Bird & Bird & Developments on NIS Directive in EU Member States

January 2020

Austria

Current status of implementation	The NIS Directive has been implemented on 29 December 2018.
Implementation Act	Net- and Information-System-Security Act (*Netz- und Informationssystemsicherheitsgesetz*, briefly "**NISG**").
Determination of operators of essential services (Art. 5 NIS)	Pursuant to Sec. 2 NISG, the NISG stipulates measures for securing a high security level in networking- and IT-systems of "operators [located in Austria or having an Austrian branch] of essential services" in the fields of (i) energy, (ii) traffic, (iii) banking, (iv) financial market infrastructures, (v) health, (vi) drinking water sully and (vii) digital infrastructure. Pursuant to Sec. 16 NISG, the Austrian chancellor has determined the specific "operators of essential services" and also provided for a more detailed definition of the terms “essential services”, “security incidents” and “security measures” by way of the Net- and Information Systems Security Regulation (*Netz- und Informationssystemsicherheitsverordnung*) that was issued on 17 July 2019.
reporting obligations	Sec. 19 NISG requires operators of essential services to immediately report security incidents concerning one of their essential services to the competent computer emergency team, which immediately shall forward the report to Minister of Internal Affairs. This report must include all relevant circumstances concerning the incident and the technical circumstances to the extent available; this particularly applies to the assumed cause, the concerned information technology and the nature of the concerned facility. Circumstances which become known at a later stage have to be furnished without undue delay. Sec. 3 fig 6 NISG defines "security incident" as a disruption of (i) availability, (ii) integrity, (iii) authenticity or (iv) confidentiality in networking- or which lead to a limitation of availability or unavailability with substantial consequences. For considering the substantiality, the following criteria have to be factored in: (i) number of concerned users, particularly of such users, who require the concerned service for providing their own services, (ii) the duration of the incident, (iii) geographic reach of the incident and (iv) impacts on economic and social activities. Pursuant to Sec. 21 NISG, operators of digital services (which have their main seat in Austria or, in case their main seat is not located in the EU, which have appointed a representative), also have to report security incidents accordingly.
sanctions regime	Sec. 26 NISG provides for the following administrative fines: up to EUR 50,000 and, for repeating offenders, up to EUR 100,000.
competent authorities	Pursuant to Sec. 6 NISG, the Austrian Minister of Internal Affairs shall establish a single point of contact at the Ministry of Internal Affairs. This is the Office for Strategic Networking- and Information-Systems Security (*Büro für Strategische Netz und Informationssystemsicherheit*, briefly "**NIS-Office**").

Jurisdictional applications	Operators of essential services: located in Austria or having an Austrian branch; Operators of digital services: having their main seat in Austria or, in case their main seat is not located in the EU, which have appointed a representative which has its seat in Austria and which was explicitly nominated by the operator to act on his behalf.
Remarks (if any)	N/A

Belgium

Current status of implementation	The NIS Directive has been implemented in Belgium on 7 April 2019. The Belgian implementation act has entered into force on 3 May 2019.
Implementation Act	Act of 7 April 2019 establishing a framework for the security of network and information systems of general interest for public security (the "**Act**")
Determination of operators of essential services (Art. 5 NIS)	An operator of essential services ("**OES**") is defined in Art. 6 of the Draft Act as a public or private entity that is active in Belgium in one of the sectors included in Annex I of the Act (which is highly similar to Annex II of the NIS-Directive) and which has been designated by the appropriate sectoral authority in accordance with the conditions laid down in the Act. These conditions are the following: the entity concerned must provide (i) a service essential for the maintenance of critical societal/economic activities, which (ii) depends on network and information systems, and (iii) where an incident would have significant disruptive effects on the provision of that service, taking into account the criteria and thresholds as envisaged in Art. 13 of the Act.
reporting obligations	Operators of essential services must notify without undue delay the national CSIRT, the sectoral authority or its sectoral CSIRT and the national competent authority of any incident having a substantial impact on the availability, confidentiality, integrity or authenticity of the network and information systems upon which the essential service(s) provided by that operator is/are dependent. The Act also stipulates that the modalities for the notification of incidents will be laid down in a Royal Decree, which will also establish a secure platform for this purpose. Such platform will be created pursuant to the Royal Decree of 12 July 2019 on the implementation of the act of 7 April 2019 establishing a framework for the security of network and information systems of general interest for public security and of the act of 11 July 2011 on the security and protection of critical infrastructures. The Royal Decree of 12 July 2019 has moreover imposed upon the national CSIRT an obligation to create a notification form for such notifications.
sanctions regime	Art. 51 and 52 of the Act provide for criminal and administrative sanctions respectively. Criminal sanctions include both prison sentences (ranging from 8 days to 3 years) and fines (ranging from EUR 26 to EUR 75,000). It should be noted however that in Belgium, criminal fines as indicated in the law must always be multiplied with a multiplication factor. The current factor is 8. Consequently, in practice a fine under Art. 51 of the Draft Act will range between EUR 208 and EUR 600,000. The administrative sanctions range between EUR 500 and EUR 200,000.

competent authorities	The Centre for Cyber Security Belgium has been identified as both the national authority and the national CSIRT for Belgium through the Royal Decree of 12 July 2019 on the implementation of the act of 7 April 2019 establishing a framework for the security of network and information systems of general interest for public security and of the act of 11 July 2011 on the security and protection of critical infrastructures.
Jurisdictional applications	The Act is applicable only to operators of essential services having at least one establishment within the Belgian territory and which effectively conduct an activity that relates to the provision of at least one essential service on Belgian territory. It is applicable to digital service providers having their main establishment in Belgium, which is understood as having their registered seat in Belgium. It also applies to digital service providers that are not established in the EU when they provide online marketplace services, online search engine services or cloud computing services in Belgium and their representative is established in Belgium.
Remarks (if any)	While the first OES have now been designated and informed thereof by the relevant sectoral authorities, the list of operators concerned will not be made public for safety reasons.

Bulgaria

Current status of implementation	The implementation of the NIS Directive has been completed.
Implementation Act	Cybersecurity Act, in force as of 16 November 2018. Ordinance on the minimum requirements for network and information security, in force as of 26 July 2019.
Determination of operators of essential services (Art. 5 NIS)	According to Art. 4 para. 2 of the Cybersecurity Act, operator of essential services shall be a public or private entity of the categories related to the sectors and subsectors listed in Appendix 1 to the Act, which meets the following criteria: (i) provides an essential service, and (ii) the provision of that essential service depends on networks and information systems, and (iii) network and information security incidents have significant disruptive effect on the provision of that service. The operators of essential services shall be identified by certain administrative authorities, taking into account the criteria listed above and in accordance with a methodology which shall be approved by the Council of Ministers (Art. 4 para. 3 of the Cybersecurity Act). By Decision No.192 of the Council of Ministers dated 09 April 2019 the administrative authorities which have the power to identify the operators of essential services in the respective sector have been determined, also a methodology has been adopted. In that regard, it shall be noted that where an operator provides an essential service in two or more Member States, the administrative authorities shall consult with the respective Member State before a decision on identification is taken (Art. 4 para. 4 of the Cybersecurity Act). Also, the Chairperson of the State Agency for Electronic Management shall create and maintain a register of the essential services which shall contain, inter alia, a list of the operators of essential services as well as the essential services provided by these operators (Art. 6 para. 1 sentence 2 of the Cybersecurity Act). Art. 6 para. 4 of the Cybersecurity Act stipulates that the register of the essential services shall not be public, but it may be inferred that the process of identification of operators of essential services has been completed as the 4 month period prescribed for the operators of essential services to comply with the provisions of the Ordinance has expired (Sec. 3 of the

	Transitional and Final provisions of the Ordinance on the minimum requirements for network and information security).
reporting obligations	According to Art. 21 of the Cybersecurity Act, the administrative authorities shall notify the respective computer security incident response team for the sector of any incident that has an impact on the continuity of their activity. The persons performing public functions and the organizations providing public services shall also notify the respective computer security incident response team for the sector of incidents that have an impact on the continuity of the administrative services provided by them electronically (Art. 22 of the Cybersecurity Act). Obligations to notify the respective computer security incident response team for the sector have also the operators of essential services regarding incidents which have an impact on the continuity of the essential services provided by them (Art. 23 of the Cybersecurity Act) and the digital service providers regarding incidents which have a significant impact on the continuity of the digital services they provide (Art. 25 of the Cybersecurity Act). According to the Cybersecurity Act, the initial notification for the incident shall be made within two hours after the finding of the incident. Full information about the incident shall be provided within five working days. Art. 27 of the Cybersecurity Act stipulates that persons and entities different from administrative authorities, persons performing public functions, organizations providing public services, operators of essential services and providers of digital services may also notify the computer security incident response teams of incidents that have an impact on the continuity of the services they provide. Pursuant to Art. 3 para. 2 of the Ordinance on the minimum requirements for network and information security the administrative body, respectively the head of the other obliged under the Cybersecurity Act bodies (namely the persons performing public functions, the organizations providing public services, the operators of essential services and the providers of digital services) shall designate a civil servant/unit to be responsible for network and information security. In case of a network and information security incident, the civil servant/unit must notify the respective computer security incident response team for the sector within the terms specified in the Cybersecurity Act. (Art. 31 para. 1 of the Ordinance on the minimum requirements for network and information security) There is a special form for that notification which is set out in Appendix 7 to the Ordinance. Further, the Ordinance provides for adoption of internal rules regarding the signal processing and the incident response activities as well as plans for dealing with certain network and information security incidents (Art. 30 of the Ordinance on the minimum requirements for network and information security).
sanctions regime	Art. 28 of the Cybersecurity Act provides for administrative fines ranging from BGN 1,000 to BGN 15,000 in case of violations relating to incidents reporting obligations under the Act. In case of a repeated violation the fines increase and shall range from BGN 2,000 to BGN 20,000. Art. 29 sets forth liability for failure to provide certain information and evidence or failure to comply with mandatory instructions, where the administrative fines range from BGN 1,000 to BGN 15,000. In case of a repeated violation the fines increase and shall range from BGN 2,000 up to BGN 25,000. Liability for other violations of the Cybersecurity Act is also laid out in Art. 30 thereof, with administrative fines ranging from BGN 1,000 up to BGN 15,000.
competent authorities	The Cybersecurity Act provides for the establishment of a system of competent authorities and units in the field of network and information security, clearly defining their obligations and responsibilities. Some more important authorities and units pursuant to the Cybersecurity Act are: (i) State e-Government Agency; (ii) National single point of contact with the State e-Government Agency; (iii) National competent authorities on the security of network and information systems for the sectors and services specified in Appendix 1 and 2 of the Cybersecurity Act which are specifically set up under the auspices of the administrative authorities determined in Decision No. 192 of

	the Council of Ministers dated 09 April 2019; (iv) Computer security incident response teams at sector level with the national competent authorities and the State e-Government Agency; (v) National computer security incidents response team with the State e-Government Agency. According to Art. 21 of Rules on the activities, structure and organization of a State e-Government Agency the Network and Information Security Directorate shall provide support to the Chairman of the State Agency by developing and implementing the functions of a National competent authority for all administrative authorities as well as for the persons performing public functions and the organizations providing public services as defined in Art. 4 para. 1, sentence 3 and 4 of the Cybersecurity Act, of a National single point of contact, of a National computer security incidents response team and of a Computer security incident response team for the administrative authorities. The Council of Ministers (along with the Cybersecurity Council and the Cybersecurity Coordinator), Ministry of Defence, Ministry of Interior and the State Agency for National Security also hold competence under the Cybersecurity Act. In addition it should be pointed out that the administrative body, respectively the Head of the other obliged under the Cybersecurity Act bodies, is directly responsible for the network and information security even when it has delegated its powers to a civil servant/unit (Art. 3 para.1 sentence 1 of the Ordinance on the minimum requirements for network and information security).
Jurisdictional applications	Art. 26 of the Cybersecurity Act deals with jurisdiction in relation to providers of digital services. It stipulates that if a digital service provider has its seat and registered address or a representative in the Republic of Bulgaria, but its networks and information systems are located in one or more other EU Member States, the respective national competent authority and the competent authorities of the other EU Member States shall cooperate and assist each other, if necessary. A digital service provider which is not established in an EU Member State, however offers in the EU the services listed in Appendix 2 to the Cybersecurity Act, shall designate its representative in the EU, which representative shall be established in one of the EU Member States where the services are offered. When such representative has its seat and registered address in the Republic of Bulgaria, it shall be deemed that the digital service provider falls under the jurisdiction of the Republic of Bulgaria.
Remarks (if any)	The Ordinance on the general requirements for security of network and information systems (approved on the ground of Art. 43, para. 2 of the Electronic Government Act) has been repealed by Order No. 186 of the Council of Ministers dated 19 July 2019 for adopting Ordinance on the minimum requirements for network and information security.

Croatia

Current status of implementation	The NIS Directive has been implemented on 26 July 2018.
Implementation Act	The implementation act has been published in Croatia's Official Gazette no. 64/2018 and has been in force as of 26 July 2018. The Act on the Cybersecurity of Essential Services Operators and Digital Services Providers (hereinafter referred to as “Cybersecurity Act”) and bylaws have also been enacted on 4 August 2018 (the Decision on Essential Services Operators and Digital Services Providers, “the Decision”).

