Morgan Lewis | White Paper

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

September 2020

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, however, 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 coronavirus (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**	**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*	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 component)	Review by network operator and selection on the basis of, inter alia, declaration of trustworthiness and certification of critical component Review by national telecoms regulator	Decision of network operator further to guidance issued by the national telecoms regulator, BSI, and the Ministry of the Interior	Focus on critical security component Risk-based assessment Case-by-case approach
Sweden	Telecoms operators with regard to equipment/software in use	Technical (critical components)	Telecoms operators to conduct first risk assessment, to be submitted to national telecoms regulator, security police, and armed forces for final decision	Administrative decision subject to appeal Appeal court may decide that a decision should be suspended pending court decision	Risk-based assessment Case-by-case approach

	DIFFERENCES			SIMILARITIES	
	Subject to Review (Operators, Suppliers, Products?)	**Review Criteria (Strategic, Political or Technical)**	**Review Decisionmaking Mechanism**	**Legal Force of Review Decision**	**Security Review with Regard to Product or Service**
Finland	Suppliers Telecoms operators with regard to equipment/software in use	Technical (legal proposal on limitations in core network pending) Critical component	National Telecoms Regulator	Administrative decision subject to appeal Appeal has suspensory effect	
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 behaviour – is subject of a legal regime that enforces transparent corporate practices	Prime Minister upon decision of CSAT	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**	**Legal Force of Review Decision**	**Security Review with Regard to Product or Service**
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 civil and human rights in the supplier's home 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	National Cybersecurity Board Plenipotentiary	Administrative decision with immediate effect subject to non-suspensory appeal first before National Cybersecurity Board and subsequent appeal to administrative court with suspensory effect 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

** The security assessment is a competence for Member State Authorities.*
*** 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.

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

The EU Toolbox identifies measures that fall into two categories: strategic and technical.

EU Toolbox: Strategic Measures

The strategic measures identified include the following:

- 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:

- 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

[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."

    - 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

EU Toolbox: Technical Measures

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
- 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

In addition, 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 will replace the current framework as of 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.

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.

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.

[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.

[7] [2018] OJ L 321/36.

GERMANY

GENERAL APPROACH

The German legislation, the Telecommunications Act ("**Telekommunikationsgesetz**" – **TKG**), 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 only available in draft form: in a draft new Security Catalogue for telecommunications networks and a draft Bill on IT Security. The law stipulates that a precaution or 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).

COMPETENT AUTHORITIES AND RELEVANT LEGISLATION

The main law regulating German telecommunications networks is the TKG. TKG Section 109 defines certain protection objectives and obligations. It 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 the protection objectives, all companies must take technical precautions and other measures.

DESCRIPTION OF CYBERSECURITY MEASURES

Operators of public telecommunications networks and providers of publicly accessible telecommunications services must present the technical and organisational protective measures they have taken in a security concept to the National Network Agency (which is the national telecommunications regulatory authority), as per Section 109(4) of the TKG. Compliance with these security requirements is mandatory for all companies.

According to Section 109(7) of the TKG, 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. The purpose of such a review is to determine whether the requirements of Section 109(1)–(3) of the TKG have been met. The catalogue for security requirements can thus also form the basis for the security audit of a qualified independent body in accordance with Section 109(7) of the TKG.

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," which was drawn up by the Federal Network Agency in agreement with the Federal Office for Information Security (BSI) and the Federal Commissioner for Data Protection and Freedom of Information.

Criticality of the Network

The security concept needs to take account of the criticality of the network, to the extent that it has to provide an analysis of the hazards expected (TKG Section 109(4)). The assessment of criticality takes

account of the *common good interests* protected by Sections 109(1) and (2) of the TKG: *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.[8]
- **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 BSI IT-Grundschutz Compendium offers assistance in selecting specific measures.

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

[8] 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).

- Monitoring of security-related events, emergency exercises, and testing procedures of network and IT systems[9]

Specific Measures Under the TKG

Specific measures apply to networks and services with increased criticality.[10]

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 BNetzA and 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 BNetzA 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.

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.[11] 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 *non-exhaustive list* of the content of a declaration of the trustworthiness of a supply source is provided in Annex 2 of the Security Catalogue:

---

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

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

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

- 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 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

Still under discussion is the so-called review of the IT Security Act 2.0. Under the current IT Security Act (BSIG), operators of critical infrastructures (KRITIS) must establish and demonstrate a minimum standard of IT security, report IT security incidents, and cooperate with the BSI. Relevant for the purpose of this report are the obligations related to "critical components," i.e., software and hardware products that are used by KRITIS and "whose lack of availability, authenticity, or confidentiality could lead to an outage or to disruptions of the proper functioning of the KRITIS" (BSIG § 9b).

