Network and Information System Security Act (Netz- und Informationssystemsicherheitsgesetz*,* "**NISG**");
- Ordinance laying down security measures and detailed provisions for the sectors and for security incidents under the Network and Information Systems Security Act (Netz- und Informationssystemsicherheitsverordnung, "**NISV**");
- Telecommunications Network Security Ordinance 2020 (*Telekom-Netzsicherheitsverordnung 2020*, "**TK-NSiV"**).

Besides, the upcoming NIS Directive II shall specify further cybersecurity measures and close gaps of NIS Directive I (cf pt 4).

The EU Cybersecurity Act, which entered into force in 2019, has not led to any specific Austrian regulation or implementation. Austria sends representatives to the **ECCG** (European Cybersecurity Certification Group), namely the CIO (of the Ministry for digitization and economic affairs) and the NIS office (situated in the Austrian chancellor's office). The focus of **certification** still lies on EU level, although the Austrian institution (*Kuratorium Sicheres Österreich*) introduced the **Cyber Trust Austria Label** in early 2021, being a novation in the EU at that time. ISO certifications are commonly used in Austria.

2. Introduction – 5G Policymaking and Cybersecurity

2.1. Member state actions: Austria as a role model?

As already shortly introduced at the beginning, the approach of the Austrian legislator with regards to the implementation of the EU Toolbox is rather **tech-neutral**:

The Austrian Ministry of Transport, Innovation and Technology specified already in April 2018 in its 5G strategy that 5G expansion should be driven forward by cooperation with *inter alia* Asian countries, including China. It was obviously well aware that high tech, particularly innovative solutions for telecom purposes are mainly developed outside the EEA. With this in mind and the ambitious national goal to enable nationwide coverage with 5G by 2027 (three years earlier than envisaged by the European Commission!), Austria was always focusing on a well-balanced approach enabling its vision.

Further, it was also open for feedback from the market and stakeholders. A political vision is worth nothing if it is not realistic and fails in its implementation. Thus, the Austrian government based its legislative steps and measures on **in-depth discussions with industry representatives** which covered all aspects of the market and society. Not only telecom providers and suppliers, but also business agencies and consumer protection associations were invited to participate and share their market insights and concerns. Based on this, the Austrian legislator has recently adopted the following laws:

- **TK-NSiV**, an Ordinance of the RTR of June 2020, which **implements the minimum standards of the EU Toolbox from a security point of view**. Due to the lack of competence, the RTR has not considered any political aspects and refrained from any regulation dealing with products or services of potential high-risk vendors.
- In November 2021, the new **TKG 2021** entered into force. With its Sec 45 TKG 2021, it transposed the requirements of the European Electronic Communications Code Directive ("**EECC**").

2.2. Avoidance of geo-political discussions and guarantee of fundamental legal rights

The Austrian approach to focus about the high-risk assessment on technical aspects, only, turned out being a very smart move: A system of prior authorization would not only lead to a considerable administrative burden and thus costs for both the respective country and the providers affected by it. Accordingly, the **Austrian legislator decided against prior authorization** from the outset and opted for an evaluation on a case-by-case basis involving expert opinions, voices from the relevant industry and most importantly the vendors concerned.

By focusing on technical criteria, the legislator avoided **any geo-political discussions** and thus allowed one of the most controversial current topics in Europe being solved in an objective and reasonable way. To go into more details: Sec 45 TKG 2021 allows the Ministry of Agriculture, Regions and Tourism ("**BMLRT**") to classify manufacturers of electronic network components as high-risk vendors in case of deficiencies in quality or safeguarding data protection. Latter might either be caused by (i) absence of security or data protection agreements or (ii) binding written declarations by suppliers ensuring that

no unlawful transfer of user data from the EU to third countries may occur. These measures shall ensure an adequate level of protection on a material level. The concept does thus not need to reference to the nationality of the supplier (cf pt 3.2.4 for details).