Determination of operators of essential services (Art. 5 NIS)	Any private or public entity shall be deemed an operator of essential services when: (i) an entity provides any of the services from Appendix I (essential services); (ii) the provision of that service by that entity depends on network and information systems; (iii) an incident would have significant negative effects on the provision of any essential service. Appendix I of the Cybersecurity Act lists the following sectors in which certain services are essential: (i) energy, (ii) transport, (iii) healthcare, (iv) water supply, (v) banking, (vi) financial market infrastructure, (vii) digital infrastructure and (viii) business services for government bodies. A detailed list of services and criteria for determining the significance of negative effects of an incident are also listed in Appendix I. The services in the above sectors considered essential are the usual services of great infrastructural importance like maintenance and operation of railways, oil and gas pipelines, telecommunications etc.
reporting obligations	In case of an incident, Essential Service Operators ("**ESO**") and Digital Service Providers ("**DSP**") are obligated to notify the relevant Computer Security Incident Response Team ("**CSIRT**") with no undue delay about incidents which have a significant effect on the continuity of their services. If an incident on network/IT systems of a DSP has significant effect on an Essential Service ("**ES**"), the ESO notifies the relevant CSIRT. The reporting is done in three phases according to the Executive Order: the initial report, the transitional period report and the final report. The initial report is to be delivered to the CSIRT no later than four hours after discovery, the transitional report within three days of the initial report, and the final report within 15 days of when the service was resumed. The relevant CSIRT may bring further directions on how incidents are to be reported.
sanctions regime	Failure to comply with the obligations laid out in the Cybersecurity Act is a misdemeanor. The fines range from EUR 20,000 to EUR 67,000 for the entity and from EUR 2,000 to EUR 6,000 for the responsible person within the entity.
competent authorities	Competent sector authorities ("**CSA**") (Ministries for relevant sectors, and various agencies and government offices, e.g. The Croatian National Bank) are responsible for identifying which entities are ESOs, keeping lists of ESOs and assessing their levels of dependence on IT and network systems. These lists are forwarded to the single point of contact. CSAs also supervise the implementation of security measures by EOSs and DSPs, cooperate with one another and share information among them and to the data protection authority. The single point of contact is the Office of the National Cyber Security Council. Its main purpose is to be the coordinator and to track progress/activity in this matter. CSIRTs are either the national Computer Emergency Response Team ("**CERT**") or Institute for security of IT systems. They are responsible for receiving incident reports and notifying the public about the incident. CSIRTs have many duties of technical nature (risk assessment, data analysis etc.). Authorities for technical assessment of compliance are the Institute for security of IT systems, National CERT or the Croatian Academic and Research Network. The full list can be found in Appendix III to the Cybersecurity Act. These authorities preform the technical side of supervision of ESOs and DSPs.
Jurisdictional applications	The Cybersecurity Act is applicable to ESOs regardless of where they are seated, their size, ownership and organizational structure. The Cybersecurity Act applies to DSPs with a seat or representative on the territory of Croatia, except micro or small subjects as understood in legislation regarding incentivizing small business.

Remarks (if any)	Institute for security of IT systems and Croatian Academic and Research Network issued in October 2019 "Framework of good practices for ESOs' harmonisation with Cybersecurity Act measures and for compliance assessment procedure" (*Okvir dobrih praksi za usklađivanje operatora ključnih usluga s mjerama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga i provođenje ocjene sukladnosti*) which contains guidelines, recommendations and good practices for complying with security measures. The document is intended for ESOs obliged to harmonise with Directive, however, it is not binding and its main purpose is to serve as the implementation guide for ESOs in process of complying with security measures, but also as a guidance for competent sectorial authorities, technical compliance assessment authorities and internal or external auditors performing supervision or compliance assessment of ESOs. The document shall be periodically updated based on the current needs and in line with information and experience gained in the compliance assessment process.

Cyprus

Current status of implementation	The NIS Directive has been implemented on 5 April 2018.
Implementation Act	Network and Information Security Law of 2018 (Law 17(I)/2018).
Determination of operators of essential services (Art. 5 NIS)	No identification of the operators of essential services has been made yet. According to Art. 2 para. 1 of the Network and Information Security Law, operators of essential services means a public or a private entity of a type referred to Annex II of the Directive which meets the below criteria: (i) the entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (ii) the provision of that service depends on network and information system and (iii) an incident would have significant disruptive effects on the provision of that service.
reporting obligations	Operators must notify the competent authority without undue delay of any incident having a substantial impact on the provision of the services. Providers of digital services must notify the competent authority without undue delay of any incident having a substantial impact on the provisions of the services within the territory of Cyprus or any other EU member state.
sanctions regime	Sec. 15 of the Network and Information Security Law provides that any person who prevents any employee of the competent authority to fulfil his duties is guilty of an offence and subject to imprisonment of up to 6 months and / or to a fine of up to EUR 10,000. Sec. 16 of the Network and Information Security Law provides that any person who breaches the Network and Information Security Law, the regulations or the decisions of the competent authority is guilty of an offence and subject to imprisonment of up to 6 months and / or to a fine of up to EUR 10,000. Sec. 30 of the Network and Information Security Law provides for administrative fines of up to EUR 8,500 for violations of the Network and Information Security Law or the decisions of the competent authority.
competent authorities	The Cyprus Digital Security Authority is an independent authority which is competent for the information security at national level, including the prosecution and repression of administrative fines.
Jurisdictional applications	Operators of critical infrastructures are subject to Cyprus law if the infrastructure is located in Cyprus.
Remarks (if any)	N/A

Czech Republic

Current status of implementation	Czech NIS Directive Implementation Act has been implemented on 1 August 2017.
Implementation Act	The Act No. 205/2017 Coll. (Collection of Acts part 74) amends Act No. 181/2014 Coll. on Cyber Security ("**CSA**"), as amended by Act No. 104/2017, Act No. 412/2005 Coll. on Protection of Classified Information and also to a lesser extent other related Acts.
Determination of operators of essential services (Art. 5 NIS)	Pursuant to Art. 5 of the NIS Directive, the Czech legislator has specified the criteria to identify operators of the following essential services: a) energy, b) transportation, c) banking, d) financial markets infrastructure, e) healthcare, f) water management, g) digital infrastructure and h) chemical industry. Operators of essential services can be legal persons, entrepreneurs or public bodies, which (i) operate one of the following essential services and (ii) are designated as such by the National Cyber and Information Security Agency. For information purposes pursuant to Art. 5 para. 7 of the NIS Directive, the following bodies are also classed as operators of essential services: i) administrators and operators of information systems of critical information infrastructure and ii) administrators and operators of communication systems of critical information infrastructure.
reporting obligations	Certain authorities and persons (listed in Sec. 3 lit. b-f of the CSA) are required to report cyber-security incidents in their Significant Network, the Critical Infrastructure Information System, Critical Information Infrastructure Communication System, Basic Service Information System, or Significant Information System, without delay after detection (Sec. 8 para. 1 of the CSA). They either report the cyber security incidents to the national CERT or the National Cyber and Information Security Agency (Sec. 8 para. 2, 3 of the CSA). Authorities and persons not listed in Sec. 3 of the CSA can report to either the national CERT or the National Cyber and Information Security Agency (Sec. 8 para. 6 of the CSA). In the event that a cyber security incident has a significant impact on the continuity of the provision of the basic service, the operator of the basic service shall notify the National Cyber and Information Security Agency (Sec. 8 para. 1 of the CSA). Providers of digital services must immediately report any cyber security incident that has significant impact on the provision of its digital service, provided that it has access to the information necessary for assessing the significance of the impact (Sec. 8 para. 2 of the CSA).

	If the cyber security incident that has affected a provider of a digital service has a significant impact on the continuity of provision of the digital service, the provider of the digital service has to report to the National Cyber and Information Security Agency (Sec. 8 para. 8 of the CSA). The type, category and assessment of the significance of the cyber security incident's impact, as well as the requisites and means of reporting the cyber security incident shall be set out in implementing legislation (Sec. 8 para. 7 of the CSA).
sanctions regime	Sec. 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 200,000, in particular in the following cases: (i) Administrators or operators of the information or communication systems of a critical information infrastructure, administrators or operators of significant information systems or administrators and operators of the basic service information systems do not introduce/carry out security measures or do not maintain security documentation. (ii) Providers of digital services do not introduce/carry out security measures. Sec. 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 40,000, in particular in the following cases: (i)Providers of electronic communication services, entities operating an electronic communication network or authorities or persons operating a significant network: – Do not fulfil their obligation imposed by the National Cyber and Information Security Agency contained in its decision or a measure of a general nature during a time of a cyber threat; or – Do not fulfil any of the obligations imposed through a corrective measure. (ii) Administrators and operators of the information or communication systems of critical information infrastructure or administrators or operators of significant information systems: – Do not report a cyber security incident; – Do not fulfil their obligation imposed by the National Cyber and Information Security Agency contained in its decision or a measure of a general nature; or – Do not hand over data, operating data and information. (iii)Administrators of the information or communication systems of critical information infrastructure or administrators of a significant information system do not notify the operator of the system. (iv) Administrators or operators of the information or communication systems of critical information infrastructure do not notify the entities operating an electronic communication network. (v) Operators of the information or communication systems of critical information infrastructure: – Do not fulfil their obligation imposed by the National Cyber and Information Security Agency contained in its decision;

– Do not hand over data, operating data and information (and they shall cease the operation); or
– Do not destroy copies of data, operating data and information.

(vi) Authorities or persons operating a significant network do not report a cyber security incident.

(vii) Administrators and operators of the basic service information systems:

– Do not report a cyber security incident;
– Do not fulfil its obligation to inform the public imposed by the National Cyber and Information Security Agency;
– Do not fulfil an obligation imposed by the National Cyber and Information Security Agency; or
– Do not fulfil an obligation imposed through a corrective measure.

(viii) Administrators or operators of the information or communication systems of a critical information infrastructure, administrators or operators of the significant information systems, administrators or operators of the basic service information systems and operators of basic services, who are public authorities, enter into a contract with a provider of cloud computing services and do not ensure that the contract complies with the requirements listed in the CSA (e.g. confidentiality agreement, customer audit rules).

(ix) Administrators or operators of the information or communication systems of critical information infrastructure do not fulfil their obligation to notify the public imposed by the National Cyber and Information Security Agency.

(x) Operators of basic services:

– Do not notify the administrators or providers of basic service information systems;
– Do not report a significant impact on the continuity of provision of the basic service whether or not caused by a cyber security incident; or
– Do not fulfil its obligation to inform the public imposed by the National Cyber and Information Security Agency.

(xi) Providers of digital services:

– Do not appoint their representative;
– Do not report a cyber security incident; or
– Do not fulfil its obligation to inform the public imposed by the National Cyber and Information Security Agency.

Sec. 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 8,000, in particular in the following case cases:

(i) Operators of the information or communication systems of critical information infrastructure:

– Do not hand over data, operating data and information (and they shall carry on with the operation); or
– Do not allow administrators to supervise the destruction of data, operating data and information.

Sec. 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 400, in particular in the following cases:

	(ii) Administrators or operators of the information or communication systems of critical information infrastructure or administrators or operators of significant information systems do not fulfil their obligation imposed by the National Cyber and Information Security Agency contained in its decision.
competent authorities	The National Cyber and Information Security Agency is the central authority competent for the cyber security on a national level (Sec. 21a of the CSA). National and government CERT are responsible for sharing information on national and international level regarding cyber security. Some of their other duties are to collect and evaluate cyber security incident reports from certain authorities and persons listed by the CSA (Sec. 17 and 20 of the CSA).
Jurisdictional applications	Providers of digital services are subject to the CSA if (i) their seat is located in the Czech Republic (Sec. 33 of the CSA); or (ii) their seat is located outside of the EU, but their representative is located in the Czech Republic (Sec. 3a of the CSA).
Remarks (if any)	The key requirements set out in the NIS Directive ("**Directive**") have already been part of the Czech Cybersecurity Act as of 1 January 2015. The changes that had to be made to Czech law resulting from the Directive were relatively small. On 28 May 2018, the new Decree on Cyber Security became effective. The Decree on Cyber Security No. 82/2018 Coll. ("**Decree**") repeals and replaces the current legislation enshrined in the Decree No. 314/2014 Coll., on Cyber Security. The Decree carries on from the repealed Decree No. 314/2014 Coll., but changes the order of succession of some sections, eliminates duplication in the text, and clarifies the differences between the obligations of Critical Information Infrastructure ("**CII**") and those of Significant Information Systems ("**SIS**"). The Decree also introduces new annexes which set out in more detail certain definitions, roles and obligations of obligated persons, i.a.: (i) Asset assessment rules (impact of intrusion of information security on individual assets) (ii) Risk assessment rules (impact, threat and vulnerability assessment) (iii) Overview of vulnerabilities and threats (iv) Rules for data erasure and technical media disposal methods (v) Content rules regarding contracts concluded with significant suppliers of obligated persons (vi) Requirements for individual security roles within the Cyber Security Committee and their competencies

Denmark

Current status of implementation	The NIS directive was implemented in Danish law in May 2018 by Act No. 436 of 8 May 2018 (the "**NIS Act**"). The implementation of the NIS directive in Denmark has been set out in the NIS Act as a framework legislation with sector specific executive orders and acts determining OES, reporting obligations, sanctions etc. for each sector. The sectors are i) digital services ii) telecom iii) utilities, iv) transportation, v) finance, and vi) healthcare. Generally, the sectors have taken quite different approaches to the extent of regulation, and the requirements within the different sectors vary highly.
Implementation Act	• Act No. 436 of 08/05/2018 on network and information security for domain name systems and certain digital services (NIS Act), Ministry of Commerce • Act No. 437 of 08/05/2018 on security in network and information systems for operators of major internet exchange points, etc., Ministry of Defense • Act No. 440 of 08/05/2018 on safety requirements for network and information systems in the health sector, Ministry of Health and Elderly • Act No. 441 of 08/05/2018 on Security in Network and Information Systems in the Transport Sector, Ministry of Transport, Building and Housing • Executive order No. 452 of 08/05/2018 on Network and Information Security for Certain Digital Services, Ministry of Commerce • Executive order No. 453 of 08/05/2018 on Security in Network and Information Systems for Operators of Essential Services in the Domain Name Area, Ministry of Commerce • Executive order No. 454 of 08/05/2018 on Security in Network and Information Systems for Operators of Essential Internet Exchange Points, Ministry of Defense • Executive order No. 457 of 09/05/2018: Declaration of Event Reporting for Operators of Essential Services, Ministry of Commerce • Executive order No. 461 of 09/05/2018 amending the Executive Order on Management and Management of Banks, etc., Ministry of Commerce • Executive order No. 424 of 25/04/2018 on Preparedness for the Oil Sector, Ministry of Energy, Supply and Climate • Executive order No. 429 of 04/05/2018 on Requirements for Safety in Networks and Information Systems of Certain Water Supply, Ministry of Environment and Food • Executive order No. 820 of 14/08/2019 on IT Preparedness for Electricity and Natural Gas Sectors, Ministry of Energy, Supply and Climate
Determination of operators of essential services (Art. 5 NIS)	Each sector specific executive order, acts, and the NIS Act itself set out the determination of OES within that specific sector.
reporting obligations	Each sector specific executive order/act set out their own reporting scheme.

sanctions regime	Breaches will generally be sanctioned by way of orders for compliance and ultimately fines. Denmark has however not implemented any specific fine levels, and generally the Danish level of fines is very low compared to, what we see in the rest of Europe. There could however be other indirect sanctions, as the supervision of compliance with NIS is also connected to the general compliance supervision under some of the regulated or even license-based sectors, and non-compliance with NIS could in some of those license-based sectors (such as within utilities and financial services) be a risk for such operating license.
competent authorities	• Ministry of Transport, Building and Housing • Ministry of Defense • Ministry of Health and Elderly • Ministry of Commerce • Ministry of Environment and Food • Ministry of Energy, Supply and Climate
Jurisdictional applications	Operators of digital services are generally subject to Danish law, if they are established in Denmark. However, each act will regulate this in detail.
Remarks (if any)	The Danish Government concluded in January 2019 a national strategy for cyber and information security which aims at protecting the most vital sectors against cyber threats. Each of the sectors has also concluded its own strategy for the specific threats and related initiatives in relation to cyber and information security within its sector. The strategies cover the period from 2018-2021 and includes overall initiatives to be further specified through workshops etc. The strategies must expect to include new legislation, agreed documents, specifically identified threats and other relevant sources for information on the NIS implementation in Denmark.