Critical components that are subject to a mandatory certification under the TKG may only be used by KRITIS if the software/hardware manufacturer concerned has provided a "declaration of trustworthiness" to the KRITIS operator, which must also cover the entire supply chain of the manufacturer (Draft BSIG § 9b).

The Ministry of the Interior is yet to define the minimal requirements for the declaration of trustworthiness (Draft BSIG § 9b(2)) and can prohibit the use of such components if it considers that the manufacturer of the component is not trustworthy, including retroactively, provided a sufficiently long time period is granted.

According to the Draft BSIG, a manufacturer is *not* considered to be *trustworthy* if

- it does not comply with the obligations entered into in the trustworthiness declaration;
- it does not cooperate with security audits;
- it does not notify security breaches or weaknesses; and
- the component does have characteristics that impact the integrity, availability, or functioning of the critical infrastructure, unless the manufacturer demonstrates it has not yet implemented this technical feature and has duly eliminated this.

OUTLOOK

The Draft IT Security Catalogue is currently under review by the Commission and member states under the TRIS procedure and will enter the legislative process thereafter. The Bill on IT Security is not expected to be introduced in Parliament before autumn this year and will be subject to debate, in particular on the minimum content of the trustworthiness declaration to be defined by the Ministry of the Interior.

SWEDEN

GENERAL APPROACH

The 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 Sweden's 5G networks must submit to an independent security review by the Post and Telecom Authority (PTS), in cooperation with the country's Armed Forces and Security Services.

COMPETENT AUTHORITIES AND RELEVANT LEGISLATION

In Sweden, PTS 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 PTS deals with potential national security risks is the Electronic Communications Act 2003 [Sw: Lag (2003:389) om elektronisk kommunikation].

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 act, operators that want to carry out radio transmission and related activities in Sweden must first apply to the PTS for formal permission (Chapter 2, para. 1 ECA03).

Licences to Use a Radio Transmitter

Chapter 3, paragraph 6 of the act 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.

However, on 1 January 2020, amendments[12] 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 PTS 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).
- A license/permission granted before 1 January 2020 may be transferred to another operator with the consent of the PTS 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).

[12] 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].

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

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 PTS.

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.[13] 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 writing, it is still uncertain when the government will present its formal legislative proposal regarding ECA20. However, ECA20 is currently set to enter into force on 21 December 2020.

Risk Assessment

In 2015, the PTS issued guidance on operational security (PTS Guidance) [Sw: Post-och telestyrelsens föreskrifter om krav på driftsäkerhet]. Under the PTS Guidance, 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:

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

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

In March 2020, the PTS Guidance was updated and new rules also came into effect which required Swedish operators 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.[14] These rules are aligned with measures recommended by the EU and also introduce stricter documentation requirements on operators. In particular, they require operators to save any procurement-related documents for five years and to respond to information requests from the PTS regarding potential threats to the national network.

OUTLOOK

Following the January 2020 update of the ECA03, the PTS has to consider the potential security threat posed by participants in the upcoming 5G auctions together with the Security Police and Armed Forces. The deadline to apply to participate in the auctions of the 3.5 GHz and 2.3 GHz bands expired on 30 June 2020. The PTS received applications for both bands and together with the Security Police and Armed Forces is currently assessing these applications. The PTS is expected to announce which bidders have been approved to participate in the auction on 20 October 2020. Thereafter, the auctions are planned to start on 10 November 2020.

Further, the Swedish government has commissioned a number of ongoing inquiries to consider how to best implement the EU Cybersecurity Act in Sweden by the June 2021 deadline.

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 by the end of 2020.

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

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],[15] 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's 5G toolkit 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;
- it 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;

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

- 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);
- 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 programs.

Draft New Act on Electronic Communications Services

The Finnish government has proposed to introduce new provisions to this act to implement the EECC.

In particular, the proposed regulation introduces a new paragraph 244a to the AECS that would make 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 would also give 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, the proposed 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 realization of national security
- Amending legislation to improve network security

Finally, under paragraph 301a, an owner/holder of a communications network should be 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 paragraph 244a. 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.

OTHER

In November 2019, Traficom launched a cybersecurity level, which guarantees to customers that a labelled device complies with basic information security requirements, thus making Finland the first country to introduce such an information security certificate. The purpose of the label is to raise awareness among Finnish consumers of information security on how to safely use connected devices.

So far, only a limited number of products have received the certificate, including the Cozify Hub and the Polar Ignited sports watch.

OUTLOOK

The draft amendments to the AECS are expected to enter into force on 21 December 2020.

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.

ROMANIA

GENERAL APPROACH

Romania is one of a number of European member states which has signed a memorandum of understanding (MoU) with the US government 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."[16] This also covers existing 3G and 4G infrastructure.[17]

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.[18]

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,"[19] 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

[16] Article 3 of the Draft Law.

[17] Article 2(e) of the Draft Law.

[18] Article 3(1) of the Draft Law.

