Morgan Lewis | Report

CYBERSECURITY IN THE EU – MEMBER STATE IMPLEMENTATION OF THE NIS 2 DIRECTIVE:

THE EXAMPLE OF THE CZECH REPUBLIC

July 2023

IMPLEMENTATION OF THE NIS 2 DIRECTIVE BY EU MEMBER STATES – WITH A PARTICULAR FOCUS ON 5G NETWORK CYBERSECURITY

This Report constitutes a direct continuation of our prior report, The Approach of the EU and Selected Member States to 5G Network Cybersecurity, and starts a series of forthcoming evaluation of European member states' legislative proposals for the implementation of the directive on measures for a high common level of cybersecurity across the European Union[1] (NIS 2 Directive) into their domestic laws. The NIS 2 Directive, establishing unified legal measures aiming to boost cybersecurity in the EU, entered into force on 16 January 2023, and EU member states must transpose it into national law by 17 October 2024 (Article 41, NIS 2 Directive).

The 2020 EU cybersecurity toolbox, jointly agreed upon between the EU Commission (Commission) and member states, advocates a risk-based approach to cybersecurity in line with general principles of EU law. The EU cybersecurity toolbox recommends a well-balanced and coordinated set of risk-mitigating measures, notably relying on EU-wide standardization and certification. In the same vein, the NIS 2 Directive proposes a risk assessment based on objective, transparent, and proportionate criteria and is technology neutral.

Some member states have started departing from this joint EU approach and have chosen to rely on a selection of exclusively non-technical or political criteria to address the security of their information and communication technology (ICT), including 5G networks and other infrastructure.

Our team is closely following the developments of the national implementations and evaluates the compatibility of national implementing legislation with the objectives of the NIS 2 Directive and general EU law and principles. After describing in detail the NIS 2 Directive, this Report analyzes— in a first of a series of chapters on EU member states' legislation—the proposed implementation of the NIS 2 Directive by the Czech Republic.

On 19 June 2023, the Czech National Office for Cybersecurity and Information Security (NUKIB) initiated a public consultation, which will end on 19 July 2023, regarding the draft Cybersecurity Act (Draft Cybersecurity Act) and its eight implementing decrees (together, the Draft Czech Implementing Measures).

The Draft Czech Implementing Measures seek to transpose the NIS 2 Directive but also attempt to go beyond the requirements of the NIS 2 Directive with the introduction of a national screening mechanism for suppliers of entities operating under the NIS 2 Directive. So-called high-risk suppliers will no longer be allowed to supply the entities subject to the Draft Cybersecurity Act.

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

THE NIS 2 DIRECTIVE

BACKGROUND: A COORDINATED CYBERSECURITY FRAMEWORK AT EU LEVEL

The NIS 2 Directive updates the previous directive concerning measures for a high common level of security of network and information systems across the Union[2] (NIS Directive) and modernizes the existing legal framework at the EU level, which notably comprises the EU cybersecurity toolbox mentioned above and the EU Cybersecurity Act[3].

The NIS 2 Directive provides legal measures aiming to ensure the standardized minimum level of cybersecurity in the EU by:

- requiring member states to have the necessary tool that will increase their preparedness and security in the digital era;
- defining new tasks of the cooperation group, previously set up under the NIS Directive (Cooperation Group), which is composed of representatives of member states, the Commission and the European Union Agency for Cybersecurity (ENISA), to encourage and facilitate information sharing and strategic cooperation among member states;
- enforcing a security-conscious culture throughout industries, such as energy, transport, banking, financial market infrastructures, healthcare, and digital infrastructure, that are essential for our society and economy.

The NIS 2 Directive requires EU countries to adopt a national cybersecurity strategy that "provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity" (Article 7, NIS 2 Directive). Member states must designate competent authorities and a single point of contact to supervise the cybersecurity requirement (Article 8, NIS 2 Directive), and for the management of large-scale cybersecurity incidents and crises (Article 9, NIS 2 Directive). Furthermore, to strengthen the reporting obligations, each member state shall designate or establish one or more computer security incident response teams (Articles 10 to 12, NIS 2 Directive). Finally, the NIS 2 Directive coordinates the dynamics of the cooperation on both national level (Article 13, NIS 2 Directive) and European level (Articles 14 to 18, NIS 2 Directive).

Summary of the NIS 2 Directive

The NIS 2 Directive expands the scope of the application of the previous NIS Directive. It erases the distinction between *operators of essential services* and *digital service providers* and defines the organizations subject to the NIS 2 Directive by distinguishing between essential and important entities (Article 3, NIS 2 Directive), depending on the sectors they operate in, according to the lists in Annex I and II, respectively. In terms of size, an entity is in scope if it meets certain turnover thresholds (€10 million turnover and at least 50 employees for important companies; at least 250 employees or with an annual turnover of at least €50 or an annual balance sheet total of at least €43 million for essential companies). Therefore, the NIS 2 Directive applies in principle to large and medium-sized operators active in the sectors of high criticality (Annex I), or other critical sectors as defined in Annex II.

