Morgan Lewis | White Paper

THE APPROACH OF THE EU AND SELECTED MEMBER STATES TO 5G NETWORK CYBERSECURITY

Updated February 2021

www.morganlewis.com

Morgan Lewis

THE APPROACH OF THE EU AND SELECTED MEMBER STATES TO 5G NETWORK CYBERSECURITY

EXECUTIVE SUMMARY

This White Paper presents a high-level overview of the current cybersecurity legislation in force or proposed at the European Union (EU) level as well as in a selection of EU member states.

This White Paper is not an exhaustive overview of cybersecurity legislation in the EU. Rather, it focuses on cybersecurity legislation to the extent it affects 5G networks as well as associated hardware, software, and technology in Europe. This White Paper is also limited to a selected sample of EU member states, representative of the very different approaches to cybersecurity of 5G networks of the EU and certain member states, on the one hand, and a group of other member states, on the other.

The EU's cybersecurity toolbox, jointly agreed upon between the EU Commission and member states, advocates a risk-based approach to cybersecurity in line with general principles of EU law. The EU approach therefore proposes a risk assessment, which is based on objective, transparent, and proportionate criteria and is technology neutral. The toolbox recommends a well-balanced and coordinated set of risk-mitigating measures, notably relying on EU-wide standardisation and certification.

Some member states have recently started departing from this joint EU approach, instead choosing to rely on a selection of political criteria in order to address security of their 5G networks and other infrastructure.

This White Paper, which will be updated as developments require,[1] highlights the differences in approach and the deviation from the jointly agreed EU toolbox, as well as, more fundamentally, general principles of EU law.

[1] The information herein is believed to be current and accurate as of the date above. However, given the COVID-19 pandemic, the status and policies of the individually identified authorities are evolving quickly and cannot always be verified. Parties that have critical deadlines pending in any of these jurisdictions should independently verify the information provided and/or request that Morgan Lewis do so on their behalf. We can coordinate with counsel in each jurisdiction upon request.

5G CYBERSECURITY LEGISLATION IN THE EU

	DIFFERENCES				SIMILARITIES	
	Subject to Review (Operators, Suppliers, Products?)	**Review Criteria (Strategic, Political or Technical)**	**Review Decisionmaking Mechanism**	**Scope of Review**	**Legal Force of Review Decision**	**Security Review with Regard to Product or Service**
EU	Suppliers Telecoms operators	Technical Strategic for core areas only, but risk based	N/A*	Different categorisation of network assets: critical and noncritical	N/A*	Categorisation of critical/high/moderate level Risk-based assessment Case-by-case approach
Germany**	Suppliers Telecoms operators with regard to equipment/software in use	Technical** (limited to critical security components) Critical components BSI lists central functions and operators' right to define the critical components/ equipment based on the list Declaration of trustworthiness by suppliers and manufacturers	Exclusion from network possible as last resort based on objective risk assessment if overriding public interests, in particular, security policy concerns of the Federal Republic of Germany, would be in conflict with the use of such critical component	Critical components	Decision of network operator further to guidance issued by the national telecoms regulator, BSI, and the Ministry of the Interior Decision of the Ministry of the Interior in case of exclusion of a critical component, upon consultation from Ministry of Economy, Ministry of Foreign Affairs, and Chancellor's office Appeal before ordinary courts	Focus on critical security components Risk-based assessment Case-by-case approach Transition period No retroactivity
Finland	Suppliers Telecoms operators with regard to equipment/software in use	Technical Strategic for critical components Traficom and operators to define the list of critical components	National Telecoms Regulator Advisory board including the representatives from telecom operators	Critical components	Administrative decision subject to appeal Appeal has suspensory effect	Risk based Case-by-case approach Compensation possible for switching costs
Sweden	Telecoms operators with regard to equipment/software in use and as 5G licence holders	16 technical criteria 1 political criterion Exclusion of operator/supplier from licence award on the following grounds: The likelihood of the operator or supplier being exposed to influence/ pressure. Such influence/ pressure may be applied by, but is not limited to, the presence of the following factors:	Joint assessment of telecoms regulator PTA with Swedish Security Service and the Swedish Armed Forces Conditions for 5G licence auction imposed by the telecoms regulator PTA	All networks	Administrative decision subject to appeal Appeal court may decide that a decision should be suspended pending court decision	Automatic exclusion of the products of two specific suppliers by name Case-by-case approach for the rest

	DIFFERENCES				SIMILARITIES	
	Subject to Review (Operators, Suppliers, Products?)	**Review Criteria (Strategic, Political or Technical)**	**Review Decisionmaking Mechanism**	**Scope of Review**	**Legal Force of Review Decision**	**Security Review with Regard to Product or Service**
		– Connections, including ownership interests, but also other links to government or authorities in third countries (non-EU countries) – Third country legislation, especially in cases where legal or democratic principles are lacking or where no security or data protection agreements can be applied – Links to countries or organisations engaged in offensive cyberoperations or other antagonistic activities against Sweden – Other opportunities for third countries to exert pressure, including in relation to the geographical location of production assets Additional conditions for 5G licence auction imposed by the telecoms regulator prohibit use of Huawei and ZTE equipment by licence holders for 5G rollout				
Romania**	Suppliers Telecoms operators with regard to equipment/software in use	Political Suppliers subject to prior authorisation assessed according to whether the supplier – is not under the control of a foreign government, in the absence of an independent judicial system – has a transparent shareholding structure – has no knowledge of any history of unethical corporate behavior	Prime Minister upon decision of CSAT	All networks	Prior authorisation procedure with decision subject to appeal before the Bucharest Administrative Court Authorisation can be revoked any time on the basis of security considerations	Extension to all telecommunications networks Retroactive effect with transition period of 5 years

	DIFFERENCES				SIMILARITIES	
	Subject to Review (Operators, Suppliers, Products?)	**Review Criteria (Strategic, Political or Technical)**	**Review Decisionmaking Mechanism**	**Scope of Review**	**Legal Force of Review Decision**	**Security Review with Regard to Product or Service**
		– is subject of a legal regime that enforces transparent corporate practices				
Poland**	Suppliers Telecoms operators with regard to equipment/software in use	Political and technical; however, political criteria only can be decisive, such as the following: – The degree and type of links between the supplier of the hardware or software and a non-EU/NATO country – The legislation on the protection of personal data in the supplier's home country, especially where there are no data protection agreements between the EU and that country – The ownership structure of the supplier of the hardware or software – The ability of a foreign state to interfere with the freedom of establishment of the supplier of the hardware or software	Classification as high-risk vendor by the Ministry of Digitalisation (MoD) National Cybersecurity Board (NCB) Plenipotentiary Option 1: ministry of digitalisation acts *ex officio* and consults with NCB Option 2: NCB initiates and provides assessment to MoD	All networks	Administrative decision with immediate effect subject to nonsuspensory appeal administrative court Court hearing *in camera* and right to redact the reasoning of the decision served on the supplier concerned Security warning can lead to prohibition of equipment	Extension to all entities of the cybersecurity system, i.e., major undertakings of critical sectors, such as security and defence, utilities Extension to all telecommunications networks *and* private telecommunications services providers Retroactive effect with transition period of 5 years for high-risk vendors 5 years: critical components (ICT) 7 years: noncritical
Slovenia**	Non-EU suppliers Non-EU service providers (operation, maintenance, upgrade, configuration, and management of networks)	Unclear	Unclear: "Slovenian Government"	All networks	Unclear	Unclear Retroactive effect with transition period of 5 years except for critical components (strictly prohibited with no transitional period)
Austria**	Suppliers	Political: – Lack of quality or cybersecurity practices of the manufacturers, in particular, lack of sufficient control over the supply chain, insufficient compliance with relevant state-of-the-art security	Possibility for the Ministry of Agriculture, Regions and Tourism to classify certain suppliers as high risk and to ban equipment partially or entirely, in all networks or for parts thereof, for a limited time or for a	All networks	Administrative decision subject to review by ordinary courts	Categorisation of high-risk suppliers Entire network No transition period Retroactive effect

	DIFFERENCES				SIMILARITIES	
	Subject to Review (Operators, Suppliers, Products?)	**Review Criteria (Strategic, Political or Technical)**	**Review Decisionmaking Mechanism**	**Scope of Review**	**Legal Force of Review Decision**	**Security Review with Regard to Product or Service**
		practices, including with regard to information security protection objectives (confidentiality, availability, and integrity) – High likelihood of influence of a third country government on the supplier – Possibility of influence on the supplier by legislative acts of a third country if the supplier has its seat in this country – Absence of security or data protection agreements between the EU and the country of residence of the supplier, to the extent this is a third country – The ability of a third country to exert pressure on the manufacturer, in particular, regarding the location of the production facilities – Specific characteristics of the manufacturer's ownership structure, which render influence of a third country possible – Insufficient capacity of the manufacturer to guarantee security of supply – General standard of rule of law in a third country	period of 2 years maximum			

** The security assessment is a competence for Member State Authorities.*
*** Draft legislation.*
****Additional, more politically framed criteria are under discussion.*

EUROPEAN UNION

General Approach

At the EU level, various legal texts and instruments govern the security of telecommunications networks. In January 2020, the European Commission (Commission) and member states agreed to a joint EU Toolbox on 5G Cybersecurity (EU Toolbox). The EU Toolbox recommends a risk-based approach to cybersecurity based "solely on security grounds"[2] and on an objective assessment of identified risks, in full respect of the openness of the EU single market.[3] As a result, the EU Toolbox does not target any supplier or country in particular, but advocates objective and proportionate security measures applicable to all, harmonisation of security standards throughout the EU, and EU-wide certification. In addition, the EU has recently published a proposal for a new cybersecurity directive which, if approved, would provide a much stricter and coordinated framework for member states. This aims at ensuring that the implementation of the EU Toolbox at member state level is consistent and complies with the basic principles of EU law.