Estonia

Current status of implementation	The NIS Directive has been implemented on 23 May 2018.
Implementation Act	The directive is implemented by the Cybersecurity Act ("**CSA**").

Determination of operators of essential services (Art. 5 NIS)	The CSA uses the term "service provider". Service providers include providers of "vital services" as specified in the current Emergency Act and the following categories of service providers: (i) certain railway companies, (ii) aviation (international aerodrome operators, providers of air traffic control), (iii) certain port operators, (iv) communications companies providing cable service to more than 10,000 end users; (v) owners of regional hospitals and central hospitals of the hospital network upon providing in-patient specialised medical care and ambulance crews upon providing emergency care; (vi) family physician upon providing general medical care (vii) certain domain name register administrators, (viii) providers of critical communications, maritime radio communications and operational communications network services , (ix) Estonian Public Broadcasting. The CSA specifies, that only such 'service providers' (as defined above) who operate in sectors mentioned in Annex II of the NIS directive, are regarded as an operator of essential services. Estonian legislator has referred to the existing term "vital service" from the Emergency Act. According to the definition in the Emergency Act, vital service is a service that has an overwhelming impact on the functioning of society and the interruption of which is an immediate threat to the life or health of people or to the operation of another vital service or service of general interest. A vital service is regarded in its entirety together with a building, piece of equipment, staff, reserves and other similar facilities indispensable to the operation of the vital service. There are 14 categories of vital services listed by the Emergency Act, but the list of providers of the vital services is not publicly available. The CSA specifies, that only such 'service providers' (as defined above) who operate in sectors mentioned in Annex II of the NIS directive, are regarded as an operator of essential services.
reporting obligations	Service providers must notify immediately, but no later than 24 hours (from becoming aware of an incident), the Information System Authority (“**ISA**”) about the cyber incidents that have a significant impact on the security of the system or the continuity of the service (including incidents a significant impact of which is not obvious but can be reasonably presumed). In addition, within a reasonable period of time, the service provider must notify persons possibly affected by the cyber incident with a significant impact or the public if the persons affected cannot be notified individually. Providers of digital services notify immediately the competent authority or the computer security incident response team (“**CSIRT**”) of the cyber incidents that have a significant effect on the digital service. The term "significant" is in particular determined by the implementing acts pursuant to Art. 16 para. 8 of the NIS Directive. The notice must allow the competent authority or CSIRT to determine the international effect of the incident. If the incident has a significant effect on the continuity of the digital service in another Member State, the competent authority will notify the affected Member State. No notification is required if the digital service provider has no sufficient access to information that are necessary to evaluate the impact and severity of the security incident.
sanctions regime	Sec 18 of the CSA provides for fines in misdemeanor procedure of up to EUR 20,000, in case of not following requirements imposed on implementing security measures as set out in Subsec. 7 para. 1-3 of the CSA.
competent authorities	The Estonian Information System Authority is the competent authority referred to in Art. 8 para. 1 of Directive, the single contact point referred to in Art. 8 para. 3 and the computer incident response team referred to in Art. 9 para. 1.

Jurisdictional applications	The service providers are generally subject to Estonian law based on the principle of territorial applicability of the CSA. Special rules apply to reporting by providers of digital services. A report must be submitted to the competent authority or CSIRT of the relevant member state where (i) the digital services provider is founded; (ii) the parent company of the group is founded in the case of a group or (iii), the representative appointed by an economic operator from a third country is located. State supervision over such digital service providers will only be exercised (i) if the digital services provider is established in Estonia; (ii) where the parent company is established in Estonia in case of a group of undertakings or (iii) if providers of digital services from third countries have appointed a representative in Estonia.
Remarks (if any)	N/A

Finland

Current status of implementation	The NIS Directive has been implemented in Finland in sector specific laws by including the necessary amendments in various already existing acts. Those amendments implementing the NIS Directive came into force on 9 May 2018.
Implementation Act	The necessary changes were made to existing sector specific acts. Altogether twelve Finnish acts were modified: the Act on Electronic Communications Services, the Aviation Act, the Railway Act, the Vessel Traffic Service Act, the Act on the Safety and the Supervision of Security Operations of Certain Vessels and Ports Servicing them, the Act on Transport Services, the Electricity Market Act, the Natural Gas Market Act, the Act on the Supervision of Electricity and Gas Markets, the Water Services Act, the Act on the Financial Supervision and the Act on the National Supervisory Authority for Welfare and Health.
Determination of operators of essential services (Art. 5 NIS)	In the government proposal it is said that network and information security obligations should be applied to a) online marketplaces, search engines and cloud providers and other digital infrastructure, b) air navigation service providers and essential airports, c) state rail network and train traffic control service, d) vessel traffic service providers and essential ports, e) smart transport service providers, f) electricity and gas transmission grid operators, g) certain water management facilities, h) credit institutions and stock exchange operators and i) electronic processing of healthcare customer data. Further specifications can be found in the sector specific laws where each entity is regulated, and in the government proposal where each of these sectors is discussed in more detail. In practice, the determination will in many cases require case-by-case consideration from companies.
reporting obligations	Operators of essential services must notify the competent authority of any significant security breach without delay. The competent authority may require the service operator to also notify the public about such disruption.

sanctions regime	No proposed new sanctions; existing sanction regimes provided in the sector specific laws may apply.
competent authorities	Sector specific authorities have competence for the supervision: The Energy Authority, the Financial Supervisory Authority, the National Supervisory Authority for Welfare and Health, the Centre for Economic Development, Transport and the Environment and the Finnish Transport and Communications Agency. The Finnish Transport and Communications Agency ("Traficom") acts as designated contact point and is responsible for cross-border cooperation with other member states.
Jurisdictional applications	Not specified in the proposed modifications. The existing provisions on jurisdiction in the sector specific laws apply.
Remarks (if any)	N/A

France

Current status of implementation	The NIS Directive has been fully implemented into the French legal system. Several texts have been adopted: • French NIS Directive Implementation Act which came into effect on 28 February 2018. • A decree which came into effect on 26 May 2018. • A ministerial order which came into effect on 27 June 2018. • A ministerial order which came into effect on 4 August 2018. • A ministerial order which came into effect on 1 October 2018.

Implementation Act	An act, a decree and several ministerial orders have been adopted in order to implement the NIS Directive into French national law. Act n° 2018-133 of 26 February 2018 relating to implementation of EU provisions in the field of security ("**Act**"). Decree n°2018-384 of 23 May 2018 relating to security of networks and information systems of essential service operators and digital service providers ("**Decree**"). Ministerial order of 13 June 2018 setting the conditions of the statements provided in Decree n° 2018-384 of 23 May 2018. Ministerial order of 1 August 2018 on the cost of an audit carried out by the National Agency for the Security of Information Systems pursuant to Art. 8 and 14 of Act n° 2018-133 of 26 February 2018. Ministerial order of 14 September 2018 setting the security rules and deadlines mentioned in Art. 10 of Decree n° 2018-384 of 23 May 2018.
Determination of operators of essential services (Art. 5 NIS)	A ministerial decree dated 23 May 2018 identified the following sectors as essential services: (i) Civil activities of the State, (ii) Judicial activities, (iii) Military activities of the State, (iv) Food, (v) Electronic, audiovisual and information communications, (vi) Energy, (vii) Space and research, (viii) Finance, (ix) Water management, (x) Industry, (xi) Health, and (xii) Transport. Art. 4 of the Act provides that the list of the essential services shall be provided by a decree of the Conseil d'Etat. This list of essential services does not replace the one provided by the decree of June 2006 according to Art. 5 Sec. 2 of the bill. Art. 2 of the decree provides that the operators of essential services ("**OES**") shall be designated according to the following criteria: • The number of users dependent on the service; • The dependence of the other sectors of activity listed in the schedule to this decree on the service; • The consequences that an incident could have, in terms of gravity and duration, on the functioning of the economy or society or on public safety; • The operator's market share; • The geographical scope with regard to the area likely to be affected by an incident; • The importance of the operator to ensure an adequate level of service, taking into account the availability of alternative means for the provision of the service; • Where applicable, sectoral factors. According to Art. 3 of the Decree the operators shall be designated by an order of the Prime Minister, if the operators provide an essential service for several Member States that appointment shall be preceded by a consultation with the relevant Member States. The operators shall have one month from the date of the notification of their appointment to present their observation.

	The operators shall appoint a representative that will be the point of contact with the National Agency for the Security of Information Systems (French national authority, "**ANISSI**"). According to the ANSSI, by November 2018 (deadline set by the NIS Directive) France had already identified 122 EOS. This number, which is not definitive, will increase in the future. A significant number of identifications, in the order of a few hundred, are already under investigation.
reporting obligations	According to Art. 7 of the Act, operators of essential services must report "without undue delay" to the ANSSI any incident significantly impacting the security of the network and information systems. Pursuant to Art. 3 of the ministerial order of 13 June 2018, to report incidents, OES must provide the national supervisory authority, by electronic means or by mail, with an incident reporting form available on the authority's website. This form includes information on the reporter, the network and information system affected by the incident, the consequences of the incident on the essential services concerned, the type of incident, its causes and the measures taken by the operator to respond to it. Reporting must be carried out as soon as the operator becomes aware of an incident, regardless of whether all the information is available. Digital Service Providers: Pursuant to Art. 13 of the Act, Art. 20 of the Decree and Art. 4 of the ministerial order of 13 June 2018, digital service providers shall also report security incidents in the same conditions that the OES. List of the networks and information systems: Pursuant to Art. 7 and 8 of the Decree, the operators shall disclose within three months from the date of their appointment the list of the networks and information systems listed in the Act. The operators shall then send an annual update of the list to the ANSSI. The operators also need to keep this information at the disposal of the ANSSI in case of inspection. Pursuant to Art. 3 of the ministerial order, to report incidents, operators of essential services must provide the national supervisory authority with the list of networks and information systems and the declaration form available on the Agency's website, duly completed, by electronic means or by mail. This form includes information on the reporter, the description of the network and information system, its technical characteristics, its operation and its security. The same conditions apply regarding the annual updating obligation.

sanctions regime	At the moment, Art. 9 of the Act provides for three criminal fines for the operators of essential services: (i) directors that do not comply with the security rules even after the timeline specified in a formal demand issued by the ANSSI shall be punishable with a fine of EUR 100,000; (ii) directors that do not comply with their reporting obligation in case of an incident shall be punishable with a fine of EUR 75,000; (iii) directors that obstruct an investigation shall be punishable with a fine of EUR 125,000. Art. 15 of the Act provides for three criminal fines for the digital service providers: (i) directors that do not comply with the security rules even after the timeline specified in a formal demand issued by the ANSSI shall be punishable with a fine of EUR 75,000; (ii) directors that do not comply with their reporting obligation in case of an incident shall be punishable with a fine of EUR 50,000; (iii) directors that obstruct an investigation shall be punishable with a fine of EUR 100,000.
competent authorities	Art. 8 of the Act provides that ANISSI is competent to investigate and to issue formal demands asking to comply with the set of security rules.
Jurisdictional applications	The Act only specifies the jurisdiction for the digital service providers. French law shall be applicable to digital service providers providing services in the EU and (a) having their registered office or their principal place of business in France, or (b) having an authorised representative in France (Art. 11).
Remarks (if any)	N/A

Germany

Current status of implementation	The German NIS Directive Implementation Act ("**Implementation Act**") came into effect on 30 June 2017. The provisions on providers of digital services are applicable as of 10 May 2018.
Implementation Act	The Implementation Act (published in the Federal Law Gazette, BGBl. I 2017 of 29 June 2017, p. 1885) has amended the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz),* "**FOIS Act**"), the Atomic Energy Act (*Atomgesetz*), the Energy Industry Act (*Energiewirtschaftsgesetz*), the Social Security Code V (*Sozialgesetzbuch V*), and the Telecommunication Act (*Telekommunikationsgesetz*). Due to the amendment of the FOIS Act by the Implementation Act, the FOIS Act now in particular contains a definition of providers of digital services and sets out specific requirements for these providers in connection with security and reporting. The key requirements set out in the NIS Directive ("**Directive**") had, however, already been part of the German IT Security Act ("**ITSA**") dated 17 July 2015 which amended the FOIS Act before the Implementation Act. Accordingly, the ITSA had a front-runner role for the Directive. In light of the ITSA, the changes required to German law resulting from the Directive were relatively small.