[2] 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

[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013

The highly critical sectors were expanded, and currently, Annex I covers the following:

- Energy (electricity, district heating and cooling, petroleum, natural gas, hydrogen)
- Transport (broadly applicable for air, rail, water, and road)
- Banking
- Financial market infrastructure
- Health (reference laboratories, medical device or pharmaceutical preparation manufacturers, and others)
- Drinking water
- Wastewater
- Digital infrastructure
- ICT service management
- Public administration
- Space

Annex II, targeting important entities, adds other critical sectors such as the following:

- Waste management
- Manufacture, production, and distribution of chemicals
- Production and distribution of food
- Postal and courier services
- Digital sectors and the providers
- Research

Nevertheless, for certain enumerated types of services, all entities, regardless of their size, will be subject to the NIS 2 Directive. This will apply to entities providing domain name registration services, providers of public electronic communications networks or publicly available electronic communications services, trust service providers, as well as entities deemed critical because of their specific importance for a particular sector or type of service, or for other interdependent sectors in a given EU member state (Article 2, NIS 2 Directive).

Notwithstanding the above, until April 2025, member states have to establish a list of essential entities and important entities, aiming to identify the entities highly exposed to a "significant cyber threat" (which under Article 6 (11) of the NIS 2 Directive means a "cyber threat which, based on its **technical characteristics**, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage (emphasis added)". This is in line with the EU rationale of an assessment based on technical and objective criteria.

According to the new **risk management obligations** set out by Articles 20 to 25 of the NIS 2 Directive, the entities in scope must take effective measures to manage the risks to the security of their network and information system. The NIS 2 Directive imposes a different level of cybersecurity risk-management measures on the selected entities. Therefore, both essential and important entities must take "appropriate and proportionate" technical, operational, and organizational measures to manage the risks posed to the security of network and information systems (Article 21, NIS 2 Directive). **Corporate**

accountability and governance are other safeguards imposed by the NIS 2 Directive (Article 20, NIS 2 Directive). To that end, the members of the management bodies and their employees of selected entities are required to follow trainings improving their knowledge regarding cybersecurity threats and risk assessment.

The NIS 2 directive also establishes a **reporting obligation**. Companies covered by the NIS 2 Directive have to immediately inform the appropriate supervisory authority of any cybersecurity incident (including data breaches) that has a significant effect on the provision of their services (Article 23, NIS 2 Directive). Entities will also be required to convey to service recipients any steps or remedies to be taken in response to serious cyber threats, as well as any potential harmful effects on the provision of services, without undue delay.

Another crucial development is the introduction of an **EU level coordinated security risk assessment** by the Cooperation Group, in cooperation with the Commission and ENISA, and, where appropriate, after consulting relevant stakeholders, including those from the industry, with the aim of identifying, per sector, the critical ICT services, ICT systems, or ICT products, relevant threats, and vulnerabilities. Such coordinated security risk assessments should identify measures, mitigation plans, and best practices to counter critical dependencies, potential single points of failure, threats, vulnerabilities, and other risks associated with the supply chain and should explore ways to further encourage their wider adoption by essential and important entities.

Finally, the NIS 2 Directive strengthens **the enforcement of the rules** by imposing that member states provide the possibility to impose effective, proportionate, and deterrent fines (Article 35, NIS 2 Directive) for essential entities, of at least up to €10 million or 2% of the worldwide annual turnover, and for important entities, of at least up to €7 million or 1.4% of the worldwide annual turnover.

Summary of Risk-Based Cybersecurity Measures for the ICT Supply Chain According to Common Criteria Established at EU Level

Per Article 21 (1) of the NIS 2 Directive, member states shall ensure that the essential and important entities take "appropriate and proportionate" technical, operational, and organizational measures to manage supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

Per Recital 90 of the NIS 2 Directive, in order to identify the supply chains that should be subject to a coordinated security risk assessment, the following criteria should be taken into account: (1) the extent to which essential and important entities use and rely on specific critical ICT services, ICT systems or ICT products; (2) the relevance of specific critical ICT services, ICT systems, or ICT products for performing critical or sensitive functions, including the processing of personal data; (3) the availability of alternative ICT services, ICT systems, or ICT products; (4) the resilience of the overall supply chain of ICT services, ICT systems, or ICT products throughout their lifecycle against disruptive events; and (5) for emerging ICT services, ICT systems, or ICT products, their potential future significance for the entities' activities.

The EU legislator aims to ensure a **balanced risk assessment** based both on technical and non-technical factors, thereby operating a hierarchy between technical and non-technical factors. In fact, Recital 90 of the NIS 2 Directive indicates that the security risk assessments of specific critical ICT services, ICT systems, or ICT products supply chains, should "take into account technical and, *where relevant*, non-technical risk factors", including those defined in Recommendation (EU) 2019/534, in the EU coordinated risk assessment of the cybersecurity of 5G networks and in the EU cybersecurity toolbox on 5G cybersecurity agreed by the Cooperation Group.