Competent Authorities and Relevant Legislation

While operators are largely responsible for the secure rollout of 5G and member states are responsible for national security, the objective of the EU Toolbox is to set out a coordinated EU approach based on a common set of measures, aimed at mitigating the main cybersecurity risks of 5G networks that were identified in the EU coordinated risk assessment report.

Description of Cybersecurity Measures

EU Toolbox

The EU Toolbox provides guidance to member states on how to mitigate risks related to security and integrity of the current or future 5G networks across Europe. It highlights several measures which member states should prioritise in their cybersecurity action plans and recommends that member states conduct a thorough risk assessment in order to set up appropriate and proportionate measures to address concrete risks.

While the EU Toolbox is not binding on member states, it proposes a risk-based mitigation strategy and details a list of technical and strategical measures that member states should look to follow.

Technical measures include measures to strengthen the security of 5G networks and equipment by reinforcing the security of technologies, processes, people, and physical factors:

- Ensuring the application of baseline security requirements (secure network design and architecture)
- Ensuring and evaluating the implementation of security measures in existing 5G standards
- Ensuring strict access controls
- Increasing the security of virtualised network functions
- Ensuring secure 5G network management, operation, and monitoring
- Reinforcing physical security

---

2 European Commission, "Secure 5G Networks, Questions and Answers on the EU Toolbox."

3 European Commission, "Secure 5G Networks, Questions and Answers on the EU Toolbox."

- Reinforcing software integrity, update, and patch management
- Raising the security standards in suppliers' processes through robust procurement conditions
- Using EU certification for 5G network components, customer equipment, and/or suppliers' processes
- Using EU certification for other non 5G-specific information and communications technology products and services (connected devices, cloud services)
- Reinforcing resilience and continuity plans

With respect to **strategic measures,** member states should adopt a holistic approach in their implementation strategy and take into account external factors such as socio-economic costs and environmental considerations. The EU Toolbox also identifies objectives or measures such as:

- Strengthening the role of national authorities
- Performing audits on operators and requiring information
- Assessing the risk profiles of suppliers and applying restrictions for suppliers considered to be high risk—including necessary exclusions to effectively mitigate risks—for key assets
- Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support
- Ensuring the diversity of suppliers for individual mobile network operators through appropriate multivendor strategies
- Strengthening the resilience of networks at the national level
- Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU
- Maintaining and building diversity and EU capacities in future network technologies

With regard to assessing the high-risk profiles of individual suppliers, the Commission suggests that this can be assessed on the basis of a variety of factors without recommending an outright exclusion of specific vendors or products:

- The likelihood of the supplier being subject to interference from a non-EU country. Such interference may be facilitated by, *but not limited to*, the presence of the following factors:
    - A strong link between the supplier and a government of a given third country
    - The third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country
    - The characteristics of the supplier's corporate ownership
    - The ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment
- The supplier's ability to assure supply
- The overall quality of products and cybersecurity practices of the supplier, including:

- The degree of control over its own supply chain and whether adequate prioritisation is given to security practices
- The assessment of a supplier's risk profile may also take into account notices issued by EU authorities and/or member states' national authorities

Each member state shall take necessary measures to respond appropriately and proportionately based on actual risks identified. Each member state shall carry out mitigation plans considering implementation factors such as cost and economic and/or social impact. The implementation of the EU Toolbox shall comply with EU basic principles; in particular, the free movement of goods and services, and fair competition, as well as general principles of EU law. Specific vendors or products are not excluded.

Finally, supporting these measures by member states, the Commission intends to take its own measures to maintain a diverse and sustainable 5G supply chain in order to avoid long-term dependency, including by making full use of the existing EU tools and instruments (FDI screening, trade defence instruments, competition); further strengthening EU capacities in the 5G and post-5G technologies; using relevant EU programmes; funding and facilitating coordination between member states regarding standardisation to achieve specific security objectives; and developing relevant EU-wide certification schemes.

Other Applicable Rules Governing Cybersecurity

Under the EU telecommunications framework, obligations can be imposed on telecommunications operators. Member states are required to ensure the integrity and security of public communications networks and that public communications networks or services take measures to manage security risks. The framework also provides that competent national regulatory authorities have powers to issue binding instructions and ensure compliance.

The European Electronic Communications Code[4] (EECC), which replaced the current framework on 21 December 2020, maintains and extends the security provisions of the current framework and introduces definitions on the security of networks and services and security incidents. In addition, the EECC provides that security measures should take into account all relevant aspects of certain elements in areas such as security of networks and facilities, handling of security incidents, business continuity management, and monitoring, auditing, and testing as well as compliance with international standards. Member states were asked to implement the EECC by 21 December 2020.

The NIS Directive[5] requires operators of essential services in other fields (energy, finance, healthcare, transport, digital service providers, etc.) to take appropriate security measures and to notify serious incidents to the relevant national authority. The NIS Directive also provides for coordination between member states in case of cross-border incidents affecting operators in its scope.

The Cybersecurity Act[6] creates a framework for European cybersecurity certification schemes for products, processes, and services. It allows for the development of cybersecurity certification schemes to respond to the needs of users of 5G-related equipment and software.

---

4 Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code (Recast).

5 Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, [2016] OJ L 194.

6 Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), [2019] OJ L 151.

Outlook

The Commission had called on member states to take steps to implement the set of measures recommended in the EU Toolbox by 30 April 2020. On 24 July 2020, EU member states, with the support of the Commission and ENISA, the EU Agency for Cybersecurity, published a report on the progress made[7] in implementing the joint EU Toolbox of mitigating measures. The Commission will be watching member states' implementation of the EU Toolbox very closely.

On 14 December 2020, ENISA published its 2020 5G Report including several recommendations, which all aim at collecting cybersecurity-related information, consolidating stakeholder work, analysing cybersecurity threats, developing joint responses, and performing gap analyses at the EU level, stakeholder level, and national level.

On 16 December 2020, the EU announced its New Cybersecurity Strategy, which contains concrete regulatory proposals and investment and policy initiatives with respect to increasing resilience and technological sovereignty; building operational capacity for prevention, deterrence, and response; and advancing a global and open cyberspace via increased cooperation. Specifically, this strategy includes two proposals for directives in the cybersecurity sector.

Proposal for a Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS 2)[8]

The proposal for an NIS 2 directive provides for a complete and detailed European framework for cybersecurity. It imposes several obligations on member states and private entities active in the EU.

First, a member state would be required to prepare and maintain a detailed cybersecurity strategy along with a set of policies regarding cybersecurity in the supply chain of ICT products and services, vulnerability disclosure, specification of cybersecurity requirements for in-public procurement, development of cybersecurity tools by research institutions, guidance for SMEs, information sharing between companies, and awareness and skills raising. The member state would also have to notify the Commission of these policies and strategies. These policies would be scrutinised via a member state–level peer review system.

Second, the member state would create or designate one (or more) competent national authority(ies) to manage potential crises and incidents in accordance with a crisis response plan that the member state is also required to create. The national authority would also hold a liaison function with the authorities in other member states and monitor the application of the directive in its state. The national authority would further enjoy a vast array of investigative powers to ensure that the obligations of the directive are not violated, including the possibility to impose administrative fines to private actors referred to as "essential and important entities" (i.e., digital providers and digital infrastructures included in a registry which will be created and kept by the EU's cybersecurity agency).

Incident handling would be conducted by each member state's "computer security incident response team" (CSIRT). Specifically, on a day-to-day basis, the team would monitor threats, provide early warnings to interested parties, respond to incidents, provide proactive assessments and analysis, and provide assistance to CSIRTs in other member states. CSIRTs would set up standardised practices to conduct the tasks mentioned above.

The proposal also provides for the creation of a "Cooperation Group" at the EU level, which would be composed of representatives from member states, the Commission, and the EU's cybersecurity agency (ENISA). The group's main purpose would be to facilitate information exchanges and strategic cooperation among member states. To further cooperation, the proposal would also create the

---

7 [2018] OJ L 321/36.

8 Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.

European Cyber Crises Liaison Organisation Network (EU-CyCLONe) to manage large-scale cybersecurity incidents and crises.