Determination of operators of essential services (Art. 5 NIS)	In accordance with Art. 5 of the NIS Directive, the German regulator has specified the criteria to identify operators of the following essential services: a) Finance and insurance, b) health, c) transportation and traffic (all identified as per ordinance of June 2017), d) energy, e) IT and telecommunication, f) water, g) food (all identified as per ordinance of May 2016).
reporting obligations	Both operators of critical infrastructures as well as providers of digital services have reporting obligations under certain circumstances: Operators of critical infrastructures must immediately report to the Federal Office for Information Security (FOIS) (i) disruptions [and (ii) significant disruptions] of the availability, integrity, authenticity and confidentiality of their IT systems that have led [might lead] to a failure or significant impairment of the operability of the critical infrastructure (Sec. 8b para. 4 of the FOIS Act). Providers of digital services must immediately report to the FOIS any security incident that has a significant impact on the provision of the digital service provided the EU (Sec. 8c para. 3 of the FOIS Act). The term "significant" is defined in the implementing acts pursuant to Art. 16 para. 8 of NIS Directive. No report is required if the provider does not have sufficient access to information as it may be necessary to evaluate the impact of the security incident.
sanctions regime	Sec. 14 of the FOIS Act provides for administrative fines of up to EUR 50,000, particularly in the following cases: Operators of critical infrastructures wilfully or negligently • fail to properly implement appropriate technical and organisational measures to prevent disruptions of availability etc. in a timely manner; • fail to properly designate a point of contact in a timely manner; • fail to properly report as described above. Providers of digital services wilfully or negligently • fail to implement appropriate and proportionate technical and organisational measures to tackle risks for the security of the network and information systems; • fail to properly report as described above. In case of infringement of an enforceable ruling, the FOIS Act provides for administrative fines of up to EUR 100,000. Infringements of providers of digital services are only sanctioned by the German authorities, if the provider (i) has no main establishment in another EU member state, or (ii) as far as the provider has no establishment in another EU member state, the provider has appointed a representative there and offers the digital services in that EU member state. It should be noted that the above-mentioned administrative fines in case of a violation of the obligation to implement appropriate technical and organisational measures run in parallel to the administrative fines which can be imposed under the General Data Protection Regulation (EU) 2016/679 ("**GDPR**").

	Further, the Implementation Act amends the sanction rules under the Atomic Energy Act, Energy Industry Act, Social Security Code V and Telecommunication Act, whilst the administrative fines remain as before: • up to EUR 50,000 under the Atomic Energy Act; • up to EUR 5,000,000, or in specific cases up to 10% of the total worldwide annual turnover of the preceding financial year, under the Energy Industry Act; • up to EUR 50,000 under the Social Security Code V; and • up to EUR 500,000 under the Telecommunication Act.
competent authorities	The FOIS is the competent authority for information security at a national level, including the prosecution and control of administrative offences (Sec. 1 and 14 para. 3 of the FOIS Act). The FOIS operates under the authority of the German Federal Ministry of the Interior.
Jurisdictional applications	Operators of critical infrastructure are subject to German law if the infrastructure is located in Germany. The reporting obligations do not apply to providers of digital services that have their main establishment in another EU member state or have appointed a representative in another EU member state, in which they offer the digital services. Consequently, other obligations (e.g. to implement appropriate TOMs) apply to providers even though their main establishment is outside of Germany (provided, of course, that information security in Germany is concerned, see "competent authorities").
Remarks (if any)	A new draft bill, which would (primarily) change the FOIS Act (*Zweites IT-Sicherheitsgesetz – IT-SiG 2.0, "***FOIS Act 2.0**") is currently being discussed in Germany. The draft bill is aiming at broadening the scope of application of the FOIS Act and to entrust the FOIS with additional powers. With respect to the scope of application of the FOIS Act, according to the information available so far, it is planned to expand the scope to manufacturers and suppliers of the companies which are qualified as operators of critical infrastructure (so called “vertical expansion”) – the objective is to secure the entire supply chain. In addition, further sectors (e.g. chemical and automotive industries) should fall under the scope of this Act and should be covered by the term of operators of critical infrastructure (so-called “horizontal expansion”). At the same time the thresholds for the assessment of whether an entity operates a critical infrastructure shall get reduced. Finally, it is planned to grant the FOIS consumer protection powers (market observation of networked consumer goods, trend and development analysis, security evaluation, etc.) and to extend its warning and investigation powers.

Greece

Current status of implementation	The NIS Directive has been implemented in Greece in December 2018.
Implementation Act	Law 4577/2018 has implemented the NIS Directive (the "**Law**").
Determination of operators of essential services (Art. 5 NIS)	For an operator to be considered as an Operator of Essential Services ("**OES**") it must meet the following criteria provided in Art. 4, para. 2 of the Law (which corresponds to Art. 5 para.2 of the NIS Directive): a. It must provide a service which is essential for the maintenance of critical societal and/or economic activities; b. The offered service should be based on network and information systems and c. An incident would have significant disruptive effects on the provision of that service, as defined in Art. 5 of the Law (corresponding to Art. 6 of the NIS Directive). The National Cyber-Security Authority in cooperation with the relevant sectorial supervisory or regulatory authorities and other national authorities will publish a catalogue with the essential services and their operators as well as determine the criteria to define an incident as having significant disruptive effects. Under the frame of the Law on 2019 was issued No. 1027/4 October 2019 Ministerial Decision on the implementation measures of the Law ("**NIS Implementation Decision**"). The NIS Implementation Decision lays down in Art. 16 the methodology and criteria for determining the OES.
reporting obligations	Providers of digital services ("**DSP**") must report to the National Cyber Security Authority without any undue delay any security incident with an impact that is significant to the provision of digital services as they are described in Annex II to the Law and provided within the European Union.
sanctions regime	Following the opinion of the National Cybersecurity Authority, the Minister of Digital Policy, Telecommunications and Information, imposes the below sanctions in case of violation of the provisions of the Law: • A fine from EUR 15,000 up to EUR 200,000 in the event of no notification / delay of notification. • A fine from EUR 50,000 up to EUR 200,000 in the event of failure to take appropriate organizational / technical measures to manage the risks to network and system security. • A fine from EUR 50,000 to 200,000 in case of non-provision or unjustified delay in the provision of information, if requested by the National Cybersecurity Authority. Procedures and criteria regarding the imposition of fines, including other sanctions such as reprimands and warnings, are provided for in Art. 13-15 of NIS Implementation Decision.
competent authorities	Competent Authority is the National Cybersecurity Authority, which belongs to the Minister of Digital Policy, Telecommunications and Information.

Jurisdictional applications	Art. 13 of the Law on jurisdiction and territoriality provides that the DSP is subject to the jurisdiction of the Greek Authorities when it has its main establishment in Greece. The DSP is considered to have its main establishment in Greece when its head offices are also situated in Greece. Furthermore, according to the Explanatory Report, accompanying the Law, a DSP shall be deemed to have its main establishment wherever it has its head office and therefore it is under the jurisdiction of the Member State where it (head office) lies. In addition, the DSP which is not established in the EU but provides services mentioned in Appendix II of the Law, within the EU must designate a representative based in a EU member state where its services are provided. The above DSPs are considered to be established in the jurisdiction of the representative.
Remarks (if any)	N/A

Hungary

Current status of implementation	The provisions of the NIS Directive have been implemented into the Hungarian legal system.
Implementation Act	The main implementing legislation are the following: **1. The legislation implementing the obligations of the digital service providers:** • Act 134 of 2017 on modifying certain interior related tasks and corresponding laws: modified Act CVIII of 2001 on Electronic Commerce and Information Society Services • Government Decree No. 270/2018. (XII. 20.) on the supervision of the electronic information security of information society services, and the procedural regime regarding security incidents. **2. The legislation implementing the obligations of the operators of essential services:** • Act 134 of 2017 on modifying certain interior related tasks and corresponding laws: modified Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities • Government Decree No. 394/2017 (XII.13) on modifying government decrees related to Act 134 of 2017 on modifying certain interior related tasks and corresponding laws: modified Government Decree No. 65/2013. (III. 8.) on the enforcement of Act CLXVI of 2012 on critical systems, and facilities • Government Decree No. 271/2018. (XII. 20.) on the powers and responsibilities of security incident management centres and on the management and technical examination of security incidents, and vulnerability tests.
Determination of operators of essential services (Art. 5 NIS)	In accordance with Art. 5 of the NIS Directive, the Hungarian regulator has identified the following sectors: (i) energy, (ii) transportation, (iii) health, (iv) finance, (v) info communication technologies, (vi) water.
reporting obligations	Providers of digital services ("**DSP**") must report to the Special Service for National Security (more specifically at the department 'National Cyber Security Institute') without any undue delay any security incident with an impact that is significant to the provision of digital services as they are described in Annex II to the Law and provided within the European Union.

	Operators of essential services must report to the Special Service for National Security, National Cyber Security Institute, without undue delay any security incident with an impact that is significant to the continuity of their services (Art 9 of the Government Decree No. 271/2018.).
sanctions regime	Annex 1 of the Government Decree 187/2015 (VII.13) specifies administrative fines to providers of Digital Services in case of breaching the obligations specified by the Annex of the Government Decree including the failure to report significant incidents. The amount of the statutory fines is rather low compared to other EU member states and depends on the type of breach. The amount of the administrative fine ranges between HUF 50,000 (approx. EUR 165) and HUF 5,000,000 (approx EUR 16,500). Sec. 9 (2) of Government Decree 65/2013 (III.8) specifies the amount of administrative fines that may be imposed on operators of essential services for breach of any obligations defined by the applicable laws. The amount of the administrative fine ranges between HUF 100,000 (approx. EUR 330) and HUF 3,000,000 (approx. EUR 9,900).
competent authorities	The incident management authority appointed by the Hungarian Government is the Special Service for National Security.
Jurisdictional applications	The provisions of Act 108 of 2001 on e-commerce and information society services (the act applies to Digital Service providers, "**E-commerce Act**") states that the E-commerce Act applies to Digital Services offered from or to the territory of Hungary. However, certain provisions of the E-commerce Act and other applicable laws are not applicable to providers (i) that are registered in the territory of another EEA member state and (ii) offer Digital Services to the territory of Hungary. Such non-applicable provisions include all general and special requirements with respect to commencing and conducting commercial activity on the territory of Hungary. The provisions of the E-commerce Act regarding providers of Digital Services are not applicable to micro and small enterprises.
Remarks (if any)	N/A

Ireland

Current status of implementation	The NIS Directive was signed into Irish law on 18 September 2018.
Implementation Act	The NIS Directive was transposed into Irish law by way of Statutory Instrument No. 360 of 2018 - European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 (S.I. 360/2018).

Determination of operators of essential services (Art. 5 NIS)	A competent authority shall designate a person as an operator of essential services in respect of an essential service where that competent authority is satisfied that: (i) The person provides the essential service in Ireland; (ii) The person has an establishment in Ireland; (iii) The person is a person of one of these types: Electricity undertakings, Distribution system operators, Transmission system operator, Electricity transmission system operators, Operators of oil transmission pipelines, Operators of oil production, refining and treatment facilities, storage and transmission, Supply undertakings, Distribution system operators, Transmission system operators, Storage system operators, LNG system operators, Natural gas undertakings, Operators of natural gas refining and treatment facilities, Air carriers, Airport managing bodies, Airports including the core airports and entities operating ancillary installations contained within airports, Traffic management control operators providing air traffic control (ATC) services, Infrastructure managers, Railway undertakings including operators of service facilities, Inland, sea and coastal passenger and freight water transport companies not including the individual vessels operated by those companies, Managing bodies of ports including their port facilities and entities operating works and equipment contained within ports, Operators of vessel traffic services, Road authorities, Operators of Intelligent Transport Systems, Credit institutions, Operators of trading venues, Central counterparties (CCPs), Healthcare providers, Suppliers and distributors of water intended for human consumption but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services, IXPs, DNS service providers, TLD name registries; (iv) The sector and, where appropriate, subsector in which the essential service is provided are the following sectors/subsectors: energy (subsectors: electricity, oil, gas), transport (subsectors: air transport, rail transport, water transport, road transport), banking, financial market infrastructures, health sector (subsector: health care settings including hospitals and private clinics), drinking water supply and distribution, digital infrastructure; (v) The provision by the person of the essential service depends on network and information systems; and (vi) An incident affecting the provision by the person of the essential service would have significant disruptive effects on the provision of that service in Ireland.
reporting obligations	Operators of Essential Services are required to report incidents which fall under the scope of the NIS Directive. A reportable incident is any incident which has a significant impact on the continuity of an essential service which an Operator of Essential Services provides. In this context, significant impact means that the essential service provided by the Operator of Essential Services must be interrupted and must not be operational for a given period of time. A reportable incident is determined using the significant disruptive effect parameters contained in the Directive and outlined in the Incident Reporting Guidelines which will be published shortly. In addition, under S.I 360/2018, the Minister for Communications, Climate Action and Environment shall in each year submit reports to the Co-operation Group in relation to incident notifications made to the CSIRT (the unit of the Department of Communications, Climate Action and Environment known as the Computer Security Incident Response Team), including the number of notifications, the nature of the notified incidents and he actions taken.

sanctions regime	A person guilty of an offence under the S.I 360/2018 is liable (a) on summary conviction, to a class A fine*, or (b) on conviction on indictment, to a fine not exceeding EUR 50,000 in case of an individual and EUR 500,000 in case of a person other than an individual. Where a person is convicted of an offence under the S.I 360/2018, the Court shall, unless it is satisfied that there are special and substantial reasons for not doing so, order the person to pay to the prosecutor a sum equal to the costs and expenses, measured by the court, reasonably incurred by the prosecutor in relation to the prosecution of the offence. Such order for costs and expenses shall be in addition to and not instead of any fine or penalty the court may impose. * Class A fine is a fine not exceeding EUR 5,000 but greater than EUR 4,000.
competent authorities	The competent authority for operators of essential services is the Minister for Communications, Climate Action and Environment. The Central Bank of Ireland is the competent authority for operators of essential services only for the following sectors: banking and financial market infrastructure. The competent authority for digital service providers is the Minister for Communications, Climate Action and Environment.
Jurisdictional applications	N/A
Remarks (if any)	The Minister of Communications, Climate and Environment published a guidance note on 27 September 2019 entitled "**NIS Compliance Security Guidelines for OES**". This document establishes a set of Guidelines designed to assist Operators of Essential Services in meeting their network and information system security incident reporting requirements.