Member states shall indeed ensure that, when considering which measures are appropriate, entities take into account the **vulnerabilities specific to each direct supplier and service provider** and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures (Art. 21 (3)1), NIS 2 Directive). Member states are required to ensure that, when considering which measures referred to in that point are appropriate, entities are required to **take into account the results of the EU-level coordinated security risk assessments** of critical supply chains carried out in accordance with Article 22(1) of the NIS 2 Directive (Article 21 (3)2), NIS 2 Directive).

Per Article 22(1) of the NIS 2 Directive and in keeping with the overall harmonization objective, **such coordinated risk assessment is exclusively conducted by the Cooperation Group together with the Commission and ENISA—i.e., at EU level and not at member state level**. Any risk assessment conducted at member state level would in fact contradict the primary objective of the NIS 2 Directive, namely to remove divergences in cybersecurity requirements and the implementation of cybersecurity measures in different member states[4]. Recital 142 of the NIS 2 Directive is explicit in that that **the objective to achieve a high common level of cybersecurity across the Union,** "cannot be sufficiently achieved by the Member States but can rather, by reason of the effects of the action, be **better achieved at Union level."** Furthermore, Article 21(5) of the NIS 2 Directive requests the Commission adopt implementing acts, in cooperation with ENISA, the Cooperation Group, and sectorial-regulated communities, laying down the technical and the methodological requirements of the supply chain security, thereby emphasizing the importance of a harmonization in this regard.

It follows that the risk assessment of critical ICT services, ICT systems, or ICT products supply chains is first, operated based on the **coordinated risk assessment at EU level** and second, **considers primarily technical factors**, supplemented, where necessary, by non-technical factors (Article 22, NIS 2 Directive).

Article 32 of the NIS 2 Directive provides that "supervisory or enforcement measures imposed on essential entities in respect of the obligations laid down in this Directive are effective, proportionate and dissuasive, taking into account the circumstances of each individual case." The Directive goes on to state that member states shall ensure that security scans and risk assessments by the competent authorities are based on "objective, non-discriminatory, fair, and transparent risk assessment criteria." Consequently, the European legislator guarantees that the supervisory or enforcement measures imposed on essential entities are **proportionate, objective, fair, transparent, and based on an individual assessment of the facts of each case**.

A further harmonization tool is the promotion of the **use of European cybersecurity certification schemes** (Article 24, NIS 2 Directive). Member states may require essential and important entities to only use designated ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. The same disposition adds that the Commission is empowered (via delegated acts) to determine which categories of essential and important entities are required to use certain certified ICT products, ICT services, and ICT processes

[4] See for example Recital 5 of the NIS 2 Directive: "This [NIS 2] Directive aims to remove such wide divergences among Member States, in particular by setting out minimum rules regarding the functioning of a coordinated regulatory framework, by laying down mechanisms for effective cooperation among the responsible authorities in each Member State, by updating the list of sectors and activities subject to cybersecurity obligations and by providing effective remedies and enforcement measures which are key to the effective enforcement of those obligations."

or obtain a certificate under a European cybersecurity certification scheme adopted pursuant to Article 49 of Regulation (EU) 2019/881.

Such harmonized implementation of risk management requirements foreshadows **the introduction of European and international standards** (Article 25, NIS 2 Directive). As such, this prevents discrimination on the basis of use of a particular type of technology. This **technology neutrality** is reflected in Article 25 of the NIS 2 Directive, which emphasizes that in imposing cybersecurity risk-management measures under the NIS 2 Directive "member states shall encourage the use of European and international standards and technical specifications relevant to the security of network and information systems without imposing or favoring the use of a particular type of technology".

CZECH REPUBLIC

Competent Authorities and Relevant Legislation

In October 2021, the Czech National Security Council initiated a legislative process on a new Cybersecurity Act in the Czech Republic. Subsequently, **NUKIB** published a preparatory working document based on the material discussed by the Czech National Security Council. On 12 April 2022, NUKIB issued an official announcement that the proposal for a mechanism for assessing and reducing the risks associated with suppliers of electronic communications infrastructure could proceed to the next stage of elaboration of a draft factual intent of the law.[5]

As detailed above, the Draft Czech Implementing Measures[6] have been prepared by NUKIB. The unofficial consultation on these texts ended on 12 March 2023. According to public information, the public consultation began on 19 June 2023 and will end on 19 July 2023. After the official approval of NUKIB's director, the Draft Cybersecurity Act will be transferred to the Czech government and parliament for further legislative process.

According to Chapter V of the Draft Cybersecurity Act, NUKIB will be the central administrative authority responsible for the area of cybersecurity and for selected areas of classified information protections. NUKIB will also operate and manage the official website "NUKIB portal"—a crucial platform for the reporting obligations. Other institutions will also be involved in the process according to Chapter V of the Draft Cybersecurity Act: the Government CERT, the National CERT operator, new inspectors, and the existing permanent commission for the control of NUKIB.