Finally, private actors, and more specifically "essential and important entities," would also have to comply with additional obligations to manage cybersecurity risks when providing their goods and services. Such entities are also required to "take into account the vulnerabilities specific to each supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers" when managing their cybersecurity risks. Such entities will also have the possibility to exchange information regarding their cybersecurity practices according to a procedure set up by their member states.

Proposal for a Directive on the Resilience of Critical Entities

This directive would apply specifically to entities that are identified by each member state as providing an essential service (a service that is "essential for the maintenance of vital societal function or economic activities") with infrastructure located within the territory of the member state and on which a cybersecurity incident would have a disruptive effect on the provision of the essential service.

These critical entities would have several obligations including reporting to the relevant authorities, conducting risk assessments, and implementing other measures which member states would require to ensure the entities' resilience in the event of a crisis or disruption.

Member states would also be required to designate a public body to conduct risk assessments regarding essential services and adopt a detailed strategy on the resilience of critical entities. Such strategy will have to include objectives and priorities, a framework to achieve these objectives, a description of specific measures to enhance resilience, and a policy for enhanced coordination among member states' authorities.

Both proposals are currently under consideration by the EU Council and Parliament, both of which must approve the text before it becomes EU law. There is no specific legislative timetable at the moment.

GERMANY

General Approach

The German legislation does not foresee the exclusion of specific 5G suppliers. Instead, security requirements are generally being tightened for everyone, with specific rules on critical infrastructure. These new criteria are defined in a new security catalogue for the operation of telecommunications networks drawn up by the Federal Network Agency, and a draft bill on IT security, the latter of which is currently being debated in German Parliament. Notwithstanding, while including the possible exclusion of networks as a measure of last resort, the Draft IT Security Act 2.0 leaves the German 5G networks open for all manufacturers, and any such exclusion would require hard evidence of an objective risk.

Competent Authorities and Relevant Legislation

The main law regulating German telecommunications networks is the Telecommunications Act (*Telekommunikationsgesetz* or TKG). TKG Section 109 defines certain protection objectives and obligations.

- TKG Section 109(1) defines the protection of personal data and the protection of telecommunications confidentiality as *general* protection objectives. It is each service provider's responsibility to pursue these general protection objectives.

- Section 109(2) of the TKG defines *special* protection objectives concerned with the protection of telecommunications infrastructure from disruptions and risks as well as the availability of telecommunications services. The pursuit of those special protection objectives is restricted to the operators of public telecommunications networks and the providers of publicly accessible telecommunications services.

To achieve these general and special protection objectives, all companies must take appropriate technical precautions and other measures. A precaution or other measure is appropriate only if the technical and economic effort required for it is not disproportionate to the importance of the telecommunications networks or services to be protected (TKG Section 109(2), sentence 5).

The competent authority to monitor compliance with TKG Section 109 is the Federal Network Agency, which is the national telecommunications regulatory authority.

In addition, security risks associated with the use of IT are investigated and monitored by the Federal Office for Information Security (*Bundesamt für Informationssicherheit in der Informationstechnik* or BSI) which also develops preventive security measures in this regard. The tasks and powers of the BSI are set forth in the Act on the Federal Office for Information Technology (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* or BSIG).

A draft bill to, among other things, amend the TKG and the BSIG (Draft IT Security Act 2.0) is currently being debated in German Parliament. Key amendments proposed concern the implementation of various mechanisms foreseen by the EU Toolbox, including also the last resort (measure SM03) to potentially exclude certain manufacturers from the procurement of critical components used in critical infrastructures, such as telecommunications networks (for more, see *Draft IT Security Act 2.0* below).

Further, the Draft IT Security Act 2.0 proposes to extend the responsibilities of the BSI to also become the national authority for cybercertification (notably of critical components) and to be responsible for ordering telecommunications operators to take necessary data and information security protection measures.

Description of Cybersecurity Measures Under the TKG

Operators of public telecommunications networks and providers of publicly accessible telecommunications services must appoint a security officer and present the technical and organisational protective measures they have taken in a security concept to the Federal Network Agency as per TKG Section 109(4). Compliance with these security requirements is mandatory for all companies. The Federal Network Agency reviews the implementation of the security concepts regularly (i.e., at least every two years).

The basis for the security concept and for the technical measures and other measures to be taken by operators is the "Catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data according to § 109 of the TKG" (Security Catalogue), which was drawn up by the Federal Network Agency in agreement with the BSI and the Federal Commissioner for Data Protection and Freedom of Information.

In addition, the Federal Network Agency can order that operators of public telecommunications networks or providers of publicly available telecommunications services undergo a review by a qualified independent body or a competent national authority (TKG Section 109(7)). The purpose of such review is to determine whether the requirements of TKG Section 109(1)–(3) have been met. The Security Catalogue can thus also form the basis for the security audit of a qualified independent body in accordance with TKG Section 109(7).

Criticality of the Network

The security concept under TKG Section 109(4) needs to take account of the criticality of the network, to the extent that it has to provide an analysis of the hazards expected. The assessment of criticality takes account of the *common good interests* protected by TKG Sections 109(1) and (2): *telecommunications secrecy, data protection, and functionality of the network*.

The decisive factor in determining criticality is the importance of the telecommunications network or service to be protected:

- **Standard criticality**: All public telecommunications networks and services.
- **Elevated criticality**: Public telecommunications networks and services for more than 100,000 subscribers.[9]
- **Increased criticality**: Public telecommunications networks and services with special importance for the common good. This is the case for the public mobile network of which the cross-sectional use can be assumed. This covers *publicly accessible 5G mobile networks*, which are operated *with a number of subscribers greater than 100,000*.

After completing the risk analysis, the obligated company must select and implement suitable, necessary, and appropriate protective measures. An assessment of individual cases is always decisive for selection and determination. It is not the abstract assignment to a hazard situation but always the result of the concrete, individual hazard analysis that is decisive for the determination of the protective measures.

First, the state of the art must be taken into account when determining the measure. Second, the protective measures to be taken in individual cases are only appropriate if the technical and economic effort is appropriately proportionate to the importance of the rights to be protected and the importance of the facilities to be protected for the general public. There must be no disparity between the effort to be made and the benefit to the general public. The IT Basic Protection Compendium of the BSI (*IT-Grundschutz Kompendium*) offers assistance in selecting specific measures.

---

[9] Reference is made to Postal and Telecommunications Security Act [Post-und Telekommunikationssicherstellungsgesetz (PTSG)]. *See also* Ordinance for Determining Critical Infrastructures according to the BSI Act (BSI-KritisV).

General Measures Under the TKG

Organisational and risk management include *supplier management*; further to which:

- Reliability of the third party must be assessed on the basis of suitable information before commissioning
- Third parties are to be bound by contract, which includes security requirements
- Third parties are bound to act in accordance with data protection law through appropriate contractual arrangements
- Compliance with security requirements is monitored on a regular basis
- Security requirements for personnel management, which includes security checks, security expertise and awareness, handling personnel changes, and dealing with violations
- Security of data systems and facilities, such as secure handling of sensitive data, information and communication and metadata, physical and elementary protection requirements, security of supply, access control, protection of integrity and availability of network and information systems, and protection against viruses, code injections, and other malware.
- Proper and secure operational, change, and asset management
- Detection of, reaction to, and reporting of malfunctions and security incidents
- Suitable emergency or failure management strategy
- Monitoring of security-related events, emergency exercises, and testing procedures of network and IT systems[10]

Specific Measures Under the TKG

Specific measures apply to networks and services with increased criticality.[11]

Certification of Critical Components

The responsible national authority for the IT security certification of critical components is the BSI. The BSI is also responsible for the national recognition of test centres as part of the national IT security certification.

In consultation with the Federal Network Agency, the BSI will draw up and publish a technical guideline for the networks. In addition, it describes conditions for the provision of certificates according to European certification schemes (CSA).

Together with the BSI, the Federal Network Agency will create a document that lists the critical functions in a telecommunications network. Critical functions are identified by the Federal Network Agency and the BSI on the basis of a joint risk analysis and on the basis of the current state of the art and are included in the list. According to the Federal Network Agency and BSI's assessment, the list is continuously updated, especially if essential conditions have changed. The results of national or international risk analyses such as ENISA or BEREC are taken into account.

---

[10] Certain further requirements are to be observed further to area-specific regulations which regulate, inter alia, the protection of personal data and traffic data.

[11] Annex 2 to the Security Catalogue, Additional security requirements for public telecommunications networks and services with an increased risk potential, as of 13 May 2020.

Manufacturers, associations of public telecommunications network operators, and associations of providers of publicly available telecommunications services are given the opportunity to comment. The list will be published in the Official Journal of the Federal Network Agency.

Certification of critical components installed after 31 December 2025 is to be made by a recognised certification body in accordance with the Cybersecurity Act or equivalent measures, where not available.[12] Components already installed or to be installed should meet the certification requirements as soon as suitable; appropriately certified products from different manufacturers are available on the market and at the latest by 31 December 2025.