Italy

Current status of implementation	The NIS directive has been implemented by the Legislative Decree no. 65/2018, published on the Official Gazette of the Italian Republic on 9 June 2018 and entered into force on 26 June 2018.
Implementation Act	The Legislative Decree no. 65/2018.
Determination of operators of essential services (Art. 5 NIS)	The Italian NIS Authorities identified 465 public and private entities as Operators of Essential Services, operating in the sectors of energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, and digital infrastructure. The name of these operators was not disclosed due to national security concerns. On 31 January 2019, the identified operators of essential services have been confidentially informed to be in the related list and to be subject to the NIS provisions, monitored by the NIS Authorities.
reporting obligations	Operators of essential services and digital service providers must immediately notify the Italian CSIRT and for information the competent NIS Authority of incidents which have a significant impact on the provision of the essential services.

sanctions regime	In Italy, according to the scheme of the Legislative Decree, operators of essential services and digital service providers which will be non-compliant with the regulations will be subject to an administrative fine ranging from EUR 12,000 to a maximum of EUR 150,000.
competent authorities	The Italian Prime Ministry is the subject in charge for the general policy of the government and of the Security Information System of the Republic for the purpose of protecting national security in the cyber space. Please find below other bodies for cybersecurity mentioned in the Directive for the cybersecurity protection and in the scheme of legislative decree: • The DIS (the "Department of the Information for Security") that has the function of coordinate the activities of informatics research finalized to enhance the cybersecurity protection and the national informational security; • The CISR (the Ministerial Committee for Security of the Republic) that has a consultancy function and provides practical activities in order to implement the National Plan for cybersecurity; • MISE, the Ministry of Economic Development; • The Digital Agency for Italy; • Both the Ministries of Defence and the Interior. • The Cybernetic Security Office, a body of DIS that supports and collaborates with the Prime Ministry and CISR for any cybernetic crisis (please see definition below). • Ministry of Economic Development, Ministry of Infrastructure and Transport, Ministry of Economics, Ministry of Health and Ministry of Environment has been indicated as Competent NIS Authorities, each for the respective sector of the operators of essential services.
Jurisdictional applications	Operators of essential services are subject to Italian law if its principal place of operation is located in Italy. The reporting obligations do not apply to providers of digital services that have their main establishment in another EU member state or have appointed a representative in another EU member state, in which they offer the digital services.
Remarks (if any)	Each Competent NIS Authority has issued specific guidelines for the policies to be implemented by the Operators of Essential Services of their respective sectors in order to be compliant with the NIS Directive. Accordingly, based on a proactive and strategic approach and despite the specific technology implementation of the Operator, 5 compliance steps have been identified to be included in a dedicated NIS policy in order to manage the cybersecurity risks. The 5 steps are: (i) to identify, (ii) to protect, (ii) to detect, (iii) to respond and (iv) to recover; the comprehensive NIS policy will have to provide for specific sub-policies to be created for each area, considering the type of business and the risk appetite of the specific Operator. Moreover, the Operators of Essential Services are required to be compliant with these guidelines relatively soon, i.e. by April / May 2020, reaching at least the first of three levels of compliance. In fact, on the basis of the maturity and complexity of the measures implemented by each Operator, the guidelines provide for a 3 levels scale of compliance: M1 Responsibility and Risk Acknowledgment, M2 Basic Organization and M3 Completely Organized. All the relevant activities included in each of the abovementioned areas in relation to such levels have been described in detail in the guidelines. In addition, 2 new positions are requested in the corporate structure of the Operator of Essential Services such as the NIS Referent, a contact point with the NIS Authority and the NIS Representative, responsible for the implementation and management of the new

	cybersecurity policies.

Latvia

Current status of implementation	The NIS Directive has been implemented as of January 2019.
Implementation Act	Implementation consisted of amendments to the 2010 Law On the Security of Information Technologies as well as drafting separate Cabinet regulations (Cabinet Regulation No. 15 of 15 January 2019 on materiality criteria for security incident, information procedure and content of report, and Cabinet Regulation No. 43 of 15 January 2019 on the conditions for determining the materially disruptive effect of a security incident and the procedures for granting, reviewing, and terminating the status of the essential service provider and the essential service).
Determination of operators of essential services (Art. 5 NIS)	The amendments to the Law On the Security of Information Technologies and the Cabinet Regulation No. 43 stipulate the criteria for an essential service provider and an essential service. It provides that: (i) the service provider is a state or local government institution, or a private legal entity; (ii) it carries out an economic activity in Latvia; (iii) it provides a service in the European Union in a particular sector; (iv) the service provided by it is essential for social or economic activities; (v) the providing of this service is dependent on network and information systems; (vi) a safety incident may cause a significant interference with the providing of the service.
reporting obligations	Before implementation, the Law On the Security of Information Technologies already provided for reporting obligations to state and local government institutions, the owner of the critical infrastructure of information technology, or the legal possessor in the event of a security incident, while to other companies reporting was left to discretion. The amendments to the law and Cabinet Regulation No. 15 now additionally stipulate that an essential service provider only reports a security incident that has a significant impact on the continuity of the underlying service, but a digital service provider reports a security incident that has a significant impact on the providing of the service. The Cabinet of Ministers determines the criteria for materiality of a security incident both to essential service providers and digital service providers.
sanctions regime	The Committee has the right to enforce its decision in accordance with the Administrative Procedure Law. The Committee is entitled to prepare a warning about the enforcement of the decision, which includes an indication of the applicable means of enforcement, such as pecuniary penalties. With the enforcement of the decision, Art. 21 of the NIS Directive on sanctions is being implemented.
competent authorities	Committee is defined as the competent authority under the NIS directive. In relation to it, the Law On the Security of Information Technologies was supplemented by an article defining the tasks and rights of the Committee as a competent authority. For example, the committee cooperates with sectoral ministries in the process of identifying essential service and essential service providers, and prepares a list of essential services and essential service providers; once every two years it sends information to the European Commission on the identification of essential service providers in Latvia, a list of essential services identified, the number of essential service providers, and the identifying factors of significant security incidents, as they vary from country to country.

Jurisdictional applications	In case that a digital service provider or its representative has its legal seat or is providing its services in Latvia, the Latvian law will apply.
Remarks (if any)	N/A

Lithuania

Current status of implementation	The NIS Directive has been implemented as of July 2018.
Implementation Act	NIS directive has been implemented into Lithuanian law primarily by amendments to the Law on Cyber Security and the Code of Administrative Offenses.
Determination of operators of essential services (Art. 5 NIS)	Art. 2 para. 5 of the Law on Cyber Security defines Operator of Essential Information Infrastructure as a person managing the essential information infrastructure. According to Art. 2 para. 4, essential information infrastructure is a communications or information system or part of it, or a group of such systems the occurrence of a cyber incident in which might have a significant negative impact on the national security, economy of the country, and interests of the state and the public. According to the Methodology for Identification of Essential Information Infrastructure approved by the Government of the Republic of Lithuania ("**Methodology**"), the essential information infrastructure is determined by the following criteria: (i) an infrastructure object is of "essential significance", i.e. ensures the provision of essential service (see the paragraph below); (ii) the provision of that service depends on information infrastructure; (iii) a cyber incident in that information infrastructure might have disruptive effects on the provision of the service; (iv) in the event of disruption of the information infrastructure, there are no alternatives to ensure the continuity of the service. In order to assess whether a particular infrastructure object is of "essential significance" (i.e. whether the operator of this object is the "operator of essential services"), the following criteria apply: (i) the infrastructure object is used to provide an essential service (the explicit list of essential services is provided in Annex 1 of the Methodology); (ii) destruction, damage or disruption of the object would have negative impact on the provision of essential service; (iii) destruction, damage or disruption of the object would have negative impact on the national security, economy of the country, or interests of the state or the public.

reporting obligations	Art. 11 para. 1 sentence 3 of the Law on Cyber Security entails that cyber security entities (entities which control and/or manage information resources of the state, operators of essential information infrastructure, service providers of public communications networks and/or public digital communication services, providers of digital information hosting services and providers of digital services) must notify the National Cyber Security Centre of cyber incidents which occur in communications and information systems controlled and/or managed by them as well as of applied cyber incident management measures in accordance with the procedure laid down in the National Cyber Incidents Management Plan. Art. 11 para. 1 sentence 4 of the Law on Cyber Security obliges cyber security entities to provide the Police with information required for the prevention and investigation of infringements of the law which have constituent elements of criminal offences in cyber space in accordance with the procedure established by the Police Commissioner General.
sanctions regime	The Code of Administrative Offenses imposes administrative liability on all cyber security entities for failing to comply with established organizational and technical cyber security requirements. The administrative fines range between EUR 30 and EUR 5,800.
competent authorities	Art. 4 of the Law on Cyber Security lists the competent authorities for developing and implementing cyber security policy in Lithuania: • Strategic goals and priorities of cyber security policy as well as measures necessary to achieve them are determined by the Government of the Republic of Lithuania. • Cyber security policy is developed, its implementation is organised, controlled and coordinated by the Ministry of National Defence of the Republic of Lithuania. The National Cyber Security Centre takes part in the development of the cyber security policy to the extent to which legal regulation of activities of cyber security entities has to be established for the performance of functions laid down in this law. • Cyber security policy is implemented by the National Cyber Security Centre, the State Data Protection Inspectorate, the Lithuanian Police and other authorities the functions of which are related to cyber security. Detailed tasks and powers of the competent authorities for cyber security in Lithuania are described in Art. 5–10 of the Law on Cyber Security.
Jurisdictional applications	The Law on Cyber Security does not provide rules for determining jurisdictional applicability, however, generally, in case a digital service provider or its representative has its legal seat in Lithuania, the Lithuanian law will apply.
Remarks (if any)	N/A

Luxembourg

Current status of implementation	NIS Directive has not been implemented yet in Luxembourg. A draft law (n°7314) has been filed on 6 June 2018 with the Luxembourg Parliament. The draft law is actually under discussion at the Luxembourg Parliament.
Implementation Act	N/A
Determination of operators of essential services (Art. 5 NIS)	The draft law specifies the criteria to identify operators of the following essential services: (i) Energy; (ii) Transportation; (iii) Banks; (iv) Financial market infrastructures; (v) Health sector; (vi) Water; (vii) IT.
reporting obligations	Operators of essential services must notify, without undue delay, the competent authority of incidents having a significant impact on the continuity of the essential services they provide. Such notifications are transmitted to the governmental agency in charge of IT urgencies or to CIRCL, the computer Incident Response Center Luxembourg - depending on their competence.
sanctions regime	Under the draft law, the following sanctions may apply: (i) Warning (ii) Reprimand (iii) Fine of maximum EUR 125,000.
competent authorities	Under the draft law the competent authorities are the Financial Supervisor (Commission de Surveillance du Secteur Financier - CSSF) and the Luxembourg Institute of Regulation (Institut luxembourgeois de régulation - ILR).
Jurisdictional applications	N/A
Remarks (if any)	N/A

Malta

Current status of implementation	The NIS Directive was implemented into Maltese law on the 6th July 2018.
Implementation Act	The Measures for High Common Level of Security of Network and Information Systems Order - Subsidiary Legislation 460.35 of the Laws of Malta ("**Order**").
Determination of operators of essential services (Art. 5 NIS)	It is the Critical Information Infrastructure Protection Unit ("**CIIP Unit**") which has general oversight over the Order. Thus, Operators of Essential Services ("**OES"**) are identified and determined by the CIIP Unit. OESs are established from the sectors and sub-sectors listed in the Second Schedule of the Order, namely: (i) Energy, (ii) Transport, (iii) Banking, (iv) Financial Market Infrastructure, (v) Health Sector, (vi) Drinking Water Supply and Distribution, (vii) Digital Infrastructure and Public Administration. The CIIP Unit has informed us that certain OESs have already been identified under the Order. It was however indicated that such identification is not to be made public, and that instead, such identification shall take place by means of private communication between the CIIP Unit and the OES concerned.
reporting obligations	OESs or Digital Service Providers ("**DSP**") shall notify the CIIP Unit "without undue delay, of incidents" having: a significant (OES) /substantial (DSP) impact on the provision of their services. To determine the significance/substantiality of the impact, account shall be taken, inter alia, of the number of affected users, the duration, the geographical spread, and the sectors effected, resulting from such incident.
sanctions regime	Art. 19 para. 1 of the Order specifies that the CIIP Unit has the right to (i) impose an administrative fine and (ii) order the cessation of any act or omission which is in breach of the Order, in respect of any undertaking which infringes any provision of the Order or any law which the CIIP Unit is entitled to enforce, or any undertaking which fails to comply with any decision given by the same CIIP Unit. In particular, any undertaking which fails to: (i) implement appropriate and proportionate security measures in accordance with Art. 11 and 13 of the Order (security and incident notification requirements of OES and DSP respectively); or (ii) fails to cooperate with the CIIP Unit when the latter exercises its monitoring obligations under the Order, shall be liable to an administrative fine of not less than EUR 1,000 and not more than EUR 100,000 for each violation. The CIIP Unit may also impose a EUR 100 fine for each day that any such violation persists, with the possibility of backdating such fine to the date of commission or commencement of the infringement. Moreover, any undertaking which: (i) fails to notify where it should have notified an incident (ii) fails to comply with lawful instructions of the CIIP Unit; or (iii) fails to comply with any other provision of the Order which is not listed under Art. 19 para. 1 (which is cited above); shall be liable to an administrative fine of not less than EUR 500 and not more than EUR 50,000 for each violation. The CIIP Unit may also impose a EUR 50 fine for each day that any such violation persists, with the possibility of backdating such fine to date of commission or commencement of the infringement.
competent authorities	The main 'competent authority' responsible for the NIS Directive is the CIIP Unit within the Maltese Ministry for Home Affairs and National Security. The CIIP Unit shall be responsible for the monitoring, application and enforcement of the NIS directive.