Description of the Proposed Czech Cybersecurity Measures

Despite harmonization efforts at the EU level, in October 2022, NUKIB stated that "the assessment mechanism will allow the government to exclude high-risk suppliers from supplies to strategic infrastructure, thereby significantly limiting the impact of undue foreign influence on the provision of essential functions of the state." This follows an official recommendation published in February 2022 for assessing the trustworthiness of technology suppliers of 5G networks in the Czech Republic.[7] The accompanying report to the Draft Cybersecurity Act (Accompanying Report), which provides the rationale

[5] See NUKIB's press release

[6] The decrees implementing the Draft Cybersecurity Act are: decree on regulated services, decree on security measures of regulated service providers in the higher duty regime, decree on the security measures of regulated service providers in the regime of lower obligations, decree on supplier risk criteria, decree on security levels of public administration information systems, decree on authorized inspections, and decree on the NUKIB portal.

[7] See the official text

of the Draft Cybersecurity Act, namely the EU's focus on technical criteria. It maintains that "the European certification system includes only technical certification of products, services and processes and does not evaluate the level of strategic credibility of the supplier". Further, according to the Accompanying Report, screening of this so-called "strategic credibility" of suppliers cannot be conducted at the EU level because internal security would not be a matter of primary EU law.

Accordingly, the Accompanying Report purports that "the European cybersecurity certification system therefore currently appears only as a suitable supplement to the proposed solution, but it cannot and does not have the ambition to replace it." [8]

Scope and Characteristics

The supplier assessment mechanism will be conducted by NUKIB and will focus on suppliers already delivering their services to the strategic infrastructure, their sub-contractors, and potential suppliers. Despite the broad application of the Draft Czech Implementing Measures (and the NIS 2 directive), it seems that NUKIB's primary focus is to target 5G suppliers.

The supplier assessment mechanism will be based on information provided by individual managers of the regulated infrastructure combined with the government's own information and information obtained from other member states. The information under scrutiny will include (1) the characteristics of the state of residence of the supplier, (2) the characteristics of the suppliers, and (3) the previous "harmful" activity of both suppliers and states that potentially influence suppliers.

Obligations

The Draft Czech Implementing Measures impose a "regime of obligations based on the type of services". As per the NIS 2 Directive, the Draft Czech Implementing Measures create two different levels of obligations: (1) the regulated service providers placed under extensive obligations and (2) the regulated service providers placed under less extensive obligations.

Under the Draft Cybersecurity Act, the regulated service providers are in particular obliged to

- register on the NUKIB's portal and to report data;
- determine the scope of cybersecurity management;
- introduce security measures as stipulated stressed out in the decree on security measures for providers of regulated services (two levels of obligations);
- report cybersecurity incidents;
- inform customers about incidents and threats;
- take countermeasures;
- apply the rules of data localization—related to the proposed decree on security measures for providers of regulated services in the regime of extensive obligations (this issue is defined in more detail in the last part of the decree);
- fulfill the obligations of the supply chain safety management mechanism in the case of selected providers of regulated services in the regime of extensive obligations—related to

[8] See page 5 of the Draft Cybersecurity Act - Supply Chain Security

the Decree on Regulated Services, the Decree on Indispensable Functions, and the Decree on Supplier Risk Criteria; and

- submit to inspection by an inspector in the case of providers of a regulated service in the regime of less extensive obligations—related to the proposed Decree on Inspectors.

Procedure of the Supplier Screening Mechanism

- NUKIB shall report the **fulfilment of the criteria** for identifying the regulated service within 30 days of the date on which it finds that the criteria have been fulfilled (within 90 days at the latest when the criteria have been fulfilled).
- NUKIB **registers** the regulated service provider
    - on the basis of a report by the entity placed under the extensive obligations regime; and
    - on the basis of NUKIB's own finding of fulfilment of the criteria, unless the registration is made by the entity placed under the extensive obligations regime within the time limit.
- NUKIB collects and evaluates information and data related to the authority or person concerning a possible threat to the security of the Czech Republic. In line with a 2022 recommendation from NUKIB and other bodies, when **assessing risks**, NUKIB takes into account the criteria set out in the decree on supplier risk criteria, which are exclusively non-technical criteria, based in particular on the supplier's country of origin (i.e., the existence of a democratic political system, division of powers, respect for human rights, independent judicial review, obligation to cooperate with intelligence services, etc.).
- NUKIB is then entitled to issue a **measure of a general nature** that lays down the conditions or prohibits the use of the supplier of security-important supply to a critical part of a specified extent, if it detects a possible significant threat to the security of the Czech Republic or internal or public order as a result of the evaluation of the supplier's risk criteria.