Declaration of Trustworthiness of Manufacturers and Suppliers

Public telecommunications network operators and providers of publicly accessible telecommunications services with increased criticality are required to obtain a comprehensive declaration from the manufacturer or supplier to demonstrate its trustworthiness. The declaration must relate to all safety-relevant components and, if applicable, functionalities, as well as the supply source itself (the manufacturer, including the supplier, and, if applicable, the seller or supplier).

The specific content is to be determined by the obligated company in each individual case. It is recommended that breaches of the declaration be punished with contractual penalties.

The following *nonexhaustive list* of the content of a declaration of the trustworthiness of a supply source is provided in Annex 2 of the Security Catalogue:

- Obligation to cooperate intensively with the consumer in the field of security technology and, in particular, to provide information at an early stage about new products, technologies, and updates of existing product lines
- Assurance that no information from its contractual relationships with the consumer or one of its offices will be passed on to third parties
- Obligation to ensure, through organisational and legal measures, that confidential information from or about its customer(s) does not end up abroad at its own initiative or at the initiative of third parties or that foreign agencies in Germany become aware of it
- Assurance that it is legally and actually able to refuse to disclose confidential information from or about its customers to third parties
- Obligation to notify the user immediately in writing if compliance with the declared obligation can no longer be guaranteed, in particular if a need or obligation arises for it or if it could have recognised one that could prevent him from fulfilling this obligation
- Obligation to provide specific information about the product development of the safety-related system parts of its products on request
- Obligation to use only particularly trustworthy employees for the development and manufacture of the safety-critical system components
- Declaration of willingness to agree to security checks and penetration analyses on its product to the required extent and to provide appropriate support
- Assurance that the product for which the declaration is made does not have any deliberately implemented vulnerabilities and that these will not be installed at a later date, and that all

[12] Details on the requirements from 2.4, in particular on the certification schemes to be used, are regulated in the BSI's Technical Guideline.

known unintended vulnerabilities have been remedied or will be remedied immediately in the future

- Obligation to immediately report known weaknesses or manipulations or ones that become known to the consumer so that measures can be taken at an early stage to limit and remedy possible consequences of quality defects

- Explanation of whether and how the supply source can sufficiently ensure that the critical component does not have any technical properties that are capable of exerting an abusive influence on the security, integrity, availability, or functionality of the critical infrastructure (e.g., through sabotage, espionage)

Diversity of Supply

Annex 2 of the Security Catalogue requires the use of critical network and system components from at least two different manufacturers for the core network (backbone and core network), the transport network, and access networks (radio access networks/wired access networks), unless the mobile network operator's own developments are used. These manufacturers should be independent of each other and not equally dependent on a third party. In particular, critical network functions and network elements should not depend on a single provider of critical components based on the network topology implemented.

The Security Catalogue proposes to support this by the application of open standards, such as Open RAN, in the event of future developments in the state of the art.Further requirements relate to the guaranteeing of product integrity, safety requirements during operation, required professional qualifications of staff, and sufficient redundancies.

Draft IT Security Act 2.0

The Draft IT Security Act 2.0 is currently being debated in the German Parliament. Among other things, the Draft Security Act 2.0 proposes significant amendments to the BSIG including the implementation of a new Section 9b, which provides for a new two-step procedure (i.e., (1) notification and (2) certification/prohibition) for critical components used in critical infrastructure (e.g., telecommunication networks).

Notification

Draft IT Security Act 2.0 Section 9b provides for the obligation of operators of critical infrastructure to notify the BSI of the use of critical components for which a certification obligation by law is required. In this context, critical infrastructure operators would need to ensure to only use critical components from manufacturers which have issued a statement of trustworthiness covering the whole supply chain (Guarantee Statement).

- The term "critical components" shall be defined (1) by law, or (2) for operators of critical infrastructure insofar as they operate public telecommunication networks or provide publicly accessible telecommunication services by the catalogue of safety requirements under TKG Section 109(6). It is expected that such definition provides an increased legal certainty.

- The Guarantee Statement would need to include, among other things, whether and how the manufacturer can adequately ensure that the critical component does not have any technical properties that could be misused; in particular, for the purpose of sabotage, spying, or terrorism to influence the security, integrity, availability, or operability of the critical infrastructure.

- The minimum requirements for the Guarantee Statement shall be determined by the BSI taking into account public interests such as particularly security policy concerns.

Certification or Prohibition

As a last resort, the BSI would be entitled to prohibit the use of critical components within one month after receipt of the critical infrastructure operator's notification. Such prohibition would be possible if overriding public interests, in particular, security policy concerns of the Federal Republic of Germany, would be in conflict with the use of such critical component.

- Whether the use of a certain critical component will be prohibited shall be decided upon agreement with the ministries affected by such decision. For example, in the telecommunication sector this would be the Federal Ministry for Economic Affairs and Energy. If foreign and security policy issues are affected, the Federal Foreign Office would need to be involved.

- If the ministries affected will be unable to reach a common understanding, this will trigger an escalation mechanism to the respective ministers and, if there is still no consensus, to the federal government's internal disputes resolution procedure.

- The examination would need to be carried out by means of an objective risk assessment. The proposed scope of examination would be rather wide. The wording in this respect requires an assessment of potentially overriding public interests, which particularly shall include security policy concerns of the Federal Republic of Germany, but may also be of technical nature.

Prohibition of Further Operation

In addition, the Draft IT Security Act 2.0 includes the BSI's right to prohibit the further operation of an already implemented critical component vis-à-vis the operator of the critical infrastructure, if the manufacturer of the critical component has proven to be untrustworthy. A manufacturer of critical components is considered untrustworthy if any of the following apply:

- The manufacturer does not comply with its issued Guarantee Statement.

- The facts indicated in the Guarantee Statement prove to be wrong.

- It does not sufficiently support security checks and penetration analyses.

- It does not notify the operator of the critical infrastructure of known weaknesses or manipulations or those that have come to his knowledge and does not eliminate them.

- The critical components are likely to lead to an abuse of the security, availability, or functionality of the critical infrastructure.

Outlook

The Draft IT Security Act 2.0 was introduced in German Parliament for a first reading on 28 January 2021. It will be subject to debate; in particular, on the minimum content of the Guarantee Statement to be defined by the Ministry of the Interior.

The two-step procedure proposed by the Draft IT Security Act 2.0 will strengthen the powers of the federal government and increase the technical and legal requirements for manufacturers of critical components for critical infrastructure. Thereby, the Draft IT Security Act 2.0 implements into German national law the recommendations of the EU Toolbox, which emphasises the objective evaluation of risk profiles of manufacturers, while ensuring that EU law principles are not violated and allowing to work toward harmonised certification and cybersecurity measures.

FINLAND

General Approach

With a dedicated authority for national cybersecurity and an advanced legal framework, Finland ranks as one of the most cybersecure nations in the world. There is, however, no specific exclusion of specific suppliers. Rather, the legislation operates with strict security requirements, supplier risk assessments, and the possibility of restrictions on use of certain equipment.

Competent Authorities and Relevant Legislation

The Finnish Transport and Communications Agency (Traficom) is responsible for monitoring and promoting the communications markets and services in Finland. Since 2014, the National Cyber Security Centre Finland (NCSC-FI) operates within Traficom. It is the national information security authority and maintains nationwide awareness of cybersecurity.

Description of Cybersecurity Measures

Act on Electronic Communications Services

Under the Act on Electronic Communications Services (AECS) [Fi: Laki sähköisen viestinnän palveluista / Sw: Lag om tjänster inom elektronisk kommunikation],[13] the NCSC-FI supervises the activities of a number of operators, including traditional telecommunications operators, providers of communications networks and communications services, and digital infrastructure providers under the NIS Directive.

Many of the measures suggested in the EU Toolbox are already in force or established practice in Finland, such as

- quality requirements for communication networks and services (AECS paras. 243-244);
- risk assessment of suppliers and equipment (*see, e.g.*, AECS para. 260); and
- the possibility of applying restrictions for equipment considered to pose a "risk" to people's health or security or other public interests (*see* AECS para. 262).

Quality Requirements for Communication Networks and Services

The AECS provides detailed information on how telecommunications companies and other relevant operators must act to ensure information security in their networks and services. In particular, paragraph 243 imposes quality requirements for communications networks and services that are designed, built, and maintained to ensure that, among other things,

- the technical standard of electronic communications is of a high standard and information secure;
- they can withstand normal and foreseeable climate-related, mechanical, electromagnetic, and other external interferences as well as threats to information security;
- performance, functionality, quality, and reliability can be monitored;
- significant violations of and threats to information security can be detected (this also includes detection of errors and disruptions that significantly disrupt the function of the networks/services);

[13] English version may not directly correspond to the most recent Finnish and Swedish official versions.

- no data protection, information security, or other rights are compromised;
- they are interoperable and the communication networks can be connected to other communication networks if necessary; and
- changes made to them do not cause unforeseen interruptions in other communication networks and services.

Risk Assessment

Under AECS paragraph 251, any radio equipment used in Finland must comply with a number of requirements, including those related to

- protection of the security and health of people and animals, and protection of property;
- electricity safety;
- adequate levels on electromagnetic compatibility; and
- efficient use of radio frequencies (including for the purpose of avoiding harmful interference).