Jurisdictional applications	The Order only specifies the jurisdictional and territorial limits of DSPs. Art. 16 states that DSPs shall be deemed to be under the jurisdiction of Malta if its main establishment is in Malta, i.e. if its head office is located in Malta. However, if the DSP's main establishment is outside the EU, but offers services captured by the NIS Directive in the EU, it shall be deemed to be under Malta's jurisdiction if it has a representative established in Malta.
Remarks (if any)	N/A

Netherlands

Current status of implementation	In the Netherlands, the NIS Directive has been implemented by the Networks- and Information Systems Security Act (the "**Act**"), which has come into effect on 9 November 2018.
Implementation Act	Network and Information Systems Security Act (*Wet beveiliging netwerk- en informatiesystemen*).
Determination of operators of essential services (Art. 5 NIS)	The (categories of) operators to which the Act applies have been appointed by decree, which entered into force on 1 January 2019. All categories included in Annex II to the NIS-Directive are represented (namely (i) Energy, (ii) Transportation, (iii) Banking, (iv) Infrastructure for the financial market, (v) Supply of drinking water and (vi) Digital infrastructure), with the exception of Healthcare. The reason the Healthcare sector has not yet been designated as an essential sector is that the Dutch government does not consider it to be sufficiently 'high risk', as it is largely decentralised.
reporting obligations	Operators of essential services are obliged to immediately notify the following events to the National Cyber Security Centre (Art. 10 of the Act): 1. Incidents with significant consequences for the continuity of the essential service (NB: these incidents must also be notified to the competent authority); 2. Breaches of the security of network and information systems which may have significant consequences for the continuity of the essential service; and 3. Incidents at DSPs if these incidents have significant consequences for the continuity of the essential service. DSPs are obligated to notify incidents with significant consequences for the continuity of the digital service to the Minister of Economic Affairs and Climate Policy and the Dutch Radiocommunications Agency (Art. 13 of the draft implementation act). However, notification is only mandatory if the DSP has access to the information required to determine whether the incident has significant consequences for the continuity of the digital service in question.

sanctions regime	The Act provides for the following administrative fines: • A maximum of EUR 5 million for any breach of the draft implementation act by essential service operators or DSPs; • A maximum of EUR 1 million for failing to cooperate with a request for further information from the National Cyber Security Centre; and • A maximum of EUR 1 million for failure to adequately cooperate with supervisory authorities exercising their competencies.
competent authorities	The following authorities have been appointed as the competent authorities: • For the sectors Energy and Digital Infrastructure: Minister of Economic Affairs and Climate Policy; • For the sectors Banking and Financial Market Infrastructures: Dutch National Bank ("DNB"); • For the sectors Transport and Drinking water supply and distribution: Minister of Infrastructure and Water Management; and • For the sector Healthcare (despite no designations as operators of essential services within this sector): Minister of Health, Welfare and Sports. The Radiocommunications Agency has been appointed as the competent authority for DSPs.
Jurisdictional applications	According to the Act, operators of essential services can be either private or public entities, but the Act does not contain a determination with regard to the territorial scope. However, departing from a decree related to the predecessor of the Act, application of the Act will most likely be limited to operators offering services within the Netherlands, but it will not always be required that the operator's main establishment is located in the Netherlands. DSPs can exclusively be legal entities and are subject to the Act if their main establishment or representative is located in the Netherlands or if they offer digital services in the Netherlands.
Remarks (if any)	In addition to essential operators, an obligation to notify exists for other 'vital providers', which have been appointed by decree from the following sectors: Nuclear, Weirs, Finance and Telecoms. Neither supervision nor sanctions apply for violation of the notification requirement by vital operators which are not classified as operators of essential services (or DSPs). However, the parliamentary history of the Act specifically mentions that this may change if deemed necessary in the future.

Poland

Current status of implementation	The NIS Directive was fully implemented in Poland on 21 November 2018, when the Regulation on serious incidents thresholds applicable to operators of essential services was published.
Implementation Act	The National Cyber Security System Act of 5 July 2018 (Dz.U.2018.1560) ("**NCSA**") plus 12 Government Regulations, including the Regulation on the list of essential services of 11 September 2018 (Dz.U. 2018 poz. 1806); The Regulation on serious incidents thresholds applicable to operators of essential services of 31 October 2018 (Dz.U. 2018 poz. 2180); The Regulation on organizational and technical conditions for entities providing cybersecurity services and internal structures of OES responsible for cybersecurity of 4 December 2019 (Dz.U. 2019 poz. 2479).

Determination of operators of essential services (Art. 5 NIS)	NCSA states that operators of essential services will be appointed from the same sectors as mentioned in Annex II to the NIS-Directive, namely (i) Energy, (ii) Transportation, (iii) Banking, (iv) Infrastructure for the financial market, (v) Healthcare, (vi) Supply of drinking water, and (vii) Digital infrastructure. Operators of essential services are designated by the competent authority if (i) they are providing essential services; (ii) these services depend on IT systems; (iii) a potential incident would have a significant disruptive effect on the service. Detailed criteria are listed in the Regulation issued by the Council of Ministers.
reporting obligations	Operators of essential services must immediately, but within no more than 24 hours, report a significant incident to the CSIRT MON (Computer Security Incident Response Team led by the Minister of National Defense), CSIRT NASK (Computer Security Incident Response Team run by Academic Computer Network - National Research Institution) or CSIRT GOV (Computer Security Incident Response Team led by the Head of the Internal Security Agency), depending on their sector (Art. 11.1.4 of the NCSA). Providers of digital services must immediately, but within no more than 24 hours, report a significant incident to the CSIRT NASK (Art. 18.1.4 of the NCSA).
sanctions regime	Art. 73 of the NCSA provides for administrative fines of up to PLN 1,000,000 (EUR 230,000) imposed by the competent authority, in particular in the following cases: Operators of essential services: – failure to implement a security management system, ensuring in particular: management of incidents, including their identification, classification and prioritization of incident handling, registration, analysis, searching for connections, undertaking corrective actions and remedying the causes of incidents and providing information on serious incidents to the appropriate CSIR; – failure to classify security incidents; – failure to properly report a significant incident (up to PLN 200,000 / EUR 50,000). If as a result of an inspection the competent authority finds that an operator of essential services persistently violates the Act, causing 1) a direct and serious threat to cybersecurity for defense, state security, public safety and order, or human life and health, 2) the threat of serious damage to property or serious difficulties in providing key services the competent authority will impose a penalty of up to PLN 1,000,000 (EUR 230,000).
competent authorities	The competent authorities for cybersecurity are the ministers competent for the sector in which the given operators of critical infrastructure operate (Art. 41 of the NCSA), the Minister of Digital Affairs and competent CSIRTs.
Jurisdictional applications	Operators of essential services are subject to Polish law and the NCSA if they have an organizational unit within the territory of Poland (Art. 5.1. of the NCSA). The provision of digital services is subject to Polish law if the digital service provider has its registered seat, or headquarters or a representative having an organizational unit within the territory of Poland. Small and micro entrepreneurs are excluded (Art. 17.1. of the NCSA).
Remarks (if any)	The decisions appointing operators of essential services are still being issued and delivered to the parties at issue.

Portugal

Current status of implementation	In Portugal, the NIS Directive has been implemented by Law no. 46/2018 of 13 August (Legal Regime of Cyber Security), which has come into effect on 14 of August 2018.
Implementation Act	Legal Regime of Cyber Security ("Regime Jurídico da Segurança do Ciberespaço"): Law no. 46/2018 of 13 August.
Determination of operators of essential services (Art. 5 NIS)	For an operator to be considered as an Operator of Essential Services it must be an entity, public or private, that provides an essential service (Art. 3 lit. g of the Law no. 46/2018 of 13 August). Art. 10 of the Law refers to the essential services as the ones described in the Annex of the Law, which includes the following: Energy; Transportation and traffic; Finance; Health; Water; IT & telecoms.
reporting obligations	Law no. 46/2018 states, in the following articles, that: • Art. 15, the Public Administration and critical infrastructures must notify the National Cybersecurity Center of incidents with relevant impact on the security of networks and information systems. In order to determine the relevance of the impact of an incident, the following parameters shall be taken into account: – The number of users affected; – The duration of the incident; – The geographical distribution, with regard to the area affected by the incident. • Art. 17, essential services must notify the National Cybersecurity Center of incidents that have a material impact on the continuity of the essential services they provide In order to determine the relevance of the impact of an incident, the following parameters shall be taken into account: – The number of users affected by the disruption of the essential service; – The duration of the incident; – The geographical distribution, with regard to the area affected by the incident. • Art. 19, digital service providers must notify the National Cybersecurity Center of incidents having a substantial impact on the provision of digital services. In order to determine the relevance of the impact of an incident, the following parameters shall be taken into account: – The number of users affected by the incident, namely users who depend on the service to provide their own services; – The duration of the incident; – The geographical distribution, with regard to the area affected by the incident; – The severity level of the service disruption; – The extent of the impact on economic and societal activities. Pursuant Art. 14 of Law, the Public Administration and critical infrastructures must comply with appropriate and proportionate technical and organizational measures to manage the risks to the security of the networks and information systems they use According

	to Art. 18, digital service providers shall identify and take appropriate and proportionate technical and organizational measures to manage the risks to the security of the networks and information systems they use in the context of the provision of digital services.
sanctions regime	The infractions and respective sanctions are foreseen in Art. 21 and following of the Law. • Very serious infractions (Art. 23) are punished with a fine of EUR 5,000 to EUR 25,000 in the case of a natural person, and of EUR 10,000 to EUR 50,000 in the case of a person collective. • Serious administrative offenses are punished by a fine of EUR 1,000 to EUR 3,000, in the case of a natural person, and of EUR 3,000 to EUR 9,000, in the case of a legal person.
competent authorities	According to Art. 7 No. 4 of the Law, the National Cybersecurity Center (*Centro Nacional de Cibersegurança*) is the Portuguese national authority for the Cybersecurity and has regulatory, supervisory, enforcement and sanctioning functions and the power to issue cybersecurity instructions and to define the national level of cybersecurity alert. Besides, the National Cybersecurity Center acts in articulation with the Portuguese Data Protection Authority (*Comissão Nacional de Proteção de Dados)* when it concerns incidents that have given rise to the violation of personal data. In addition, there is a National Computer Security Incident Response Team ("**CERT.PT**") which operates within the National Cybersecurity Center and, according to Art. 9, has as its main competences: (i) Implement operational coordination in response to incidents, in particular in liaison with existing sectoral IT security incident response teams; (ii) monitor incidents with national implications; (iii)activate early warning mechanisms; (iv) to intervene in the reaction, analysis and mitigation of incidents; (v) undertake a dynamic risk analysis; (vi) ensure cooperation with public and private entities; (vii) promote the adoption and use of common or standardized practices; (viii) participate in national cooperation fora for computer security incident response teams; (ix) ensure national representation in international cooperation fora of computer security incident response teams; (x) participate in national and international training events.
Jurisdictional applications	Law No. 46/2018 applies to digital service providers who have their headquarters or principal place of business in national territory or if they appoint a representative established within national territory, if they provide digital services there.
Remarks (if any)	The digital services providers must communicate immediately to the National Cybersecurity Center (*Centro Nacional de Cibersegurança*) the exercise of their activity, according to Art. 30 No. 1 of Law.

Romania

Current status of implementation	NIS Directive has been transposed into national legislation.

Implementation Act	Law No. 362/2018 on ensuring high common level of security of network and information systems, published in Official Gazette of Romania, Part I, No. 21 of 09.01.2019 ("**Law No. 362/2018**"). Law No. 362/2018 entered into force on 12 January 2019. During 2019 further technical and methodological norms for the implementation of Law No. 362/2018 were enacted, namely: (i) Order No. 599/2019 on the approval of the methodological norms for identifying the essential service operators and digital service providers, published in the Official Gazette of Romania, Part I, No. 584 of 17.07. 2019; (ii) Order No. 600/2019 on the approval of the methodological norms for the organization and functioning of the Register of essential service operators, published in the Official Gazette of Romania, Part I, No. 542 of 02.07.2019; Order No. 601/2019 on the approval of the methodological norms for establishing the significant disruptive effect of incidents on the networks and information systems of the essential service operators, published in the Official Gazette of Romania, Part I, No. 590 of 18.07. 2019.
Determination of operators of essential services (Art. 5 NIS)	Law No. 362/2018 provides a list of sector of activities and activities deemed to be essential, namely: (i) energy (electricity, oil and gas), (ii) transport (including all type of transportation), (iii) banking industry, (iv) financial market infrastructures, (v) health care sector (both private and public health care providers), (vi) drinking water supply and distribution, (vii) digital infrastructure. For each sector, Law No. 362/2018 also provides an indicative list of categories of entities carrying out activities in the relevant sectors which would be subject to the requirements of this law. Within 5 months as of entering into force of Law No. 362/2018, the Ministry of Information Society and Communication should have had laid down specific thresholds based on which the entities activating in the relevant sectors would qualify as operators of essential services, namely: (i) thresholds for determining the significant disruptive effect of incidents at the level of key service providers' networks and systems; (ii) the thresholds corresponding to the cross-sectoral impact; (iii) specific sectoral criteria and thresholds for each sector and subsector of activity set out in the Annex of Law No. 362/2018. Specific thresholds and criteria prepared by the Ministry of Information Society and Communication were submitted with the Romanian Government for approval in 2019. Still, the draft government decisions approving these are still pending the legislative approval process. The entities falling under the abovementioned criteria should submit with CERT-RO an application for the registration in the Registry of essential service operators ("**RESO**"). While RESO is already operational, the registration obligation is not yet enforceable against the entities potentially qualifying as operators of essential services, given that the Government decisions regulating the thresholds and criteria mentioned above have not yet been formally enacted.
reporting obligations	The essential service operators and digital service providers have the obligation to notify incidents that have a significant impact on the continuity of services. The notification obligations correspond to the obligations provided at Art. 16 of the NIS Directive. Further notification procedure will be detailed in technical / methodological norms of Law No. 362/2018 which needs to be approved within 6 months as of this law entering into force.

sanctions regime	Failure to comply with the prescribed obligations may be sanctioned with administrative fines ranging from RON 3,000 (approx. EUR 670) to RON 50,000 (approx. EUR 11,000). Repeated breaches of the obligations may be sanctioned with administrative fines of up to RON 100,000 (EUR 22,000). In case of companies with a turnover exceeding RON 2,000,000 (approx. EUR 440,000), the administrative fines may be of up to 2% of the company's turnover and, for repeated breaches, of up to 5% of the company's turnover.
competent authorities	The Romanian National Center of Response to Cyber Security Incidents ("**CERT-RO**").
Jurisdictional applications	A draft government decision on the composition, attributions and organization of the Interinstitutional Working Group for the determination of the thresholds necessary to determine the significant disturbing effect of the incidents at the level of the networks and computer systems of the essential service operators has been published on 07.03.2019 on the website of the Ministry of Information Societies and Communications for public consultation. The draft government decision is still pending approval by the Government. The Interinstitutional Working Group, among other attributions, is supposed to assist CERT-RO in drafting the government decision for the determination of the relevant thresholds necessary to determine the significant disturbing effect of the incidents (legal enactment which pursuant to Law No. 362/2018 needs to be approved within 5 months as of entering into force of the law). The intention is clear - to unify and ensure a high level of network security and information systems across the European Union.
Remarks (if any)	A draft government decision on the composition, attributions and organization of the Interinstitutional Working Group for the determination of the thresholds necessary to determine the significant disturbing effect of the incidents at the level of the networks and computer systems of the essential service operators has been published on 7 March 2019 on the website of the Ministry of Information Societies and Communications for public consultation. The draft government decision is still pending approval by the Government. The Interinstitutional Working Group, among other attributions, is supposed to assist CERT-RO in drafting the government decision for the determination of the relevant thresholds necessary to determine the significant disturbing effect of the incidents (legal enactment which pursuant to Law No. 362/2018 needs to be approved within 5 months as of entering into force of the law). The intention is clear - to unify and ensure a high level of network security and information systems across the European Union.