The Austrian model also foresees legal remedies against decisions to safeguard **fundamental legal rights**. Prior to measures being taken the respective vendor is to be heard. He is further granted the opportunity to take measures to remedy any detected deficiency with the proceedings being discontinued if this was successful. Furthermore, there is the possibility of legal recourse against any decision taken to the independent Federal Administrative Court (*Bundesverwaltungsgericht*). Its decision might be challenged with the Highest Administrative Court (*Verwaltungsgerichtshof*) in case of a legal question of fundamental importance being involved. In the administrative proceedings, the BMLRT is obliged to investigate the facts relevant to the decision *ex officio*. For technical questions that go beyond the expertise of the BMLRT official experts are consulted. Their expert opinion may be commented by the enterprise concerned. These procedural processes are crucial legal instruments to safeguard constitutional legality. With the described approach Austria has achieved a balance between the need to regulate this sensitive area and to prevent drastic consequences (in individual cases even threatening the existence) for component suppliers and network operators.

2.3. Legislative participation: Voices from industry representatives (including chamber of commerce, various associations and MNOs)

During the consultation period of the TK-NSiV and TKG 2021, various industry representatives and political stakeholders raised their voices against a politically driven high-risk vendor assessment. Overall, the following main concerns were issued:

- The industry representatives and political stakeholders took a clear position **against vague worded political criteria** and demanded technical factors for assessing and safeguarding security. The law should **focus solely on components** and their compliance with the necessary safety and legal requirements, instead of classifying a company by its country of origin/seat as this is a non-objectifiable criteria. Various representatives and stakeholders suggested to base the criteria on clear, simple, objective, comprehensible, technical and organizational measures based on an **evidence- and risk-based approach** and not to exclude individual manufacturers per se.
- A frivolous possibility to exclude vendors from the market for geo-political reasons would **massively affect** operators' **choice** of equipment suppliers and **hinder** the concept of the **multi-vendor strategy** by limiting the choice of alternative manufacturers and vendors.
- Even though the regulations directly address equipment suppliers, network operators would be left in a state of **legal uncertainty** due to indeterminate grounds for exclusion and **very far-reaching legal consequences**, as they do not know when selecting their supplier whether the latter will still be able to supply new equipment to Austria or service existing equipment years/months/weeks later. The introduction of almost exclusively politically motivated grounds for restriction would represent an enormous legal uncertainty for network operators, who would have to

rely on European manufacturers, only, to avoid the risk that their supplier is not suddenly black listed. This would severely restrict operators' room for manoeuvre.

- They also highlighted that many components from a wide range of manufacturers are **already in use in Austrian networks**. A (subsequent) **restriction of individual suppliers** could therefore have **unforeseeable consequences** for **domestic network operators** in technical and financial terms. It was stated that an approach based on political criteria in determining high-risk suppliers would be likely to negatively affect investments and increase the economic risk for operators and service providers. The possible exclusion of an essential supplier could subsequently **jeopardize the entire economic basis** of an operator. It would thus be necessary to base an assessment of the (overall) risk and adequate security measures on objectifiable, in particular technical criteria. In this respect reference has also been made to the European level, for example, in the BEREC 5G toolbox, and Art 41 EECC.

- Furthermore, also **lots of companies in the private sector**, *inter alia* telecom providers, demanded a balanced multi-vendor-strategy, arguing with their freedom to provide services:
    - The respective companies emphasized that any **restriction of fundamental rights** in the EU with regard to the free movement of goods and services or entrepreneurial freedom must be based on **objective, non-discriminatory criteria**. This would not be guaranteed by implementing predominantly political criteria. Criteria based on clear, simple, objective technical and organizational measures related to relevant products (IT components and related services) would need to be implemented.
    - A **wrong approach** in determining high-risk vendors **may destroy investments and enormously increase economic risk** for operators and service providers. The withdrawal of an essential vendor could jeopardize the entire economic basis of an operator. Furthermore it is considered to be an interference in free competition and causing lasting damage to the development of Austria as business location. Interventions in the very dynamic telecommunications market are considered to have far-reaching consequences and should not be undertaken lightly.
    - **Political criteria** should be left out of network security issues and would be **unsuitable for assessing** the security of individual components. It targets vendors rather than the security of individual components or services. But this is precisely what should be of paramount importance for network security and integrity. Technical and objective instead of political criteria should be included in the assessment, which would enable a transparent and comprehensible classification of a vendor.
    - The relevant companies in the private sector emphasized that the decision to take action against a vendor must be **uniform and coordinated** across the European Union. The law must consider the **massive impact** such a decision could have on one or more operators or providers. In some cases, even the continued operation of **essential functions** (e.g., voice telephony) could be at **risk**. For operators and providers, swapping one vendor for

another involves enormous effort, as this normally entails far-reaching changes to the architecture.