If Traficom has reason to believe that certain radio equipment poses a potential risk to people's health or security, or other aspects of public interest, it shall conduct a full assessment on whether it is compliant with the legal requirements set out (para. 260). If it concludes that the radio equipment does not comply with the requirements of the law, Traficom may order the provider to take appropriate corrective actions to make it compliant, withdraw the equipment from the market (i.e., ensure that is no longer sold) or recall it (i.e., take back) within a reasonable time (as set out by the authority).

However, even where the authority concludes that the equipment in question complies with the requirements set out by the law, it may still order a provider to take appropriate correct measures, withdraw the equipment, or recall it (para. 262)—but only where it finds that the equipment interferes with public interests.

Information Security

Under AECS paragraph 247, communications providers must ensure information security of their services, messages, traffic data, and location data when transmitting messages. The information security measures adopted should be aimed at ensuring an appropriate level of safety, taking into account the seriousness of threats, the level of technical development to defend against threats, and the cost incurred by the measures.

The law further specifies that communications providers (and providers of value-added services) may take "necessary" measures to ensure information security for the purpose of, e.g., detecting, preventing and investigating interferences that may adversely affect information security in the communication networks or services connected to them and in the information systems and making the disturbances subject to preliminary investigation (para. 272). This includes measures such as automatic analysis of messages, preventing messages from being sent/received, or automatically removing harmful computer programmes.

Amendments to the Act on Electronic Communications Services

The Finnish government has introduced new provisions to this act, which came into force as of 1 January 2021 to fully implement the EECC.

In particular, these amendments introduce a new paragraph 244a to the AECS that makes it possible to limit particular network equipment in critical parts of the communications network "if there are serious grounds for suspecting that the use of the equipment would endanger national security or

national defence." In this regard, endangering national security includes activities such as those that threaten people's lives or health or vital functions of society, and the activities of a foreign state or a company closely influenced by it, which may damage Finland's international relations, economic or other important interests, or foreign intelligence.

This regulation also gives Traficom the authority to oblige an operator to remove communications network equipment from its network. In this regard, "critical parts" are considered to be those that are used to centrally manage and control the network and the communications passing through it (i.e., the "core"). This regulation would also oblige Traficom to consult with the owner/holder of the communications network and give it an opportunity to remedy the safety deficiencies before taking a decision (unless urgency requires it to act immediately).

Further, paragraph 244b introduces a new Network Security Advisory Board to assess the implementation of national security in the communications network. This advisory board should include both representatives from the Finnish administration and representatives of key telecommunications companies. For example, this board should monitor the development of and address/make recommendations on the following:

- The development of communication networks and technologies
- The definition of critical parts of communication networks
- The promotion and protection of national security in communications networks, in particular critical parts of the network
- Measures to combat the risks affecting the security of communications networks and the realisation of national security
- Amending legislation to improve network security

Finally, under paragraph 301a, an owner/holder of a communications network is entitled to compensation (based on actual cost and financial losses) from the Finnish state for any network equipment that is ordered to be removed under the new amendments. In general, this right to compensation only applies to communications network devices that have been put into use before the act enters into force. However, where equipment has been introduced at a later stage but the removal is based on "a significant and material change in circumstances" or other reason that could not have been reasonably foreseen, compensation may still be received.

Outlook

Finland has already auctioned licenses for the 700MHz (November 2016), 3.5GHz (September 2018), and 26GHz (June 2020) bands. However, it has been emphasised that the security of 5G networks and related technology must be verified before implementation.

In addition, on 13 January 2021, the Ministry of Transport and Telecommunications published a draft Cybersecurity Development Programme for public comments. This programme would aim to guide cybersecurity developments at several levels of society, from private individuals to government entities. Specifically, the programme provides for enhanced cybersecurity education at different levels of instruction, enhanced preparedness and monitoring from governmental authorities, harmonised cybersecurity requirements in key sectors, and support to the Finnish cybersecurity industry. Accordingly, the programme would provide funding for these objectives until 2025. The public consultation is open until 3 February 2021.

SWEDEN

General Approach

Swedish legislation does not contain any general provisions that regulate, e.g., "high-risk vendors," but operates a general preapproval process. Recent amendments have, however, tightened security criteria for electronic communications on the grounds of national security. As such, all vendors that want to participate in the rollout of Sweden's 5G networks must submit to an independent security review by the Post and Telecom Authority (PTA), in cooperation with the country's Armed Forces and Security Service, which is conducted according to technical criteria and one political criterion. Fulfilling one risk criterion is sufficient for an operator or vendor to be excluded from obtaining a license or from supplying license holders. Further, by decision of 20 October 2020, the PTA has added an additional condition in its decision on conditions for 5G license holders, pursuant to which these may not use products or services from Huawei or ZTE.

Competent Authorities and Relevant Legislation

In Sweden, the PTA is responsible for regulating and monitoring electronic communications and relevant operators. As such, it is also the primary authority to deal with cybersecurity issues. The main legislation under which the PTA deals with potential national security risks is the Electronic Communications Act 2003 [Sw: Lag (2003:389) om elektronisk kommunikation]. This legislation is expected to be updated to fully transpose the EECC.

Description of Cybersecurity Measures

Electronic Communications Act 2003 (ECA03)

The Electronic Communications Act 2003 (ECA03) regulates the use of electronic communications in Sweden to ensure access to secure and efficient electronic communications. Under the ECA03, operators that want to carry out radio transmission and related activities in Sweden must first apply to the PTA for formal permission (Chapter 2, para. 1 ECA03).

Licences to Use a Radio Transmitter

Chapter 3, paragraph 6 of the ECA03 specifies that licenses to use a radio transmitter shall be granted if

- it may be assumed that the radio transmitter will be used in such a way that the risk for prohibited harmful interference does not arise;
- the radio use constitutes an efficient use of radio frequencies;
- it may be assumed that the radio use will not impede such radio communications as are particularly important having regard to the free opinion formation;
- the radio use does not utilise radio frequencies that are required to maintain a reasonable preparedness for the development of existing and new radio uses or frequencies for which the radio use has been harmonised in accordance with international agreements to which Sweden has acceded or provisions adopted in accordance with the Treaty establishing the European Union;
- it may be assumed that the radio use will not infringe on radio frequencies that are required for operations referred to in Chapter 3;
- having regard to the fact that the applicant has previously had a licence revoked or some other similar circumstance, there is no reasonable cause to assume that the radio transmitter will be used in violation of the licence conditions; and

- it can be assumed that the radio use will not cause harm to Sweden's security.

Further, Chapter 3, paragraph 11 specifies that a licence to use a radio transmitter may be combined with conditions concerning

- the frequencies to which the licence relates;
- which electronic communications services or kind of electronic communications networks or techniques the licence relates to;
- coverage and rollout within Sweden;
- the geographical area in which a mobile radio transmitter may be used;
- obligation for the application to share the frequency spectrum with another party;
- such matter as in accordance with a decision on the harmonised use of radio frequencies should be imposed as conditions when the party to be allocated a radio frequency has been nominated in accordance with international agreements or provisions adopted in accordance with the Treaty establishing the European Union;
- obligations arising in accordance with applicable international agreements as regards the use of frequencies;
- undertakings that have been made in conjunction with the grant of a licence where the number of licences within a frequency spectrum has been limited;
- technical requirements and other requirements to ensure the actual and efficient use of frequencies; and
- requirements that are important for Sweden's security.

However, such conditions may only be imposed if necessary to, e.g., avoid harmful interference, ensure efficient utilisation of frequencies, protect human life and health, and satisfy public interest in having certain electronic communications services available in Sweden.

This preapproval process (combined with the possibility of imposing certain conditions on licensees) has generally been deemed sufficient to address any potential security risks related to radio services.

On 1 January 2020, amendments[14] to the ECA03 entered into force to further ensure that national security risks are taken into account before (and after) a license is granted. In particular, the updated version of the act specifies the following:

- The PTA must take into account Sweden's national security when treating applications for permission to use radio transmitter (Chapter 3, para. 6, p. 7, as noted above).
- Permission may be conditional on requirements to ensure Sweden's security (Chapter 3, para. 11, p. 10, noted above).

[14] These amendments were presented in the Swedish government's legal proposal 2018/19:41 on Amendments to the Electronic Communications Act, the Top Domain Law and the Radio Equipment Act [Sw: Regeringens proposition 2018/19:41 Ändringar i lagen om elektronisk kommunikation, toppdomänlagen och radioutrustningslagen].

- A license/permission granted before 1 January 2020 may be transferred to another operator with the consent of the PTA if it can be presumed not to harm Sweden's security (Chapter 3, para. 23, p. 5).

- A permission may be recalled or conditions may be changed with immediate effect if the radio transmission has caused harm to, or can be assumed to cause harm to, Sweden's security (Chapter 7, para. 6, p. 4).

- The Security Police and the Swedish Armed Force should be involved in the vetting process and can appeal decisions to issue permits on grounds of national security (Chapter 7, para. 19a).