Slovakia

Current status of implementation	Slovakia implemented INC Directive by the Act No. 69/2018 Coll. On cybersecurity effective as of 1 April 2018, amended with an effectiveness as of 1 January 2019 by the Act No. 373/2018 Coll.

Implementation Act	The Act comprehensively regulates the area of cybersecurity and information assurance, it implements basic security requirements and measures necessary for coordinated protection of information and communication managing systems. This is the first legal norm governing the cybersecurity within the Slovak Republic. It comes into effect on 1 April 2018. At the same time, it transposes European directive on network and information security ("**NIS Directive**") into Slovak legal order. The New Act on Cyber security amended further Acts, in particular the Act No. 145/1995 Coll. on Administration Fees as amended; the Act No. 73/1998 Coll. on the State Service of the Police Corps, the Slovak Information Service, the Prison and Judicial Guards of the Slovak Republic and the Rail Police as amended; the Act No. 319/2002 Coll. on the Defence of the Slovak Republic as amended; the Act No. 321/2002 Coll. on the Armed Forces of the Slovak Republic as amended; the Act No. 553/2003 Coll. on the remuneration of some employees in the performance of their work in the public interest as amended; the Act No. 215/2004 Coll. on the protection of classified information as amended; the Act No. 45/2011 Coll. on Critical Infrastructure as amended; and the Act No. 55/2017 Coll. on State Service as amended. Mentioned novelisation was related mainly to implement opinion of the European Central Bank dated on 31 August 2018 on critical infrastructure, cyber security and bonds (CON/2018/39) and also such novelisation reflected application issues and required changes and findings of the Slovak National Security Office based and in accordance, but not exclusively, with the Intelligent Industry Action Plan. The Slovak National Security Authority issued several ordinances covering (i) content of the security measures, structure of the security documentation and the range of the general security measures (Ordinance No. 362/2018 Coll.); (ii) criteria of the essential services (Ordinance No. 164/2018 Coll.); (iii) laying down identification criteria for each category of major cyber security incident and details of cyber security incident reporting (Ordinance No. 165/2018 Coll.); and (iv) details of the technical, technological and personnel equipment of the cyber security incident handling unit (Ordinance No. 166/2018 Coll.).

Determination of operators of essential services (Art. 5 NIS)	According to Act on cybersecurity the essential service is a service recognized in the list of essential services and: (i) is depending on networks and information systems and is carried out at least in one sector or subsector; (ii) is an information system of public administration; or (iii) is an element of critical infrastructure. The Authority shall add an essential service to the list of essential services and its operator to the registry of essential services operators (i) on the basis of the notification of a service operator; (ii) on the basis of an initiative of a central body, if an excess of the identification criteria of the operated service was reached; (iii) on the basis of own initiative if they learned on the excess of identification criteria and there was not made any step in accordance to previous items. Impact identification criteria taking into account especially: (i) number of users using essential service; (ii) dependency of other sectors of the essential service; (iii) effect the cybersecurity incidents might have as to the extend, lasting time on economic and social activities and interests of the state or on the state security; (iv) the market share of the service operator; (v) geographical extension as to the area possibly affected by cybersecurity incident; (vi) importance of the essential service operator as to the maintenance of providing service continuity. Specific sectorial identification criteria are taking into account criteria given by general binding regulation issued by the Authority. The service operator is obliged to notice the Authority the excess of the impact criteria at least within thirty (30) days since the excess discovery. They notice the Authority the specific sector criteria excess within the same period and even in case the impact criteria excess was not recognized.
reporting obligations	Operators of essential services must notify any incident with significant impact without undue delay (via a single cyber security information system). In case the operator of essential services uses for providing essential services also the operator of digital services, the obligation to notify any incident with significant impact shall be transferred to the operator, i.e. for this notification the operator of a digital services shall be responsible (Sec. 24). A digital service provider is obliged to notify any security incident, regardless of the impact (Sec. 25). The Act on cyber security also permits voluntary reporting of security incidents (Sec. 26).

sanctions regime	The authority is able to impose a fine to a natural person in the amount of EUR 100 up to EUR 5,000. The legal entity / operator of the essential services or a digital service provider may be sanctioned by impose of EUR 300 up to 1% of annual turnover not exceeding sum of EUR 300,000. The authority shall be also authorized to impose fine in the amount of EUR 300 to up to EUR 100,000 to anyone, who would not provide required information related to national cyber security strategy. When determining the amount of fines, the authority shall take into account the seriousness of the administrative offense / tort, in particular the manner of committing it, the duration, consequences and circumstances in which it was committed (Sec. 30 and 31).
competent authorities	National Security Authority is responsible for cyber security sphere (Protection of Classified Information, Cryptographic Services, Trust Services and Cyber Security). The Authority as the central government body is in the performance of its duties governed by several acts (e.g. Constitution of the Slovak Republic, legally binding acts of the European Union, international treaties binding the Slovak Republic, laws and other generally binding legal regulations, resolutions of the Government of the Slovak Republic, and also its status and organizational regulations and other internal regulations of the Authority). The Authority is also the single point of contact for national security.
Jurisdictional applications	If a digital service provider or its representative is established or provides services in the Slovak Republic, the Slovak laws are binding (Sec. 23).
Remarks (if any)	Any company operating in critical sectors and providing targeted services has to reflect the requirements of NIS and the new law in its systems and processes. Even the Authority, as one of the "creators" of the Bill, has shown a negative impact, especially on small and medium-sized enterprises. The intention is clear - to unify and ensure a high level of network security and information systems across the European Union. National Security Authority shows and helps enterprises by the issuance of mentioned Ordinances and also by organising several seminars and attendance on conferences. By such actions is authority trying to describe and explain all potentially unclear issues and discrepancies; thus, we appreciate authorities' effort.

Slovenia

Current status of implementation	On 17 April 2018 the Slovenian National Assembly adopted Act on Information Security that came into effect on 11 May 2018, thus implementing the NIS Directive into the Slovenian legal system.
Implementation Act	Act on Information Security (Official Gazette of the RS, No. 30/18) ("**ZInfV**").

Determination of operators of essential services (Art. 5 NIS)	Pursuant to Art. 5 of the NIS Directive, the ZInfV specifies the criteria to identify operators of the following essential services: (i) energy, (ii) digital infrastructure, (iii) water management and distribution, (iv) healthcare, (v), transportation (vi) banking, (vii) financial markets infrastructure, (viii) food supply and (ix) environmental protection. Operators of essential services can be legal persons, entrepreneurs or public bodies, which (i) operate one of the following essential services (further described by Government Ordinance (Official Gazette of the RS, No. 39/19) ("Ordinance"), which entered into force on 22 June 2019); (ii) meet the criteria set out in Art. 7 of the ZInfV ((1) the operator provides a service that is essential for the preservation of key social or economic activities; (2) the provision of this service depends on networks and information systems and (3) the incident would have a significant negative impact on the provision of this service) and further described in the Ordinance and (iiii) are designated as such by the Government of Republic of Slovenia. The aforementioned Ordinance foresees that the Ordinance is not applicable for provision of services and information systems under the jurisdiction and supervision of the Bank of Slovenia or European system of Central Banks. In addition, prior consent of the Bank of Slovenia is foreseen for designation of the operators in the field of banking as operators of essential services, if the provision of services or information systems does not fall under the jurisdiction or supervision of Bank of Slovenia or European system of Central Banks. The Ordinance includes a further subdivision of essential services laid down in ZInfV and detailed sectoral and inter-sectoral factors that determine significant negative impact. To meet the criteria of significant negative impact, the operator must meet at least three inter-sectoral and at the same time at least two sectoral factors laid down in the Ordinance. Pursuant to ZinfV the following inter-sectoral factors must be considered: (i) number of users depended on the essential service; (ii) dependency of other sectors of the essential service; (iii) effect the cybersecurity incidents might have as to the extent and lasting time on economic and social activities or on the public security; (iv) the market share of the service operator; (v) geographical extension as to the area possibly affected by cybersecurity incident; (vi) importance of the essential service operator as to the maintenance of providing service continuity. The Ordinance further elaborates the above-mentioned inter-sectoral factors and sectoral factors for each of the nine essential services. Pursuant to the provisions of ZinfV and the Ordinance, the Government of the Republic of Slovenia shall designate the individual operators of essential services with an individual act. However, such acts are not publicly available, therefore it cannot be discerned from the publicly available information which legal persons or entrepreneurs (if any) have been designated as operators of essential services in the Republic of Slovenia.
reporting obligations	Pursuant to ZInfV, operators of essential services must immediately report to the competent authority (National Computer Security Incident Response Team - National CSIRT) any security incident that has a significant impact on the provision of essential services. ZInfV also foresees the same obligation for the providers of digital services that provide such services in the EU and state administration authorities.

sanctions regime	Art. 37 of the ZInfV provides for fines in misdemeanor proceedings from EUR 10,000 up to EUR 50,000 for medium and large companies and EUR 500 up to EUR 10,000 for other companies, in particular in the following cases: Operators of essential services – fail to properly designate a point of contact in a timely manner; – fail to implement appropriate technical and organisational measures to prevent disruptions of availability etc.; – fail to properly report a security incident; – fail to properly implement the decision of competent national authority. Art. 38 of the ZInfV provides for fines in misdemeanor proceedings from EUR 10,000 up to EUR 50,000 for medium and large companies and from EUR 500 up to EUR 10,000 for other companies, in particular in the following cases: Providers of digital services – fail to implement technical and organisational measures to tackle risks for the security of the network and information systems; – fail to properly report a security incident; – fail to properly implement the decision of competent national authority. Art. 39 of the ZInfV provides for fines in misdemeanor proceedings from EUR 200 up to EUR 2,000, in particular in the following cases: The responsible person of the state administration authority – fails to implement appropriate technical and organisational measures to prevent disruptions of availability etc.; – fails to properly report a security incident; – fail to properly implement the decision of competent national authority.
competent authorities	"Slovenian Information Security Administration" (*Uprava RS za informacijsko varnost*) as well as National CSIRT, a national response centre primarily responsible for examining security incidents. The ZInfV also provides for the establishment of state administration authorities' CSIRT. The Slovenian Information Security Administration operates under the authority of the Ministry of Government Administration. Slovenian Information Security Administration began operating as of 1 January 2020, while the other authorities began operating as of 1 January 2019.
Jurisdictional applications	Pursuant to Art. 1 of the ZInfV the Act regulates information security of the networks and information systems in the Republic of Slovenia, which are essential for the smooth functioning of the state in all security conditions and provide essential services for the preservation of key social and economic activities in the Republic of Slovenia. ZInfV contains no other jurisdictional provisions, except in one case: According to Art. 6 para. 4 the Slovenian Information Security Administration must consult with the respective EU member state before issuing its decision regarding a designation of a certain operator of essential services, if the operator provides essential services in Republic of Slovenia as well as in another EU member state.
Remarks (if any)	The ZInfV is the first of such kind (i.e. in the field of cyber security) in Slovenian legislature. Nonetheless, some progress in the field has been made in 2016 when the Government adopted the Cyber Security strategy, which outlined future policy and measures in the field of cyber security. In April 2017 the Government also adopted a decision, temporary granting the operational tasks in the field of cyber security to Office of the Government of Republic of Slovenia for Protection of Classified Information. The Office shall retain this jurisdiction till 1 January 2020, when the Slovenian Information Security Administration shall begin operating, as the ZInfV proposes.

	Pursuant to the provisions of ZinfV and the Ordinance, the Government of the Republic of Slovenia shall designate the individual operators of essential services with an individual act. However, such acts are not publicly available, therefore it cannot be discerned from the publicly available information which legal persons or entrepreneurs have been designated (if any) as operators of essential services in the Republic of Slovenia.