NUKIB may authorise an exemption from the conditions or prohibition provided for by a measure of general nature if the performance of the measure of a general nature could jeopardise the provision of a regulated service. However, it will not allow such exception if this would completely defeat the purpose of the measure of a general nature.

Analysis of the Czech-Proposed Implementation Measures Under EU law and Principles

The Czech Republic Disregards Principles of EU Law Governing the Implementation of EU Directives

According to Article 288 of the Treaty on the Functioning of the European Union (**TFEU**), "a directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods." The effective implementation of European law is a prerequisite for achieving the policy objectives of the European Union. A fortiori, while transposing directives, member states guarantee the effectiveness of EU law, in accordance with the principle of sincere cooperation established in Article 4(3) of the Treaty of the European Union.

National measures must achieve the objectives set by the directive. In other words, **the transposition of a directive cannot go against the spirit of the directive**. Furthermore, a domestic legislation

aiming at implementing a directive, but which **goes beyond the minimum objectives of the directive** (referred to as "gold plating") must (1) not impede the functioning of the EU internal market and must (2) not infringe the principle of non-discrimination under Article 18 of the TFEU, both of which will be analyzed in the next section of this Report.[9] Member states and the Commission have acknowledged that the correct and timely transposition of directives is a legal obligation.[10] Importantly, member states are under an obligation to entirely implement EU directives. This means that member states cannot partially implement a directive without facing a potential infringement procedure. It is also settled case-law that national legislation cannot run counter upcoming EU legislation that will need to be implemented by member states. According to the principle of the **primacy of EU law**, a national measure may not contradict a directive, even if the latter has not yet been transposed by member states.[11]

Here, contrary to the EU cybersecurity toolbox and the NIS 2 Directive which enumerate both technical and non-technical criteria allowing member states to effectively mitigate risks, the risk assessment as set by **the Draft Czech Implementing Measures rely exclusively on several non-technical – political – criteria**.

It is in fact the proclaimed objective of the Draft Cybersecurity Act to "complement" the NIS 2 Directive by addressing the "level of strategic credibility of the supplier person" where the NIS 2 Directive" only involves technical certification of products, services and processes." In other words, it purports to not only add but also exclusively rely on subjective assessment criteria to the security certification which the NIS 2 Directive does not foresee.

As a result, the Draft Czech Implementing Measures list several countries and the entities established in these countries as a direct risk (for the Czech ICT supply chain) and exclude companies headquartered in these countries from the market - without the requirement for any technical or other risk screening.

This would not seem in line with the NIS 2 Directive's objectives of a harmonized approach to cybersecurity based on uniform, objective, proportionate, non-discriminatory, fair and transparent EU security standards. The impact assessment of the NIS Directive deplores that member states have opted for very different approaches when implementing the NIS Directive. With the NIS 2 Directive, therefore, the European legislator aims to introduce a high common level of cybersecurity in the EU that will prevent fragmentation at different levels across the internal market.[12] This general objective of increasing a common level of cybersecurity in the EU in the longer term will be implemented by a coordinated risk assessment at EU level.[13]

[9] Such practice is commonly referred to as "gold-plating" and is sanctioned by the Commission (see Communication from the Commission titled "EU law: Better results through better application (2017/C 18/02)". Furthermore, the European Court of Justice stated in Judgment of 18 December 1997, *Inter-Environnement Wallonie ASBL v Région wallonne*, case C-129/96, EU:C:1997:628, paragraph 44: "it is during the transposition period that the Member States must take the measures *necessary to ensure that the result prescribed by the directive is achieved* at the end of that period." (emphasis added). In Judgment of 13 November 1990, *Marleasing SA and La Comercial Internacional de Alimentación SA*, Case C-106/89, EU:C:1990:395, the European Court of Justice stated in paragraph 12: "It follows, therefore, that each ground of nullity provided for in Article 11 of *the directive must be interpreted strictly*." (emphasis added).

[10] See Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents, 2011/C 369/02.

[11] See for example Judgment of 18 December 1997, *Inter-Environnement Wallonie ASBL v Région wallonne*, case C-129/96 EU:C:1997:628.

[12] See Recital 4, NIS 2 Directive

[13] See Recital 4, NIS 2 Directive

Also, the NIS 2 Directive includes a variety of technical and non-technical criteria to address identified security risks. By contrast, the Czech supplier screening mechanism picks non-technical criteria only in order to protect critical networks against non-defined cybersecurity risks (see the decree on the supplier's risk criteria) by country of origin.

The Draft Czech Implementing Measures Are in Conflict With the Internal Market Rules and General Principles of EU Law

A national measure has to respect the EU Treaties and the general principles of EU law, such as the principle of proportionality, transparency, legal certainty, and non-discrimination as well as the rule of law.