Operational Reliability

Under Chapter 5, paragraph 6, a provider of public communication networks or publicly available electronic communication services must take "appropriate technical and organizational measures" to ensure that the business meets "reasonable requirements" for operational reliability. Such measures should be suitable for creating a level of safety which, taking into account available technology and the costs of implementing the measures, is adapted to the risk of disruption and interruption.

Protection of Data

The ECA03 further specifies that providers of public electronic communications services should take "appropriate technical and organizational measures" to ensure the protection of data processed in connection with the provision of the service, as well as "necessary measures" to maintain such protection in the network (Chapter 6, para. 3). Any measures adopted should be aimed at ensuring that the level of safety which, taking into account available technology and the costs of implementing the measures, is adapted to the risk of privacy incidents. If there is an incident, the provider shall without undue delay notify the PTA.

Other Relevant Regulations

Since the PTA needs to carry out its national security risk assessment together with the Swedish Security Service and the Swedish Armed Forces, amendments were also introduced to the Public Privacy Act to enable the exchange of information between these public bodies.

In addition, the Swedish Security Service's position on the consultation with the PTA prior to granting frequency licenses outlines 16 technical criteria which should be taken into account in the risk assessment of frequency license applicants:[15]

1. The operator must show that central functions[16] are operating and accessible within Sweden in the event of a supplier or product disruption. Therefore, it must also have a plan to handle, in Sweden, security incidents or disruptions, and system or user data must be stored in Sweden.

2. The operator must be able to easily and quickly disconnect connection points to foreign countries without affecting the network. Accordingly, it must have a plan to ensure the network's functionality in case of a security incident from abroad and demonstrate how foreign influence is prevented.

---

15 In addition to criteria previously published in the "General invitation to apply für permission to use radio transmitters in the 3.5 GHz and 2.3 GHz bands."

16 Central functions are defined broadly as all "functions in the radio access network, the transmission network, the core network and the service and maintenance network that are necessary to maintain network functionality and electronic communication services provided by the license holder."

3. The operator must provide specifications regarding the functions required to ensure high accessibility and secrecy of the network as well as demonstrate the safeguards in place to protect these functions.

4. The operator must have appropriate processes in place to track and identify network traffic and minimise the risk that components may be used for tracking and manipulation. It must also report on the transparency and control it has over its suppliers.

5. The operator must have measures in place to protect central functions against unauthorised manipulations.

6. Central functions of the network must be located in Sweden and may not be accessed from abroad.

7. The network must be designed to prevent unauthorised tracking of services, capacity, location, or users.

8. The network must be designed to prevent unauthorised attacks (such as cyberattacks) and, where possible, detect and prevent them.

9. The operator must set up appropriate authorisation procedures to access the control system of central functions.

10. The operator must have appropriate procedures in relations to login, log assessment, and security review for the equipment connected to central functions.

11. Equipment, staff, and services for central functions of the network must be located in Sweden. Security incidents must be handled in Sweden and user data must be stored in Sweden.

12. The operator must continuously provide information to the designated recipients at the sectoral authority regarding actions taken in communication networks which may affect secrecy, strength, accessibility, insight, or control.

13. The operator must provide information in due time such that the sectoral authority can determine what risks are involved with the measures taken in the communication networks and whether measures need to be taken.

14. The operator must actively facilitate the sectoral authority's insight and control of the sector by establishing reporting and information procedures.

15. The operator must develop, implement, operate, and maintain adequate security measures. It must inform the relevant authority accordingly and refer to each of the above-mentioned principles.

16. The operator must ensure that personnel who have access to data that may impact confidentiality, accuracy, strength, and accessibility are approved, and are trained in security protection and aware of the secrecy of the information.

A final political criterion seeks to assess the likelihood of the operator or supplier being exposed to influence/pressure. Such influence/pressure may be applied by, but is not limited to, the presence of the following factors:

- The likelihood of the operator or supplier being exposed to influence/pressure. Such influence/pressure may be applied by, but is not limited to, the presence of the following factors:

- Connections, including ownership interests, but also other links to government or authorities in third countries (non-EU countries)
- Third country legislation, especially in cases where legal or democratic principles are lacking or where no security or data protection agreements can be applied
- Links to countries or organisations engaged in offensive cyberoperations or other antagonistic activities against Sweden
- Other opportunities for third countries to exert pressure, including in relation to the geographical location of production assets

Draft Electronic Communications Act 2020 (ECA20)

In September 2019, the Swedish government announced its plan to replace the ECA03 with a new Electronic Communications Act 2020 (ECA20). The purpose of the proposal is to further harmonise Swedish legislation with EU legislation by implementation of the EECC.[17] As such, it is not intended to introduce any radical changes to the legislative framework, but rather to take into account the development of the market and introduce a more appropriate structure of the law.

The proposal to update the legislation was published before the January 2020 amendments to the ECA03 entered into force, and a formal legislative proposal (following completion of the relevant steps in the legislation process, including formal inquiry and consultation processes) has yet to be tabled. However, under the currently proposed wording, a general requirement to factor in Sweden's security whenever applying the new law is introduced (Chapter 1, para. 1) to account for the rapid development of technology and the increase in information sharing through electronic communications. Depending on the feedback received during the consultation stages, this wording may be amended or clarifications added to the final legislative proposal once introduced.

At the time of this writing, it is still uncertain when the government will present its formal legislative proposal regarding the ECA20. In addition, the ECA20 was set to enter into force on 21 December 2020 according to the EU's transposition schedule but, so far, has not and its status remains unclear.

Risk Assessment

In April 2020, the PTA issued updated guidance on operational security (PTA Guidance) pursuant to which providers of electronic communications services should undertake operational safety work, which must be conducted in the long term, continuously, and systematically. This includes analysing potential risks of disruption or interruption in the network or to its services at least once a year, and taking appropriate measures to protect against such disruption/interruption. In particular, this assessment should take into account the following:

- Intrusion and other external interference (both physical and logical)
- Weather-related threats
- Planned changes and updates to the network and services

In addition, Swedish operators are required to conduct full risk assessments (including both the risks mentioned above and an analysis of the threat of network sabotage) before procuring new products and services (para. 5) to address risks raised during the country's planned 5G rollout.[18] These rules are aligned with measures recommended by the EU and also introduce stricter documentation requirements

---

[17] *See* memorandum [Sw: Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation].

[18] *See* regulation on changes to the PTA's regulation on operational security [Sw: Föreskrifter om ändring i Post-och telestyrelsens föreskrifter (PTSFS 2015:2) om krav på driftsäkerhet].

on operators. In particular, they require operators to save any procurement-related documents for five years and to respond to information requests from the PTA regarding potential threats to the national network.

Most recently, as mentioned above, on 20 October 2020, based on the ECA03 procedure, the PTA, after having selected eligible bidders (Hi3G Access, Net4 Mobility, Telia Sverige, and Teracom), adopted additional 5G licence auction conditions which impose a strict ban on the use of equipment from Huawei and ZTE by future licence holders. This decision was based on the grounds that they allegedly pose a threat to Sweden's national security. In practice, new installations and new implementation of central functions for the radio use in the frequency bands must not be carried out with products from these two suppliers; and if existing infrastructure for central functions is to be used to provide services in the concerned frequency bands, products from Huawei and ZTE already in use must be phased out by 1 January 2025 at the latest.

Outlook

An interim court injunction initially prohibited the launch of the 5G auction subject to the additional licence conditions in November 2020 but the auction was authorised to go ahead by a court decision upon appeal. The auctions took place on 19 January 2021. The court case is still pending on the merits.

Finally, as part of its recent legislative developments, Sweden is currently also working on establishing a National Cyber Security Centre to strengthen information security and Sweden's resilience against cyberattacks. Consequently, the Swedish government requested the National Defence Radio Establishment (FRA), the Swedish Armed Forces, the Swedish Civil Contingencies Agency (MSB), and the Security Police to prepare for the creation of a National Cyber Security Centre. On 10 December 2020, the government officially commissioned the aforementioned agencies to establish this center and assigned funding for its setup and operation until 2025. This center's activities will be developed gradually between 2021 and 2023.

ROMANIA

General Approach

Romania is the first EU member state which signed a 5G memorandum of understanding (MoU) with the US government in 2019 in order to exclude certain suppliers from its telecommunications networks. Transposing the wording of this MoU, the Romanian government has submitted draft legislation that submits all 5G suppliers to a prior authorisation procedure, allowing for the exclusion of certain suppliers based on political criteria, with retroactive effect.

Competent Authorities and Relevant Legislation

According to the MoU between Romania and the United States, both governments commit to a risk assessment of 5G vendors. This risk assessment should include an evaluation of (1) whether the vendor is subject, without independent judicial review, to control by a foreign government; (2) whether the vendor has a transparent ownership structure; and (3) whether the vendor has a history of ethical corporate behaviour and is subject to a legal regime that enforces transparent corporate practices.