- Even the national independent Telecommunications-Control-Commission ("**TKK**") and the authority responsible for the broadcasting and telecom regulation ("**RTR**"), which have a leading role both in the legislative and implementation/enforcement of the Telecommunications Act, stressed in the pre-parliamentary review of the TKG 2021 that the classification of a network vendor as a high-risk vendor and its replacement might have serious technical and economic effects on existing networks and that this fact should also be taken into account when assessing the situation. Overall, from authority perspective, the criteria indicating a high risk vendor should focus on security aspects from a technical perspective.

3. Cybersecurity Protective Measures: Regulatory regime in Austria

This intense involvement of the relevant stakeholders led to following fact-driven 5G specific regulatory regime:

3.1. Telecom Network Security Ordinance 2020 - TK-NSiV

In July 2020 the RTR issued the TK-NSiV which applies to operators of electronic communication networks and services. It defines the security and integrity requirements for operators of electronic communications networks and services with regards to in greater detail. As regards 5G networks, the ordinance implements particularly the following measures of the EU Toolbox:

- **Minimum security measures**: Sec 5 requires that providers of 5G networks need to implement certain security measures and policies. Both shall reflect best industry practice, *ie* be "*state of the art*", and cover specific areas, such as governance and risk management, security staff, security of systems and premises.
- **Security measures for 5G-networks**: As of 31st December 2021 operators must regularly demonstrate the RTR that they have implemented appropriate information security management systems, *eg* by complying with standards like ÖVE/ÖNORM EN ISO/IEC 27 001:2017.

  Operators of 5G networks with more than 100,000 users shall further comply with the standards contained in Annex 1 to the TK-NSiV (Annex 1 to this Report). As of 30th June 2021, they must prove compliance with this catalogue by rendering a declaration of conformity.

  In addition, operators must at RTR's request demonstrate compliance with further, specific requirements, eg:
  - Operation of Network Operation Centers (NOC) as well as Security Operation Centers (SOC) on their own premises within the EU;
  - Effective monitoring of all critical network components and sensitive parts of the 5G networks by NOC/SOC to detect anomalies and to identify and prevent threats;

- Protection of communications networks or services to prevent unauthorized changes to network or service components;
- 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;
- Multi-vendor strategy that takes into account the technical constraints and interoperability requirements of different parts of the 5G network. According to the explanatory remarks, the requirement is fulfilled when the operator uses components of minimum two vendors. The provision aims to avoid dependencies in the supply-chain. Further, operators shall not depend on vendors with a similar risk profile. The risk assessment follows Sec 45 TKG 2021.

Operators of 5G networks shall also submit a list of functions and manufacturers of the security-relevant components used for the operation of the 5G network in accordance with Annex 2 to the RTR (including information about the network architecture [Access Network, Packet Switched Core Network, IP Multimedia Subsystem, Service Components, Number Portability, Lawful Intercept, Charging and Billing], architecture description, as well as Network Function Virtualization (NFV), Network Slicing, Software Defined Networking (SDN) and Management and Network Orchestration (MANO) according to the ENISA Threat Landscape for 5G Networks, Version 1.0, November 2019, Multi-access Edge Computing, Physical active switching and transmission systems, components with physical computing, storage and network resources, and telecommunication management), and, if applicable, a list of other components used.

- **Information requirements**: Operators must inform the RTR about relevant incidents via a specific form ("*Notification of incidents with significant impact*").