First, the **principles of free movement** of goods and freedom to provide services established by Articles 28, 34, and 56 of the TFEU, respectively prohibit quantitative restrictions and all measures having equivalent effect on goods traded or services provided within the internal market. Restrictions on free movement may only be justified if they serve a legitimate aim and are proportionate. While the protection of national security can in principle constitute a legitimate aim, the public security exception available under the TFEU is construed narrowly. It is available only where there is "a genuine and sufficiently serious threat affecting one of the fundamental interests of society."[14]

In the case at hand, the Draft Cybersecurity Act leads to the potential exclusion of certain suppliers and would thus create barriers to the free movement of a variety of goods and technology without identifying a "cyber threat," as defined by the NIS 2 Directive.

Second, the **principle of proportionality** (Article 5(4) of the Treaty on the European Union (TEU)), directly referred to in the NIS 2 Directive, requires that a measure must not go further than what is necessary to achieve its objective. A measure has to serve the pursued objective in order to be proportionate. Here, the draft Czech Implementing Measures provide the possibility to rely exclusively on non-technical (political) criteria, without the need to consider any technical security enhancing measures. This in itself defeats the purpose of guaranteeing the objective of more security and reliability of the networks.

Moreover, when there is a choice between several appropriate measures, the least onerous must be adopted, and the disadvantages caused must not be disproportionate to the aims pursued.[15] Here, no technical or other remedial measures seem possible in the first instance. *There are, however, less restrictive and even more efficient ways* to mitigate network security risks, such as the establishment of tightened general security standards and certification, strengthened interoperability requirements, flexible multivendor commitments from network operators, localization of production capacities, requirements with regard to local storage of particularly sensitive data, requirements to comply with locally applicable product safety standards or as specified in the EU cybersecurity toolbox, regular supply chain audits and robust risk management.

Third, the fact that all assessment criteria contained in the screening mechanism are non-technical and open to broad interpretation is problematic with regard to **the principle of legal certainty**, according to which member states need to word their legal rules "unequivocally so as to give the persons concerned a clear and precise understanding of their rights and obligations and to enable national courts

[14] Judgment of 21 January 2010, Case C-546/07, *Commission v Germany*, EU:C:2010:25, paragraphs 48, 49; Judgment of 9 March 2000, *Commission of the European Communities* v *Kingdom of Belgium*, Case C-355/98, EU:C:2000:113, paragraph 28.

[15] Judgment of 13 November 1990, The Queen v Minister of Agriculture, Fisheries and Food and Secretary of State for Health, ex parte: Fedesa and others, Case C-331/88, EU:C:1990:391, para 13.

to ensure that those rights and obligations are observed."[16] When assessment criteria use non-objective concepts, they are difficult for hardware and software suppliers to verify and evaluate with any certainty.

Although for some obligations, such as reporting of cybersecurity incidents, a transitional period will apply to adapt the organization's environment, other obligations under this law will need to be fulfilled immediately after notification of registration (Section - "Transitional Provisions" of the Rationale for the Draft Cybersecurity Act). The fundamental principles of legal certainty and proportionality generally require adequate transition periods, giving market players opportunity to adapt to new requirements. This applies here in particular because 5G infrastructure is technically composed of infrastructure for the older generation 4G and 3G technology, which is already built in.

Fourth, to the extent that the criteria for assessment are not based on objective criteria, the risk assessment mechanism is also inherently discriminatory and in contradiction with **the principle of non-discrimination (Article 2 TEU, 18 TFEU).**[17] This applies here in particular as there is a clear reference to specific countries under whose jurisdiction the supplier falls. As an illustration, a supplier that operates in the EU through EU-established subsidiaries but which has its headquarters under the jurisdiction of a third country (non-EU member state) could face an automatic ban.

Discrimination between products or services based on geographic origin, on grounds of nationality, is also caught by World Trade Organization (WTO) rules, in particular **Article 3 of GATT and Article 17 of GATS** (commonly referred to as the most-favoured-nation (MFN) rule).[18] Under Article XVI(4) of the Agreement establishing the WTO, each member of the WTO is obliged, within the framework of its internal legal order, to ensure compliance with its obligations under WTO law within the various parts of its territory.

The MFN rule is a clause that also typically appears in free trade agreements (FTAs). The Czech Republic is party to numerous FTAs, primarily as an EU Member State, but also within bilateral FTAs.

Additionally, it seems that the Draft Cybersecurity Act runs against general principles of the European Charter on Fundamental Rights, such as the **freedom to conduct business or the right to property**, consecrated by Articles 17 and 18 of the European Charter of Fundamental Rights.

This conclusion does not change in light of Article 4(2) TFEU, which confers on each Member State the sole responsibility to protect national security. Indeed, the CJEU has recently held in *Privacy International*, that derogations from EU law based on a national security justification are still subject to a proportionality assessment in accordance with Article 52(1) of the Charter of Fundamental Rights of the European Union.[19]

By operating a risk assessment at national level and by exclusively relying on non-technical, discriminatory, non-transparent, and non-objective assessment criteria, the Draft Cybersecurity Act seems to run counter to the general spirit and objectives of the NIS 2 Directive and only partially transposes it.