The Draft Law on the adoption of measures relating to the information and communication structures of national interest and the conditions for the implementation of 5G networks implements this by introducing a prior authorisation requirement for manufacturers of technology, software, or equipment for telecommunications "infrastructures of national interest as well as 5G networks."[19] This also covers existing 3G and 4G infrastructure.[20]

The Romanian prime minister is the competent authority to decide on the authorisation of 5G equipment, software, or technology, upon a prior vote of the Supreme Council of National Defense (CSAT). The Romanian telecommunications regulatory authority, ANCOM, is to interact with network operators and telecommunications operators to supervise and enforce the prohibition.

Description of Cybersecurity Measures

Under the Draft Law, approval would be granted only to manufacturers that

- are not controlled by a foreign government, in the absence of an independent legal system;
- have a transparent shareholding structure;
- have no history of unethical corporate conduct; and
- are subject to a legal system that requires transparent corporate practices.[21]

The objective of the approval mechanism is to eliminate what is broadly identified in the proposal as "risks to national security and/or national defense,"[22] which is open to interpretation.

The prime minister is to decide on applications by manufacturers for authorisation, further to an assent of the CSAT, "based on assessments from the perspective of risks, threats and vulnerabilities to national

19 Article 3 of the Draft Law.

20 Article 2(e) of the Draft Law.

21 Article 3(1) of the Draft Law.

22 Articles 1 and 5 of the Draft Law.

security and/or national defense."[23] The authorisation can be withdrawn at any time "if there are risks, threats and vulnerabilities to national security and/or national defense."[24]

Network operators and telecommunications services providers will not be allowed to use technology, software, or equipment from manufacturers that are not authorised pursuant to the Draft Law, and technology, software, or equipment from such manufacturers currently in use may only be used for another five years. The Romanian telecommunications regulator, ANCOM, will request from network operators and telecommunications service providers detailed information about the technology, equipment, and software in use in their networks, as well as the degree of outsourcing to third parties of certain activities related to the management of the telecommunications networks.[25]

All equipment from these suppliers will be prohibited for sale on the Romanian market, and network operators and telecommunications service providers may not use such equipment. Upon receiving any report of the use of nonauthorised equipment, ANCOM is to order the immediate prohibition of such equipment.[26] Any violation of the prohibition will be a criminal offence.

Finally, it is proposed that equipment installed prior to the introduction of the Draft Law will be prohibited retroactively and must be removed within a transition period of five years.

Outlook

The Draft Law was not put before Parliament before the 6 December 2020 general election and the legislative timetable remains to be seen. 5G auctions are expected to take place in the second quarter of 2021, once the selection procedure for granting radio-spectrum rights in the 700 MHz, 800 MHz, 1500 MHz, 2600 MHz, and 3400-3800 MHz frequency bands for the provision of 5G services is finalised. This will involve establishing conditions for granting right of use and drafting rules for carrying out the selection procedure. Once the process is established, the actual selection procedure will be carried out in the second quarter of 2021.

[23] Article 5 of the Draft Law.

[24] Article 7 of the Draft Law.

[25] Article 12 of the Draft Law.

[26] Article 14(5) of the Draft Law.

POLAND

General Approach

Poland is one of a number of European member states that signed an MoU with the US government in 2019 in order to exclude certain suppliers from its telecommunications networks. Transposing the wording of this MoU, the Polish government has submitted draft legislation which submits all 5G suppliers to a prior authorisation procedure, allowing for the exclusion of certain suppliers based on political criteria, with retroactive effect.

Competent Authorities and Relevant Legislation

According to the MoU signed between Poland and the United States in September 2019, both governments commit to a risk assessment of 5G vendors. This risk assessment should include an evaluation of (1) whether the vendor is subject, without independent judicial review, to control by a foreign government; (2) whether the vendor has a transparent ownership structure; and (3) whether the vendor has a history of ethical corporate behaviour and is subject to a legal regime that enforces transparent corporate practices.

In order to implement this MoU, the Polish government has proposed a Draft Amendment to the Polish National Cybersecurity System Act (the Draft Amendment). The Polish Draft Amendment aims at introducing a risk assessment for suppliers of "equipment or software essential for cybersecurity" to entities of the so-called Polish national cybersecurity system, which according to the Draft Amendment shall be been extended to include, among other things,[27] telecommunications network operators and services providers.[28]

Following a public consultation on the Draft Amendment, where a number of stakeholders voiced their concerns on the implications of such measures, the Polish government published a new version of the draft on 21 January 2021.

Description of Cybersecurity Measures

The Draft Amendment is an amendment of the Polish National Cybersecurity System Act (the Cybersecurity System Act), which entered into force on 28 August 2018. Transposing the NIS Directive,[29] the Cybersecurity System Act defined a set of security obligations for a group of entities critical to cybersecurity, consisting of national and local government institutions as well as the biggest undertakings active in key economy sectors.

The initial version of the Draft Amendment provided for a risk assessment of equipment suppliers by the Cybersecurity Matter Board culminating in a ranking of these suppliers in different risk categories (from no risk to high risk). This ranking was coupled with a prohibition to use equipment from suppliers classified as "high risk."

In the latest version, the Draft Amendment instead introduces a procedure for the classification of high-risk vendors of hardware or software-specific security and defense-related entities but also including all sizeable telecommunications undertakings.

---

[27] The Draft Amendment encompasses "electronic communications providers," which arguably goes beyond network operators and private telecommunications providers.

[28] In parallel, the Polish government proposes a new Electronic Communications Law (Draft PKE). The Draft PKE is to include a Chapter 5 governing the security of networks and services and obligations for the security of the state. This chapter is set to introduce specific obligations for telecommunications undertakings to apply measures ensuring the security of networks or services.

[29] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, [2016] OJ L 194/1.

Decision of the Ministry

The classification as "high-risk supplier" is initiated by the Minister for Digitisation *ex officio* or at the initiative of the chairman of the Cybersecurity Matter Board.[30] It is subject to the general rules of administrative procedure.[31] However, in this specific instance, the appeal is not suspensory, the court hearing is *in camera*, and the reasoning of the classification decision can be redacted with regard to the undertaking concerned on grounds of national security.

The Minister for Digitisation is required to consult with the Cybersecurity Matter Board for its opinion on the classification. The Board then has three months to deliver its opinion based on the following criteria:

- An analysis of threats to national security of an economic nature, counterintelligence and terrorism, and threats to the fulfilment of obligations of the allied and the European obligations, represented by the hardware and software supplier.
- The likelihood that the hardware or software vendor is under influence of a country outside the EU or NATO, taking into account the following:
    - The degree and type of relationship between the hardware or software supplier and this country.
    - Legislation on the protection of personal data, especially where there are no data protection agreements between the EU and the country concerned.
    - Ownership structure of the hardware or software supplier.
    - The capacity for interference by that state with the freedom of economic activity of hardware or software vendors.
- The number and types, as well as the method and time of eliminating, the detected vulnerabilities and incidents by the supplier.
- The degree to which the hardware or software supplier exercises supervision over the process of manufacturing and delivering hardware or software, and the risks to the hardware or software manufacturing and delivery process.
- The content of previously issued recommendations under the Cybersecurity System Act concerning vendor hardware or software.

Once its assessment is finalised, the Board submits its opinion to the Minister who then takes its decision to classify the supplier as "high risk" if said supplier presents a "serious threat to national security."[32] Suppliers classified as "high risk" are prevented from providing their equipment as specified in the Minister's decision. In addition, the equipment described in the decision that is already in use must be removed within five years of said decision for equipment used in what the Draft PKE lists in Annex 3 as "functions critical for the security" of the network[33] or seven years for equipment in other functions.

[30] New Article 66a(1) of the Cybersecurity System Act.

[31] New Article 66a(3) of the Cybersecurity System Act.

[32] New Article 66a(8) of the Cybersecurity System Act.

[33] New Article 66b(2) of the Cybersecurity System Act.

Warning of the Plenipotentiary

The Draft PKE also empowers the Government Plenipotentiary for Cybersecurity Matters to issue warnings to inform institutions and private stakeholders of cyberthreats coupled with recommendations to remedy the situation and reduce the risk of a critical incident.

In the event a critical incident cannot be avoided, the Minister for Information Services can issue a Security Order in the form of an administrative decision. This order will include the specific behavior that the concerned entities must adopt to mitigate the incident. Specifically, the order can include the following:[34]

- An assessment of the risk associated with using a specific equipment and the corrective measures associated to the identified risks.
- A review of the continuity and recovery plans related to the relevant vulnerability.
- Instructions to apply security measures to software or hardware equipment with a specified vulnerability.
- Instructions to implement a specific configuration for relevant software or hardware.
- Instructions relating to increased monitoring.
- Prohibition to use certain hardware or software.
- Prohibition to connect to certain URLs and IP addresses.
- Suspension or prohibition to install a certain version of a software.
- Instructions to secure certain information.
- Creating snapshots of infected devices.

In case of violation of the prohibition of hardware and software of high-risk vendors, entities of the cybersecurity system in Poland are subject to fines up to 3% of their worldwide turnover of the previous financial year.