3.2. Sec 45 TKG 2021 - High-risk vendor assessment

3.2.1. Applicability and Scope

Sec 45 para 1 TKG 2021 states that the BMLRT **may**, **for reasons of national security**, **classify manufacturers of components of a network for electronic communications or providers of services for such networks** (…) **as high-risk vendors** by notice. Doing so, the ministry must follow a specific, strict procedure:

3.2.2. Technical criteria to determine high-risk vendors

A high-risk vendor is defined as someone highly likely unable to comply with the relevant standards applicable in the EU, in particular in the area of information security and data protection. The BMLRT shall, in this assessment, consider the following **technology-neutral criteria**:

- Deficiencies in the quality of the manufacturer's products and cybersecurity practices;
- The absence of either security or data protection agreements between the European Union and the manufacturer's country of residence, if it's a third country, or of declarations of the vendor containing specific binding written provisions to take

technical and organizational measures to prevent unlawful transfers (regardless of whether direct or indirect) of user data to countries outside of the EU;
- An insufficient level of the manufacturer's ability to ensure continuity of supply.

Thus, Austria **neither restricted vendors based on the country of origin nor singled out any corporation**.

3.2.3. Risk-based approach

Further, the BMLRT shall limit the classification based on a **risk-based approach** to

- specific security-relevant business areas;
- a specific period of time (up to 2 years maximum);
- a geographical area; or, as *ultima ratio*,
- exclude the manufacturer/service provider from the supply/provision of security relevant components/services.

3.2.4. Expert council: Advisory Board for Security in Electronic Communications Networks

Prior to classifying a vendor, the BMLRT must consult the Expert Advisory Board and hear the vendor. The Board is to issue an expert opinion on the existence of relevant technical issues for classifying a manufacturer as high-risk vendor within twelve weeks.

The Expert Advisory Board is established at the RTR, which also chairs the Board, conducts its business and acts as its administrative office.

The Expert Advisory Board consists of a chairperson and 12 additional members which are appointed on the proposal of various ministries (*eg* the Federal Ministry for Digital and Economic Affairs or the BMLRT itself), the Chamber of Commerce, the Federal Chamber of Labour, the Federation of Austrian Industry, the National Computer Emergency Team and the Austrian Institute of Technology for a period of 4 years. The Managing Director of the RTR's Telecommunications and Postal Services Division chairs the Expert Advisory Board.

Noteworthy since ensuring a completely independent decision making, is the fact that the chairperson and the other members shall not be bound by instructions in their work for the Expert Advisory Board. This freedom is also guaranteed by the Austrian Constitution (Art 20 Par 2 No 1 Federal Constitution Act).

The quorum of the Expert Advisory Board is constituted if the chairperson and at least six other members are present. The Board passes its resolutions by simple majority of the votes cast. In the event of a tie, the chairperson shall have the casting vote.

The Expert Advisory Board ensures that the broadest possible expertise as a basis for a declaration as high-risk vendor is employed: Its members need to have relevant experience with network infrastructure, IT and security issues. In addition, the Expert Advisory Board can also hear third parties, who may also be representatives of civil society.

By implementing the **obligatory consultation mechanism with the Expert Advisory Board**, the Austrian lawmakers ensure a **foremost technical, fair and justified decision-making process**.

3.2.5. Decision by BMLRT, penalties and right to remedy

The BMLRT determines classification as a high-risk vendor by administrative decision (*Bescheid*) which is open to appeal by the company concerned to the Federal Administrative Court (*Bundesverwaltungsgericht*). The classification as a high risk vendor is not a penalty. In our opinion, the TKG 2021 should be read that the appeal against a high risk vendor decision has suspensive effect. However, this is still unclear, as the Highest Administrative Court (*Verwaltungsgerichtshof*) has not yet clarified whether the BMLRT is also considered a regulator authority.

If a manufacturer has been classified as a high-risk vendor by a legally binding decision and is excluded from the supply (restricted to security-relevant components/ or in general) of network components for electronic communications networks for all or individual of these components, he has to comply with this ruling. Otherwise, he could face penalties up to EUR 100,000 or, in the event of uncollectability, imprisonment for up to six weeks. The same consequences also apply to service providers.

3.2.6. No effect on the 5G spectrum auction participation

It has to be noted that the classification as high risk vendor does not automatically mean an exclusion of the respective vendor from the 5G spectrum auction in Austria.