An incorrect implementation of a directive can result in legal action from the Commission against the member state under Article 258 of the TFEU, a so-called infringement procedure. If the Commission

[16] Judgment of 9 July 2015, Radu Florin Salomie and Nicolae Vasile Oltean v Direcția Generală a Finanțelor Publice Cluj, Case C-183/14, EU:C:2015:454, paragraph 32.

[17] See also for sectoral secondary legislation: Article 1) of Regulation 2015/2120 (ICT Regulation); Article 3 (4) (b) c) of the EEEC

[18] See also Annex on Telecommunications

[19] Judgment of 6 October 2020, *Privacy International*, Case C-623/17, EU:C:2020:790, paragraphs 74-82.

concludes that the member state is failing to fulfil its obligations under EU law, the Commission may decide to refer the matter to the Court of Justice of the European Union (CJEU) and ultimately ask the CJEU to impose penalties.

By way of illustration, the European Commission launched infringement proceedings against Poland in July 2020 because Poland amended certain provisions of the Polish telecommunications law concerning the appointment and dismissal of the heads of the Polish national regulatory authority, the Office of Electronic Communications, and prematurely dismissed the head of the Polish national regulatory authority (NRA).[20] Similarly, it opened infringement proceedings against Hungary considering that Hungary is in breach of EU law by applying disproportionate and non-transparent conditions to the renewal of rights to use radio spectrum in violation of the rules of the EEEC[21].

No Enforceability Without TRIS Notification

Directive No 2015/1535[22] (TRIS Directive) establishes a notification procedure allowing the Commission and member states to examine the technical regulations member states intend to introduce for products and for Information Society services, prior to their adoption, thereby ensuring that these texts are compatible with EU law and internal market principles. Prior authorization mechanisms constitute such technical regulations within the meaning of Article 1(1)(f) of the TRIS Directive.[23]

Procedurally, member states have to suspend the adoption of a draft technical regulation for three months from the date of receipt by the Commission to allow for comments on the draft technical regulation by the Commission and member states (Article 6, TRIS Directive). **A breach of the notification obligation would** constitute a procedural defect in the adoption and **render those technical regulations inapplicable and therefore unenforceable against companies and individuals**.[24] Furthermore, a technical regulation adopted in breach of the obligation to postpone the adoption of a notified national legislation (i.e., to respect the standstill period), can also be declared inapplicable to individuals by national courts).[25]

Where it emerges that the notified drafts may create barriers to the free movement of goods or to the free provision of Information Society services or to EU secondary legislation, the Commission and the other member states may submit a detailed opinion to the member state that has notified the draft. This has the effect of extending the standstill period and starts a process during which the member state will have to propose amendments to accommodate the legal concerns raised.

[20] See press release

[21] See press release

[22] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services

[23] Judgment of 21 April 2005, *Lindberg*, Case C-267/03, EU:C:2005:246, paragraph 76; Judgment of 19 July 2012, *Fortuna and Others*, Cases C-213/11, C 214/11 and C 217/11, EU:C:2012:495, paragraph 31.

[24] Judgment of 4 February 2016, *Ince*, Case C-336/14, EU:C:2016:72, paragraph 67; Judgment of 16 July 2015, *UNIC and Uni.co.pel*, Case C-95/14, EU:C:2015:492, paragraph 29. Judgment of 28 May 2020, S*yndyk Masy Upadłości ECO-WIND Construction S.A. w upadłości anciennement v Samorządowe Kolegium Odwoławcze w Kielcach*, Case C-727/17, EU:C:2020:393, paragraph 46; Judgment of 21 April 2005, *Lindberg*, Case C-267/03, EU:C:2005:246, paragraph 77; Judgment of 19 July 2012, *Fortuna and Others*, Case C-213/11, C 214/11 and C 217/11, EU:C:2012:495, paragraph 32

[25] Judgement of 26 September 2000, *Unilever Italia SpA v Central Food SpA,* Case C-443/98, EU:C:2000:496.

OUTLOOK

In line with the fundamental principles of the EU law, member states should act in full respect of the openness of the EU internal market. Although NIS 2 Directive presents minimum harmonization (as endorsed by the Article 5 of the NIS 2 Directive), member states, aiming to adopt or maintain provisions ensuring a higher level of cybersecurity have to respect the obligations laid down in EU law.

The EU legislator aims to assure the harmonized evaluation and risk evaluation mechanism throughout the EU. Only centralized and uniform methodology will cumulatively guarantee the equal standard of evaluation and ensure the level playing field within the market between market operators.

The Czech Draft Cybersecurity Act as it stands today **deviates from the harmonized approach agreed upon at the EU level in that it relies only on non-technical criteria and relies on a separate risk assessment conducted exclusively at national level.**

As mentioned before, after the official approval of NUKIB's director, the Draft Cybersecurity Act will be transferred to the Czech government and parliament for further legislative process. It is suggested that the Czech Republic adapt the national rules so that the identification of the security concerns be proportionate to the objectives they seek to attain. There are less restrictive ways to mitigate network security risks, such as the adoption of the objective security standards and certifications.