[19] Articles 1 and 5 of the Draft Law.

security and/or national defense."[20] The authorisation can be withdrawn at any time "if there are risks, threats and vulnerabilities to national security and/or national defense."[21]

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.[22]

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.[23] 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 is currently subject to consultation. The political process is likely to be accelerated in light of a heated debate on the law and the upcoming elections in the United States.

[20] Article 5 of the Draft Law.

[21] Article 7 of the Draft Law.

[22] Article 12 of the Draft Law.

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

POLAND

GENERAL APPROACH

Poland is one of a number of European member states that has signed an MoU with the US government 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.

RELEVANT LEGISLATION AND COMPETENT AUTHORITIES

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,[24] telecommunications network operators and services providers.[25]

The competent authority to carry out the risk assessment is an advisory board on cybersecurity matters of the Council of Ministers,[26] the Cybersecurity Matter Board. Suppliers will be classified into risk categories ranging from "no risk" to "high risk." The risk classification of vendors will be published in the Official Journal of the Republic of Poland.

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,[27] 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 Draft Amendment extends this group to include all electronic communication services providers and network operators.[28] The Draft Amendment further proposes a risk assessment of suppliers of equipment

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

[25] In parallel, the Polish government proposes a new Electronic Communications Law (Draft PKE). The 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.

[26] New Article 64, New Article Art. 65 No. 7 of the Cybersecurity System Act.

[27] 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.

[28] New Article 1(4) of the Cybersecurity System Act.

and software to entities of the cybersecurity network, which would be carried out by the Cybersecurity Matter Board[29] at the request of one of the members of the Board.

In particular, the risk assessment would include 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 European Union or NATO, taking into account the following:
    - The degree and type of relationship between the hardware or software supplier and this country.
    - Its legislation on the protection of civil rights and human rights.
    - 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 hardware or software vendors.
- The number and types, as well as the method and time of eliminating, the detected vulnerabilities and incidents.
- 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.

On the basis of these criteria, suppliers are then classified as "low risk," "medium risk," or "high risk" vendors.[30] Vendors are defined as one of the following:

- **High risk** if the hardware or software supplier is a serious threat to state cybersecurity and reducing the level of its risk by implementing technical or organisational measures is not possible.
- **Moderate risk** if the hardware or software vendor provides a serious threat to state cybersecurity and the reduction of the level of this risk is possible by implementing technical or organisational measures.
- **Low risk** if the hardware or software vendor is a low threat to state cybersecurity.
- **No risk** level if no risk has been identified for state cybersecurity or its level is negligible.

The classification of vendors will be published in the Official Journal of the Republic of Poland.[31]

Low- to medium-risk vendors can propose remedial measures and a recovery plan. In case of acceptance these remedial measures and recovery plan, the Board may revise the assessment.[32] The equipment and

[29] New Article 64, New Article Art. 65 No. 7 of the Cybersecurity System Act.

[30] New Article 66a(4) No. 5 of the Cybersecurity System Act.

[31] New Article 66a(4) No. 6 of the Cybersecurity System Act.

software of such supplier may not be used, but hardware and software already installed may continue to be used.[33]

Equipment and software of high-risk vendors, on the other hand, may not be used by entities of the national cybersecurity system, and any hardware, software, or services of such high-risk suppliers already in use must be stopped within five years from the date of the announcement.[34] The classification as a high-risk vendor may be appealed within 14 days from the publication of the announcement before the Board.[35] The Board reviews the appeal within two months from receipt. The lodging of an appeal does not, however, suspend the prohibition. A further appeal against the decision of the Board upon appeal may then be lodged before the competent Provincial Administrative Court.[36]

In particularly justified cases, the Plenipotentiary may oblige the entity of the national cybersecurity system to which the risk assessment applies to draw up and deliver within 3 months a plan and a schedule of decommissioning of the hardware, software, and services of the hardware or software supplier that has been assessed as high risk.[37] The plan and schedule are subject to approval by the Plenipotentiary after consultation.

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. In case of violation of the prohibition of hardware and software of moderate risk vendors, fines can go up to 1% of the worldwide turnover of the previous financial year of the entity concerned. Pursuant to New Article 67 of the Cybersecurity System Act, the Plenipotentiary may also issue security warnings and security orders with regard to certain vendors and may recommend the "prohibition to use specific hardware or software."[38]

OUTLOOK

The Draft Law is currently subject to consultation. The political process is likely to be accelerated in light of a heated debate on the law and the upcoming elections in the United States.

---

[32] New Article 66a(4) No. 7 of the Cybersecurity System Act.

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

[34] New Article 66b(1) of the Cybersecurity System Act.

[35] New Article 66b(1) of the Cybersecurity System Act.

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

[37] New Article 66c of the Cybersecurity System Act.

[38] New Article 67b(3) No. 6 of the Cybersecurity System Act.

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.