3.2.7. Outlook and next steps

Given the intrusive nature of the high-risk vendor system, policy makers must take particular care to ensure that the **assessment criteria are objectively justified, proportionate and sufficiently determined**.

From vendor's perspective, it would be useful if legislators issued a list of critical components or published other (binding) criteria or guidance in order to enable a higher degree of legal certainty for all market participants.

3.3. NIS Act / NIS Regulation

The NIS Directive was implemented in Austria in 2018 via the NISG, which applies to (i) operators of essential services, (ii) digital service providers, and (iii) public administration institutions. The key obligations under NISG correspond with the NIS Directive and aim also at ensuring cybersecurity (including 5G infrastructure):

- **Operators of essential services** must take appropriate and proportionate, state of the art technical and organizational security measures to ensure the security of network and information systems that they use in the context of offering the essential service. They must also provide evidence to the Federal Minister of the Internal Affairs that they meet the requirements.
- Similar security measures apply for **digital service providers**.
- Operators of essential services as well as digital service providers must further **notify incidents** to the competent (sector-specific or national) **CSIRT** or **GovCERT**. Such notification must include all relevant information regarding the security incident and the technical environment known at the time of the initial notification, in particular the presumed or actual cause, the information technology concerned, the type of entity or facility concerned. Subsequent notifications are required if information becomes known at a later point in time.

The Federal Minister of Internal Affairs further has an audit right. It is entitled to inspect the network and information systems used for providing the essential service/digital service and any related documents to verify compliance with the security requirements (including on-premises inspections).

4. Way forward: NIS 2.0 concerns/suggestions

The EU Commission has already adopted a proposal for a revised Directive on Security of Network and Information Systems ("**NIS 2 Directive**", latest draft of December 2020; Trilogue negotiations have started in January 2022). The draft expands the scope of the current NIS Directive by **adding new sectors** based on their criticality for economy and society, and by introducing a **size cap** – meaning that all medium and large companies in selected sectors will be included in the scope. The previous possibility for member states to **tailor requirements**, which led to **major fragmentation** with the implementation of the (original) NIS Directive, is thus eliminated, but this broadening also brings negative implications: A large number of institutions is thereby included in the scope on a "flat-rate" basis, without distinguishing which activities or types of installations are in fact classified as important or material. This could hinder the implementation of NIS 2.0 with existing national cybersecurity rules.

Amongst others, the proposal strengthens security requirements for companies by imposing a **risk management approach** providing a minimum list of basic security elements that must be applied. However, it would be advisable if operators could (at least) differentiate according to **sector-specific safety measures**, in order to achieve a **balance between the required safety level and the burden to prove compliance**. Otherwise, the compliance effort especially for small institutions would become disproportionate. Furthermore, the Commission proposes (for the first time) to address **security of supply chains** and vendor relationships. The supply chain risk assessments would consider both technical factors (hardware- or software-related) and, where relevant, non-technical factors. NIS 2.0 envisages a coordinated **EU-wide risk assessment of critical supply chains**, but details are currently unclear, eg about the consequences of such assessments.

Under these circumstances, it would be in the interest of all stakeholders as well as all parties that benefit from improved security (which is, in fact, the entire society), if EU legislators put up a **zero trust approach built on common, certified and technical standards**. Thereby, all entities would gain (legal) certainty and a clear understanding of supplier engagement under NIS 2.0. Such **certification framework** could be drawn up by leading bodies specialized in these fields, such as ENISA, EU member state governments, the European Commission, the International Telecommunications Union and the European Telecommunications Standards Institute. Supplier assessment should be based mainly, if not solely, on technical security criteria that reflect the latest practices in relevant industries as promoted by the aforementioned organizations. If non-technical factors remain to be considered, they must be **inclusive, fact-based and comply with EU law as regards non-discrimination and proportionality**. Further, NIS 2.0 should clarify that Member States must guarantee the **independence of the competent authorities** with a view to ensuring the impartiality of decisions.

Returning to Austria: It is obvious that the **Austrian way** described above, considering practical input in the legislation process, in order to eventually ensure a technical, fair and justified decision-making process, **could also be a role model for EU legislators in drafting NIS 2.0:** It has shown that open and constructive dialogue with industry and relevant business associations should be a major part of the NIS 2.0 legislative process and is of great benefit.