Outlook

This second iteration of the Draft PKE has not been submitted to the public consultation process at this point and the legislative timetables remain unclear. 5G spectrum auctions in Poland were suspended in May 2020 and are expected to resume for some frequencies by August 2021 (for 3.6GHz bands) [TBC], July 2022 (for 700MHz bands), and December 2022 (for 2.6GHz bands).

[34] New Article 67b (9) of the Cybersecurity System Act.

SLOVENIA

General Approach

Slovenia is one of a number of European member states which signed an MoU with the US government in 2020 in order to exclude certain suppliers from its telecommunications networks. Transposing the wording of this MoU, the Slovenian government has submitted draft legislation that submits non-EU suppliers or third-level service providers to a prior authorisation procedure. This procedure would also apply to existing infrastructures and contracts.

Competent Authorities and Relevant Legislation

The Agency for Communications Networks and Services (Akos) is the regulatory authority in charge of telecommunications networks in Slovenia. It is unclear, however, which authority within the "Slovenian government" would be in charge of authorising a non-EU supplier or service provider according to the new Draft law.

Description of Cybersecurity Measures

On 28 August 2020, the Ministry of Public Administration published a Draft Law which reorganises existing provisions of the previous Act on Electronic Communications and essentially transposes the European Electronic Communications Code[35] into Slovenian law. In addition, Article 112 of the Draft Law introduces the obligation for "mobile network operators" to carry out a risk assessment of their suppliers of information systems and network equipment ("suppliers") as well as their third-level "service providers."

Third-level support services are defined in the Draft Law as "services related to the operation, maintenance, upgrade, configuration, and management of a virtualized or physical network and services."[36]

This risk assessment shall include "risks related to the ownership . . . of the supplier or service provider of third-level services, from a business continuity perspective, while taking into account any potential national security restrictions and policies of the government, which shall be set by the government in a resolution" (Article 112(2) of the Draft Law). So far, no government resolution setting out national security restrictions and government policies has been enacted.

Article 112(2) of the Draft Law further introduces a prior authorisation requirement for any supplier or service provider "having its seat outside the Member States of the European Union." Before selecting such equipment or services, the mobile network operator must "obtain the prior consent of the government." At this point, it seems unclear from which governmental entity consent is to be obtained, or on what grounds such consent is granted, or according to which procedure and whether and how recourse is possible against such a decision by the government.

Article 294(1) No. 17 of the Draft Law subjects medium-size and large mobile telecommunication operators to a fine of between 50,000€ and 400,000€ in case of a violation of Article 112(2) of the Draft Law.

The risk assessment obligation extends to existing suppliers or service providers. Article 305(1) of the Draft Law stipulates that mobile telecommunication network operators carry out a risk assessment of their existing suppliers and service providers within six months of entry into force of the Draft Law.

---

35 Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code (Recast).

36 Article 3, No. 77 of the Draft Law.

Mobile network operators may, however, continue to use existing network equipment and information systems until the end of their lifetime, but for no longer than five years after the entry into force of the Draft Law (Article 305(2)). They may also continue to retain their existing service providers for a period of up to five years after the entry into force of the Draft Law (Article 305(3)).

Yet, no such transition period seems available in the case of "key parts of the national security system" which "support the critical infrastructure, to essential service providers and state administration bodies" as soon as the risk assessment is completed (Article 305(4) of the Draft Law).

Outlook

The status of the Draft Law is currently unclear, although Akos had aimed for an adoption in early 2021.

On 17 December 2020, Akos published the schedule and tender procedure for the 5G frequencies auction process. The deadline to bid is set for 1 February 2021 and the authority currently expects the auction to be completed by spring 2021.

AUSTRIA

General Approach

The current Austrian legislation focuses on technical criteria and the security features of 5G equipment. There is an obligation to report 5G equipment for critical functions to the Austrian Telecommunications Regulatory Authority. However, a recent legislative proposal is aiming to tighten security criteria for electronic communications on the grounds of national security. Under this new legislation, a supplier or manufacturer can be deemed "high risk" to national security and subsequently be prohibited from providing network equipment in Austria for mobile communication networks.

Competent Authorities and Relevant Legislation

The legislation currently in place[37] does not include substantive cybersecurity measures other than what is included in the EU NIS directive.[38]

Under the new legislative proposal, while the Ministry of Agriculture, Regions and Tourism is the entity that will ultimately qualify a supplier as "high risk" and issue an administrative decision, a newly appointed Expert Council will also provide an opinion on the matter to assist the Ministry in the decisionmaking process.

Description of Cybersecurity Measures

Telecommunication Network Security Ordinance

The Austrian Telecommunications Regulatory Authority (RTR) published in the first quarter of 2020, along with the Ministry of Agriculture, Regions and Tourism and the Ministry of Interior, a regulation on obligations for communication network operators and electronic communication services providers regarding minimum security measures, taking into account 5G networks, and with information requirements in the event of security incidents (Network Security Regulation 2020). This regulation draws mostly from the EU Toolbox and provides for (1) reporting obligations for network operators and service providers in the event of significant security incidents; (2) specific requirements for minimum security measures; and (3) special security requirements for 5G networks.

It also introduced a mandatory notification system, further to which network operators have to notify twice a year all functions and suppliers of "security relevant" (and possibly other) components used for the network operation. Furthermore, operators must pursue a "multi-vendor strategy" to avoid depending on one provider as well as ensure network security.

Draft Telecommunications Act 2020

The Draft Telecommunications Act 2020 is an amendment of the previous Telecommunications Act 2003 and seeks to consolidate various applicable texts and implements a number of EU texts, including the EECC and the NIS Directive. However, the text also goes beyond these obligations and introduces the possibility for the Ministry of Agriculture, Regions and Tourism to qualify manufacturers of electronic network components as so-called "high-risk suppliers" of network components for communication networks on grounds of "national security" (Section 44a, paragraph 1 of the Draft Telecommunications Act).

Pursuant to Section 44a, paragraph 2 of the Draft Telecommunications Act, suppliers are qualified as "high risk" if it has to be considered as "highly likely that they will not be in a position to comply or permanently comply with European Union rules applicable to them, in particular with regard to

---

37 Telecommunications Act 2003; Network and Information System Security Act (NISG).

38 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the EU.

information security and data protection." In order to evaluate whether this is the case, the following criteria are to be taken into consideration, according to the current draft:

- Lack of quality or cybersecurity practices of the manufacturers; in particular, lack of sufficient control over the supply chain and insufficient compliance with relevant state-of-the-art security practices, including regard to information security protection objectives (confidentiality, availability and integrity)
- High likelihood of influence of a third country government on the supplier
- Possibility of influence on the supplier by legislative acts of a third country if the supplier has its seat in this country
- Absence of security or data protection agreements between the EU and the country of residence of the supplier, to the extent this is a third country
- The ability of a third country to exert pressure on the manufacturer; in particular, regarding the location of the production facilities
- Specific characteristics of the manufacturer's ownership structure which render influence of a third country possible
- Insufficient capacity of the manufacturer to guarantee security of supply

The Minister for Agriculture, Regions and Tourism can take various types of decisions, limited to a maximum duration of two years (Section 44a, paragraph 5):

- Decide that the classification be limited to certain security-relevant business areas, products, services, or individual hardware or software components and possibly for a certain period of time or a certain geographic area
- Exclude a manufacturer from the supply of all or individual security-relevant components for communication networks or for communication network parts
- Exclude certain service providers from the provision of all or certain services for communications networks

The Minister's decision is rendered after having consulted with the newly created Expert Council at RTR, which will deliver an expert opinion in the procedure for the classification of high-risk manufacturers. Importantly, this opinion also takes into account the "compliance with general standards of the rule of law in the third countries under assessment."

The Draft Telecommunications Act 2020 thus introduces a procedure by which a supplier or manufacturer can be classified as "high risk" and excluded from electronic communication networks. As it currently stands, this exclusion seems to potentially cover all network generations and all parts of the network. It also seems to extend to hardware already in use. Finally, there is no specific timeline for taking a decision and no transition period is foreseen in the current draft.

Outlook

Austria appears to be slightly ahead of the curve with respect to the 5G rollout as its 5G auctions took place in 2019 and early 2020 and the rollout is already ongoing. In the meantime, the regulatory authority conducts frequent cybersecurity assessments (the last one being in 2020) to identify new risks and corrective measures in order to maintain a high level of protection. The Draft Telecommunications Act 2020 is currently subject to public consultation until 10 February 2021.

Contacts

If you have any questions or would like more information on the issues discussed in this White Paper, please contact any of the following Morgan Lewis lawyers:

Brussels
Christina Renner +32.2.507.7524 christina.renner@morganlewis.com

Washington, DC
Andrew D. Lipman +1.202.739.6033 andrew.lipman@morganlewis.com

About Us

Morgan Lewis is recognized for exceptional client service, legal innovation, and commitment to its communities. Our global depth reaches across North America, Asia, Europe, and the Middle East with the collaboration of more than 2,200 lawyers and specialists who provide elite legal services across industry sectors for multinational corporations to startups around the world. For more information about us, please visit www.morganlewis.com.