CONTACT

If you have any questions or would like more information on the issues discussed in this report, please contact:

Brussels

Christina Renner	+32.2.507.7524	christina.renner@morganlewis.com
Jasmeen Bahous	+32.2.507.7523	jasmeen.bahous@morganlewis.com
Maciej Bernard Plotka	+32.2.507.7518	maciej.plotka@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.

ANNEX I: PROVISIONS OF THE NATIONAL TRANSPOSITION

THE CZECH REPUBLIC'S DRAFT CYBERSECURITY ACT AND DECREES	NIS 2 DIRECTIVE	OUR COMMENT
Draft Cybersecurity Act (Title II) Determination of Regulated services "Regulated services criteria"; and Decree on regulated services, §2	**Article 2 - Scope** And **Article 3 – Essential and important entities**	Directive assures expansion of the number of obliged organizations.
Draft Cybersecurity Act	**Article 7 – National cybersecurity strategy** including (d) a mechanism to identify relevant assets and an assessment of the risks in that member state;	The general obligation to elaborate the national plans seems to be accomplished by the elaboration of the New Cybersecurity Act.
Decree on the security measures of regulated service provider in the regime of extensive obligations and less extensive obligations	**Article 9 – National cyber crisis management frameworks**	NIS 2 recommends designating and establishing one or more competent authorities responsible for management of large-scale cybersecurity and adopt a plan where the objectives of risk management will be described.
Decree on the security measures of regulated service provider in the regime of extensive obligations and less extensive obligations	**Article 12 - Coordinated vulnerability disclosure and a European vulnerability database**	The coordinated publication of information on vulnerabilities and the establishment of a European database of vulnerabilities.
Draft Cybersecurity Act – Part two (Title I)	**Article 13 – cooperation on national level**	NIS 2 sets a closer cooperation between authorities and organizations, and establishes coordination of supervisory activities for organizations that have the obligation to ensure cybersecurity from multiple legal regulations (e.g., in the energy, aviation, or personal data protection sectors). Nevertheless, an organization at the national level is the responsibility of the member states.
Draft Cybersecurity Act (Chapter V Performance of State Administration)	**Articles 14, 15 and 16 – cooperation on international level**	NIS2 secures deeper cooperation with member states in the areas of cyber crisis management, the resolution of large-scale cybersecurity incidents and

THE CZECH REPUBLIC'S DRAFT CYBERSECURITY ACT AND DECREES	NIS 2 DIRECTIVE	OUR COMMENT
		the sharing of strategic information and good practice.
Decree on the security measures of regulated service provider in the regime of lower and extensive obligations	**Article 20 – on governance**	NIS 2 guarantees mandatory education of the top management of the organization and greater management responsibility for ensuring cybersecurity in the organization.
Decree on the security measures of regulated service provider in the regime of lower and extensive obligations	**Articles 20 and 21 – cybersecurity risk-management**	Concretization of security measures, which are based on an approach that takes into account all types of risks (physical and cyber) aimed at protecting information systems from incidents. These measures will have to be implemented by the obliged entities and must include the minimum obligations.
Draft Cybersecurity Act (part One, title II of the Act) Decree on Regulated Services; Supply Chain Security – Cyber Security Act	**Article 22** – Union level coordinated security risk assessment **Recital 90 of the NIS 2 Directive** – assessment for the ICT services and infrastructure	NIS 2 establishes a supranational coordinated security risk assessment of critical supply chain.
Draft Cybersecurity Act (Reporting of data by a regulated service provider)	**Articles 21 and 23 – cyber security risk and reporting obligations**	NIS 2 established greater involvement of the European Commission in the unification of regulation in member states. The Commission may adopt implementing acts laying down technical, methodological and, where applicable, sector-specific requirements regarding measures to manage cybersecurity risks or specifying the type of information, format, and notification procedure in the event of a cybersecurity incident.
	Article 25 – on Standardization	A crucial tool aiming to promote the convergent implementation of Article 21 NIS 2.

THE CZECH REPUBLIC'S DRAFT CYBERSECURITY ACT AND DECREES	NIS 2 DIRECTIVE	OUR COMMENT
Draft Cybersecurity Act (Regulated service provider registration)	**Articles 27 and 28 –** on Registry of entities and database of domain name registration data	The EU legislators specified more detailed requirements for maintaining the register of internet top-level domains and the activities of registrars.
Draft Cybersecurity Act (Title VI) and Decree on Authorized inspections	**Articles 32 and 33 –** the assurance of supervisory powers of the authorities	NIS 2 aims to equip authorities with the instruments to issue warnings, reactive measures, carry out audits and controls, and the ability to impose fines or other administrative penalties.
The New Act on Cyber Security	**Articles 34 – general conditions for imposing the fines**	The reform of the NIS Directive secured a significant increase in fines for non-compliance with imposed obligations.