Spain

Current status of implementation	NIS Directive has been implemented in Spain through Royal Decree 12/2018. This Royal Decree was published in the Spanish Official Gazette (BOE) on 8 September 2018.
Implementation Act	Royal Decree 12/2018, 7 September 2018 on security networks and information systems
Determination of operators of essential services (Art. 5 NIS)	According to the Royal Decree this law will apply to: (i) Operators of essential services ("**OES**") established in Spain or with a permanent establishment in Spain in sectors covered by the Spanish Law 8/2011 on Critical Infrastructures which includes amongst others the following sectors: energy, transport, health, digital infrastructures etc. The Spanish Government will publish the list of essential services affected by the Royal Decree within the sectors covered by the Law 8/2011 on Critical Infrastructures. The first list was published on 13 December 2018. (ii) Digital services providers ("**DSP**") considered as online marketplaces, online research engines and/or providers of cloud computing services with more than 50 employees and whose turnover exceeds 10 million of euros. The Royal Decree applies to those digital services providers that have their registered office in Spain or that constitute their main establishment in the UE, as well as, those that designate in Spain their representative to comply with NIS Directive.
reporting obligations	According to the Royal Decree OES and DSP must notify the incidents having significant impact on the provision of the services to the competent authority through the computer incident security response team ("**CSIRTs network**"). Note that OES must notify not only those incidents that may have significant impact on the provision of the services, but also all incidents that may affect the network even though they have not a real adverse effect on the network/system. Otherwise, DSP shall only notify those incidents over which the DSP has access to the necessary information to assess the impact on the incident. The Royal Decree (in line with NIS Directive) established the factors that must take into account to assess whether an incident can have significant impact on services (for example, the availability of the alternatives to maintain a sufficient level of essential services provision, affected graphic extension, market share etc.). The factors to determine whether an incident have or not significant impact on services - where those are provided by DSP - are established in implementing Regulation of the Commission nº2018/151. Under the Royal Decree, OES must make a first notification of the incidents without any delay. The notification shall include, amongst others, any information enabling the determination of the cross border effects of the incidents. In addition, operators should make other intermediate notifications to update the information on the incidents and a final notification after the resolution of the incident.

sanctions regime	According to the Royal Decree infringements are divided into very serious, serious or minor. A very serious infraction would be, e.g., the repeated breach of the obligation to report incidents (it is considered "repeated" from the second default) or the failure to take necessary measures to resolve the incidents in accordance with what it is established in the regulation. A serious infraction would be, e.g., the breach of the obligation to report incidents with significant impact on services or the failure to comply with regulatory provisions or technical instructions issued by the competent authorities regarding the minimum precautions that operators must take into account to ensure the safety of the networks and systems. A minor infringement would be, e.g., the breach of the obligation to report incidents without significant impact on services. The following penalties will apply: (i) fines of EUR 500,001 to EUR 1,000,000 in case of very serious infringements; (ii) fines of EUR 100,001 to EUR 500,000 in case of serious infringements and a reprimand or fines to EUR 100,000 in case of minor infringements.
competent authorities	According to the Royal Decree, competent authorities are as follows: (i) For OES: – In the case that these are also critical operators designated according to Law 8/2011 of April 28, the Secretary of State of the Ministry of the Interior, through the National Center for Protection of Infrastructures and Cybersecurity (CNPIC). – In case they are not critical operators, the sectoral authority corresponding by reason of the matter, as determined by the regulation. (ii) For DSP: The Secretary of State for the Society of Information and the Digital Agenda, of the Ministry of Energy, Tourism and Digital Agenda.
Jurisdictional applications	According to the Royal Decree this law will apply to: (i) OES established in Spain. It will be understood that an OES is established in Spain when his residence or registered office are within the Spanish territory, provided that they coincide with the place where the administrative management and management is effectively centralized of your business or activities. Also this law will be applicable to essential services that operators resident or domiciled in another state offer through a permanent establishment located in Spain. (ii) DSP that have their registered office in Spain as well as those who, without being established in the European Union, designate their representative in the Union for compliance with Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016.
Remarks (if any)	The Spanish legislator will have to coordinate the new obligations under this Royal Decree with some existing legislation, such as (i) Law 8/2011, of April 28, which establishes measures for the protection of the critical infrastructures, (ii) Law 36/2015, of September 28, of National Security, and (iii) with the Real Decree 3/2010, of January 8, which regulates the National Security Scheme, as special regulations on the security of information systems in the public sector. It is expected that development regulation of the Royal Decree 12/2018 will be passed in the following months.

Sweden

Current status of implementation	The new Act (2018:1174) and the ordinance (2018:1175) implementing the NIS Directive in Swedish law, entered into force on the 1st of August 2018.
Implementation Act	• Act (2018:1174) on information security for certain operators of essential services and digital services providers. • Ordinance (2018:1175) on information security for certain operators of essential services and digital services providers. • MSBFS 2018:7 regulations regarding notifications and identification of suppliers of essential services. • MSBFS 2018:8 regulations and general advice regarding information security for suppliers of essential services. • MSBF 2018:9 regulations and general advice regarding incident reporting for suppliers of essential services. • MSBF 2018:10 regulations and general advice regarding incident reporting for digital service providers. • MSBF 2018:11 regulations and general advice regarding voluntary incident reporting in services which is important for the functionality of the society.
Determination of operators of essential services (Art. 5 NIS)	The Swedish Civil Contingencies Agency ("**MSB**") has specified in its regulation MSBFS 2018:7 the criteria to identify operators of the following essential services: (i) energy, (ii) transportation, (iii) banking, (iv) financial markets infrastructure, (v) health care, (vi) water management and (vii) digital infrastructure.
reporting obligations	Operators of essential services must immediately report significant disruptions to the Swedish Civil Contingencies Agency. The reporting obligation must not have a negative effect on correcting the disruption. Specifications on what defines a significant disruption will be announced in an ordinance or government agency regulation. Providers of digital services must immediately report to the Civil Contingencies Agency any disruptions that have a substantial effect on providing the services. MSB has provided a procedure to follow when reporting an incident. The procedure includes three steps: 1) CERT-SE shall be notified about the incident through phone within 6 hours from when the incident was detected, 2) a written report (specific form available at MSB's website) shall be provided to CERT-SW within 24 hours after the incident was detected, 3) within 4 weeks a second report shall be provided to CERT-SE (specific form available at MSB's website). Currently, the reports shall be sent to CERT-SE by post. However, MSB is working on an online tool for incident reporting.
sanctions regime	In case the supervising authority finds that the supplier has failed to file a notification with the supervising authority, implement appropriate safety measures and report incidents in accordance with Sec. 23, 12-16 and 18-19 or with the relevant regulations, the supervising authority may impose the supplier with an administrative fine from SEK 5,000 up to SEK 10,000,000.

competent authorities	Swedish Civil Contingencies Agency (MSB) is appointed CSIRT-unit. The regulatory authorities will be specified in an ordinance. A government report (SOU 2017:36) suggested the following regulatory authorities for the different sectors: • Energy: Swedish Energy Agency; • Transportation: Swedish Transport Agency; • Banking: Swedish Financial Supervisory Authority; • Finance: Swedish Financial Supervisory Authority; • Health care: Health and Social Care Inspectorate; • Distribution of drinking water: The National Food Agency; • Digital infrastructure: Swedish Post and Telecom Authority; • Digital services: Swedish Post and Telecom Authority.
Jurisdictional applications	Operators of essential services are subject to Swedish law on the condition that the supplier is located in Sweden, that the service is dependent on networks and information systems and that an incident would cause a significant disruption in the supply of the service. Providers of digital services are subject to Swedish law when its main establishment is located in Sweden or when it has appointed a representative that is established in Sweden.
Remarks (if any)	N/A

United Kingdom

Current status of implementation	On 10 May 2018, the NIS Directive (NISD) was transposed into UK law as the NIS Regulations (NISR).
Implementation Act	The NISD was implemented into UK law on 10 May 2018 through Sec. 2 para. 2 of the European Communities Act 1972.

Determination of operators of essential services (Art. 5 NIS)	In accordance with Regulation 8 and Schedule 2 of the NISR, the UK Government has identified operators of the following essential services to fall within scope of the regulations:(i) Drinking water supply and distribution, (ii) Energy (including electricity, oil and gas), (iii) Digital Infrastructure, (iv) Health Sector, and (v) Transport (including air, maritime, rail and road). Within these sectors there are a series of detailed minimum thresholds to ensure the NISR applies to only those who are large enough to provide critical societal or economic activities. Alongside essential operators, Relevant Digital Service Providers (RDSPs) are required to comply with the requirements of the NISR. A RDSP is a (i) search engine, (ii) cloud computing service, or (iii) online marketplace, with an office or nominated representative established in the UK, and with over 50 employees or an annual turnover of at least £10 million.
reporting obligations	NIS incidents which are considered to have a significant impact on the continuity of the essential services which a service provider provides must be reported. In order to define the thresholds of having a significant impact, the competent authorities have published incident reporting thresholds for each sector and/or sub sector. In order to determine the significance of an incident's impact an operator must have regard to (i) the number of users affected by the disruption of the essential service; (ii) the duration of the incident; and (iii) the geographical area affected by the incident. In addition, competent authorities may also use the following optional parameters: (iv) the dependency of other sectors on the service provided by the affected entity; and (v) the impact that incidents have, in terms of degree and duration, on economic and societal activities, public safety or national security. Operators must report an incident without undue delay and in any event no later than 72 hours after having become aware of an incident. The UK Government encourages the voluntary reporting of incidents that do not meet the NIS Directive thresholds of a reportable incident, such as: 1. incidents where operators have to take action to maintain supply, provision, confidentiality or integrity of the service; and 2. incidents where software/intrusions are found that could potentially disrupt, or allow to be disrupted, the supply, provision, confidentiality or integrity of the service. Voluntary reporting can be reported to either the competent authority or the National Cyber Security Centre (NCSC). The voluntary reporting of such incidents will not subject operators of essential services to increased liability. However, an operator of essential services will be expected to respond to such incidents as part of their duty to ensure that appropriate risk-management measures are in place to mitigate the impact of any adverse incident. Engagement with the voluntary reporting systems (through NIS or other systems) will be considered as evidence that such measures are in place, in particular when considering the effectiveness of risk management and incident management systems. A relevant DSP must notify the competent authority, the Information Commissioner's Office (ICO), about any security incident which has a substantial impact on the provision of any of the following digital services (i) online marketplace; (ii) online search engine; or (iii) cloud computing service. In order to determine whether the impact of a security incident is substantial a relevant DSP must have regard to a set of criteria set out in the draft NIS Regulation which implements the NIS Directive. Additionally the NIS Regulation provides that a relevant DSP must also have regard to the following (i) (in so far as the relevant DSP is able to assess) the number of users affected by the incident, and in particular, any users relying on the digital service for the provision of their services; (ii) the duration of the incident; and (iii) the geographical area affected by the incident; (iv) the extent of the disruption to the service provision; and (v) the extent of the impact on economic and societal activities. It is possible to qualify as an essential operator and as a DSP and those who do will have to comply with reporting requirements in each role.

sanctions regime	Competent authorities can serve an information notice upon a service provider to, among other things, obtain information relating to (i) that service provider's NIS security; and (ii) and the implementation of that service provider's security policies. The Information Commissioner has the power to service a similar notice upon a relevant DSP. Should an enforcement authority suspect a potential breach of the NIS Regulations, they have the power to conduct an inspection in order to assess whether a service provider or relevant DSP is fulfilling its respective obligations imposed by the Regulations. If the enforcement authority finds or has reasonable grounds to suspect a breach or failure of the obligations imposed by the NIS Regulations, they may serve an enforcement notice upon a service provider or relevant DSP. The enforcement notice, among other things, must specify the alleged failure by the recipient and what steps, if any, must be taken to rectify the failure. Should a service provider or relevant DSP, having been served with an enforcement notice, fail to rectify any alleged failure, the enforcement authority may follow up with the service of a penalty notice. A penalty notice may also be served when a service provider or relevant DSP fails to provide sufficient representations in response of the alleged breach. Financial penalties may be attached to the penalty notice and should be appropriate and proportionate to the failure in respect of which it is imposed. Financial penalties will only be levelled as a last resort where it is assessed appropriate risk mitigation measures were not in place without good reason. The NIS Regulations set out caps on the penalties which can be imposed reflective of the breach; from a limit of £1 million for any contravention which could not cause a NIS incident; to £17 million for the most severe breaches, being a material contravention which has the potential to cause an incident resulting in an immediate threat to life or significant adverse impact on the UK economy. In the event of any enforcement action by the competent authority, it will notify the operator of impending action, allow the operator an opportunity to make representations, and confirm the final decision and reasoning of the competent authority. Decisions taken by the competent authority will be enforceable by civil proceedings, and appealable through the court system. Under the NIS Regulations, a competent authority must have regard to whether the breach would also be result in liability under another enactment or regime. As such, there may be reason for an operator to be penalised under different regimes for the same event, such as the GDPR, because the penalties might relate to different aspects of the wrongdoing and have different impacts. This will not limit a competent authority's ability to apply the penalty it feels is appropriate to the circumstances, but will encourage it to factor in other regimes if this is appropriate.
competent authorities	The NIS Regulations take a multi authority approach to designating competent authorities to supervise each regulated sector regulated by the NIS Directive. Where there are operators that provide essential services to more than one sector, and therefore fall under the remit of more than one competent authority, the relevant competent authorities will be encouraged to cooperate, to ensure that they do not put an unnecessary burden on the operator. However, they will retain responsibility for their jurisdiction. The NCSC has a significant supporting role, providing expert advice to competent authorities, publishing guidance and assessment tools to enable them to undertake duties effectively and providing incident response capability to cyber-attacks. The Government has stated that there must be a clear separation of powers between the NCSC and competent authorities. Ultimate authority and responsibility for any regulatory decision will lie solely with the competent authority. A list of the designated competent authorities is set out in Schedule 1 of the NIS Regulations.

Jurisdictional applications	The territorial scope of the UK's implementing legislation adopts the position as set out under the NIS Directive. Each Member State has to identify essential operators with an establishment on its territory. The recitals to the Directive clarify that, for the purpose of identifying operators of essential services, establishment in a Member State implies the effective and real exercise of activity through stable arrangements. This means that a Member State can have jurisdiction over an essential operator not only in cases where the operator has its head office in its territory but also in cases where the operator has a branch (or other type of legal establishment). As such, several Member States could have jurisdiction over the same entity. Where a DSP is established in the EU, it will be subject to the jurisdiction of the Member State where it has its main establishment (i.e. head office). Where a DSP is not established in the EU but offers digital services into the EU, it must designate a representative in the Union. In that case, the Member State where the representative is established will have jurisdiction over the company.
Remarks (if any)	The NISR gives competent authorities powers to serve information notices, conduct inspections to assess an organisation's systems and serve enforcement notices setting out the steps an organisation must take to rectify an issue. In terms of financial penalties, the NISR includes a maximum fine of £17m for 'material contravention which the enforcement authority determines has caused, or could cause, an incident resulting in an immediate threat to life or significant adverse impact on the United Kingdom economy'. A breach of the NISR is cumulative with any GDPR sanction. However, the NISR includes text which encourages the enforcement authority to be reasonable and proportionate, taking into consideration whether the contravention is also liable to enforcement under another regime.

Follow us

@twobirdsde

www.facebook.com/TwobirdsDE/

twobirds.com

Abu Dhabi & Amsterdam & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & San Francisco & Shanghai & Singapore & Stockholm & Sydney & Warsaw