DORDA

Clarity.

Annex 1: Annex 1 to the TK-NSiV 2020

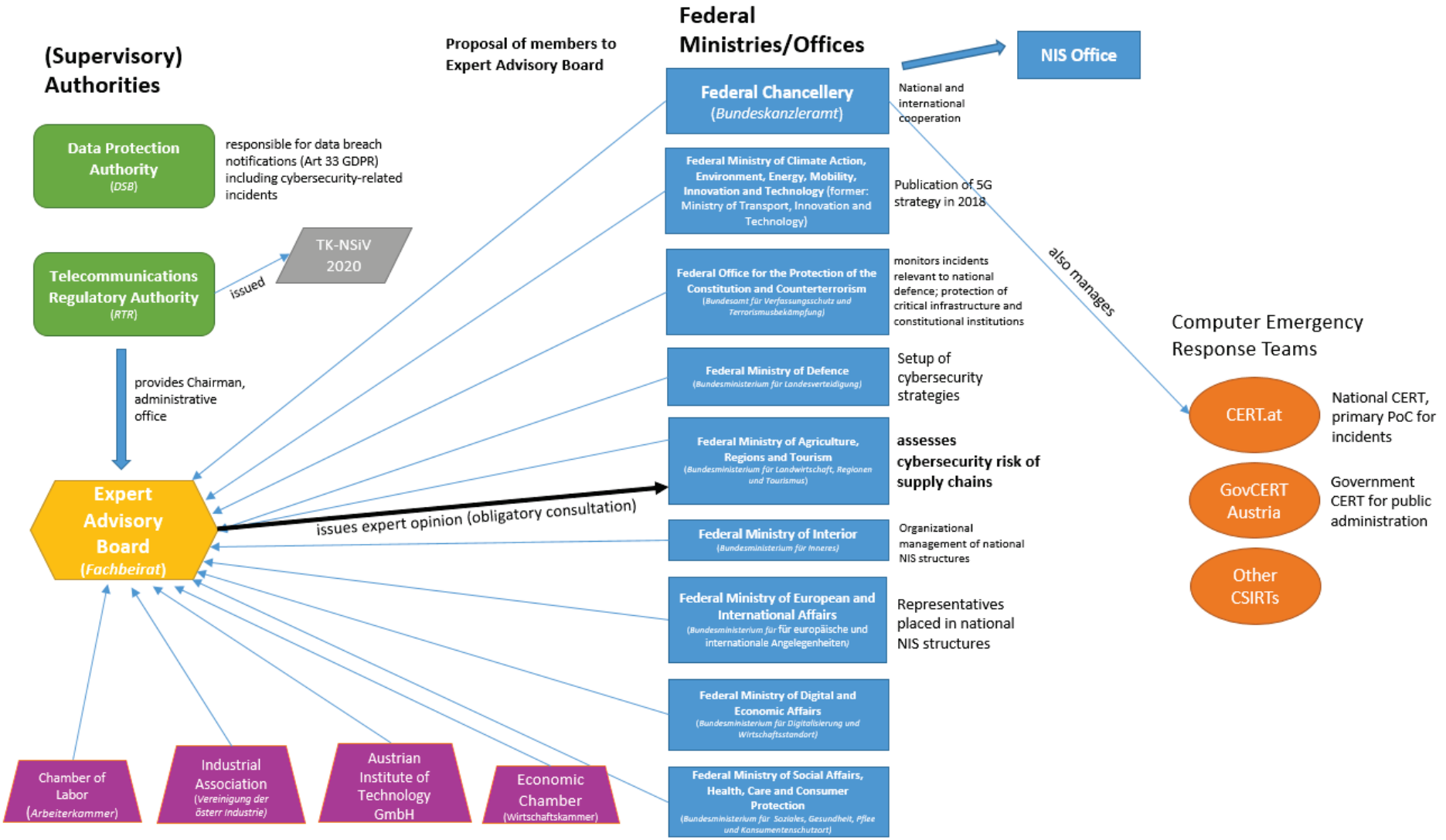
3GPP-Standards:

3GPP TS 33.116 V15.0.0 (2018-06), Security Assurance Specification (SCAS) for the MME network product class
3GPP TS 33.117 V16.3.0 (2019-12), Catalogue of general security assurance requirements
3GPP TS 33.216 V16.2.0 (2019-12), Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class
3GPP TS 33.250 V15.1.0 (2019-09), Security assurance specification for the PGW network product class
3GPP TS 33.401 V16.1.0 (2019-12), 3GPP System Architecture Evolution (SAE); Security architecture
3GPP TS 33.402 V15.1.0 (2018-06), 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses
3GPP TS 33.501 V16.1.0 (2019-12), Security architecture and procedures for 5G System
3GPP TS 33.511 V16.2.0 (2019-12), Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
3GPP TS 33.512 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
3GPP TS 33.513 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS); User Plane Function (UPF)
3GPP TS 33.514 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class
3GPP TS 33.515 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class
3GPP TS 33.516 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class
3GPP TS 33.517 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class
3GPP TS 33.518 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class
3GPP TS 33.519 V16.1.0 (2019-12), 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class

ENISA-Documents:

ENISA Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services, Version 1.0, December 2016
ENISA Security Aspects of Virtualization, February 2017

Annex 2: Austrian Cybersecurity Institutional Map/Ecosystem



Annex 3: HRV clauses legislative process

Previous Draft (Sections 44a and 44b TKG 2020)	Comments issued during the public consultation period	Amended/final version (Section 45 TKG 2021)
• Mostly political criteria for assessing the classification as high risk vendor, such as: ○ A high probability of influence of governmental organizations of a third country on the supplier ○ The possibility of influencing the supplier through legislative acts of a third country, if the supplier is based in this third country ○ The ability of a third country to exert pressure on the manufacturer, especially with regard to the production site ○ Certain characteristics in the ownership structure of the manufacturer that allow a third country to exert influence	• Possibility to exclude vendors from the market for geo-political reasons hinders the concept of the multi-vendor strategy. Instead of vague worded political criteria -> evidence- and risk-based technical factors to assess security • Focus solely on components instead of classifying a company by its country of origin/seat • Approach based on political criteria is likely to negatively affect investments and increase economic risk for operators/service providers and generally represents an enormous legal uncertainty • Any restriction of the free movement of goods and services or entrepreneurial freedom must be based on objective, non-discriminatory criteria, which cannot be guaranteed by implementing predominantly political criteria. The planned restriction could cause lasting damage to the development of Austria as business location. The decision to take action against a manufacturer/supplier must be uniform and coordinated across the European Union.	• Deletion without replacement of all political criteria
• Mere reference to the absence of security or data protection agreements between the European Union and the vendor's country of domicile, if this is a third country when assessing the classification as high risk vendor	• Currently there are only corresponding data protection agreements with only 6 major third countries put in place, which would mean the exclusion of vendors from all other countries.	• Insertion of possibility, that the vendor issues a declaration containing specific and binding written provisions obliging him to take technical and organizational measures to ensure that user data cannot be unlawfully transferred to countries outside the EU or obtained directly or indirectly by the organizations, institutions or authorities of such countries.
• When preparing its expert opinion, the Expert Advisory Board shall also take into account compliance with general rule-of-law standards in the observed third countries in its assessments. No relevance of the technical and economic impact on the electronic communications networks already existing in Austria and their operators in its assessment.	• Exclusion of individual suppliers could have unforeseeable consequences for domestic network operators in technical and financial terms, since many components from a wide range of manufacturers are already in use in Austrian networks.	• Explicit obligation for the Expert Advisory Board to also consider the technical and economic impact on the electronic communications networks already existing in Austria and their operators in its assessment.
• 10 members plus chairperson (without a right of nomination for Austrian Chamber of Labour and Austrian Industry Association)	• Concerns that valuable input form network operators and technical know-how from the field will not be heard enough. Advice to increase the number of representatives and a right to nomination for the Austrian Industry Association. • Necessity to include representatives of users (consumer protection organizations or independent civil society organizations that deal with network security issues)	• Increase in the number of members to 12 plus chairperson including a right of nomination for Austrian Chamber of Labour and Austrian Industry Association