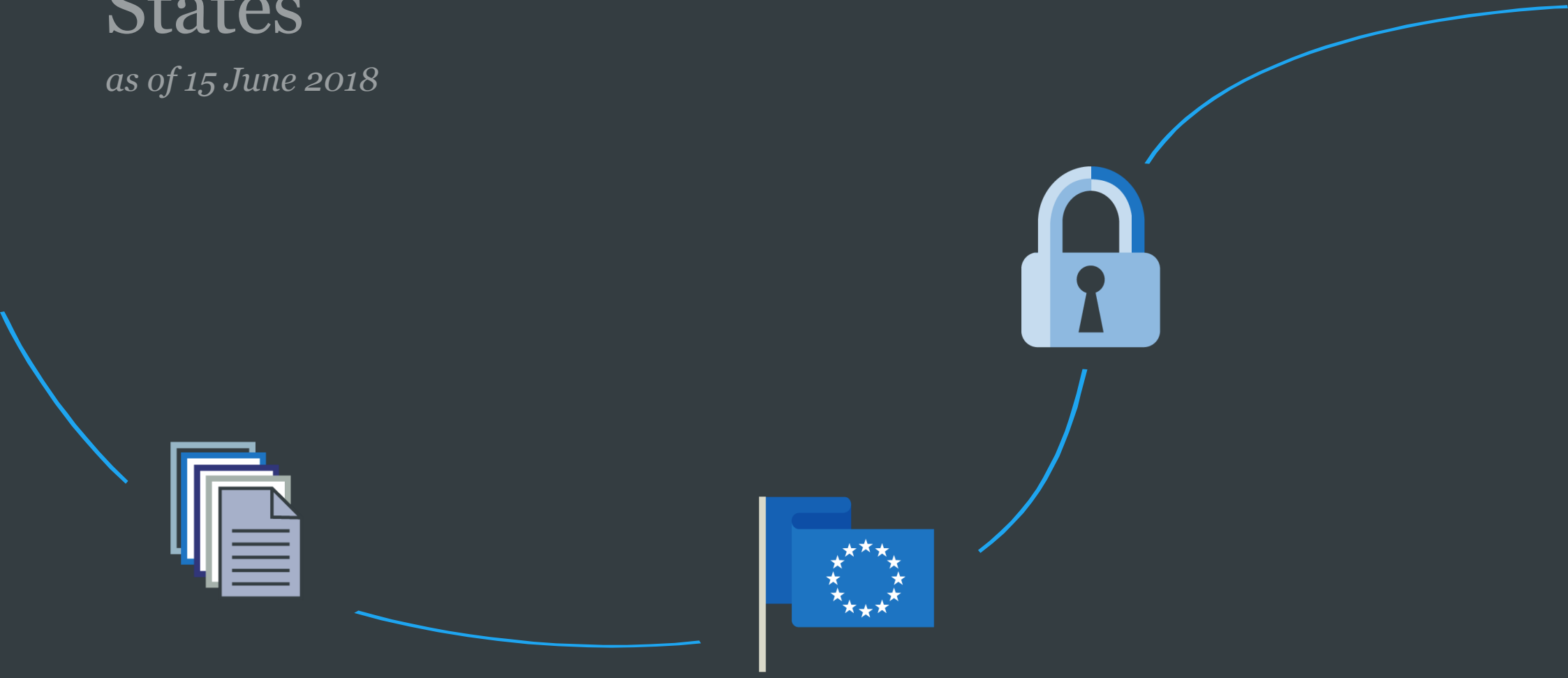
Bird & Bird & developments on NIS Directive in EU Member States

as of 15 June 2018



Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
Austria	The NIS Directive has not yet been adopted in Austria. Although a corresponding draft law was announced for mid-2017, no draft has yet been published, probably due to the early Austrian elections which were held in October 2017. As the new Austrian government was yet sworn in on18 December 2018, there are no updates on the envisaged Austrian Cybersecurity Act (Cybersicherheitsgesetz)at present stage, which shall adopt the NIS Directive into Austrian national law.	N/A	N/A	N/A	N/A	N/A	N/A	As the new Austrian government was sworn in on 18 December 2017, we expect the (draft) law adopting the NIS Directive, i.e. the (draft) Cybersecurity Act (Cybersicherheitsgesetz)to emerge at a later date (probably in Spring 2018).
Belgium	In progress. On 20 July 2017, the ministerial cabinet has taken note of the general implementation framework of the NIS Directive.	N/A	N/A	N/A	N/A	N/A	N/A	The legislator will have to coordinate the new obligations with some existing legislation, such as the Law of 1 July 2011 on the security and protection of critical infrastructures.
Bulgaria	Not yet finalized but there has been some development.	The implementation act currently exists in the form of a draft, named the Cybersecurity Act, which has been	No identification of the operators of essential services has been made yet. According to the said ordinance, the NIS	Each administrative body which provides electronic administrative services shall designate a civil	Article 64 of the Electronic Government act provides for administrative fines ranging from BGN	The Network and Information Security Directorate shall provide support to the State e-Government Agency by	Article 24 of the Cybersecurity Act (draft) deals with jurisdiction. It stipulates that a digital service	According to the Director of the Network and Information System Security Direction, a general overview of

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
		approved by the Council of Ministers on 16th of May and is now to be submitted for discussion and voting in the National Assembly of Bulgaria. Meanwhile there is an effective ordinance which provides for general requirements for security of network and information systems (in force since 2008, last amended on 17 January 2017). The ordinance was approved on the ground of Art. 43, par. 2 of the Electronic Government Act, which stipulates that the Council of Ministers adopts an ordinance to specify the general requirements for the NIS security.	policies of the administrative bodies have to comply with the requirements of the NIS Directive. The Cybersecurity Act (draft) defines the requirements for the operators of essential digital services for each sector, subsector and services listed in the Appendices thereto. It stipulates that the following criteria shall be taken into account when defining the operators of essential services: 1. the entity provides a service that is essential to the maintenance of particularly important public and / or economic activities; 2. the provision of that essential service is dependent on the network and information security of the entities; 3. network and information security incidents would have significant disruptive effects on the provision of that service. Also the Chairperson of the State Agency for Electronic Management shall create and maintain a register of the	servant/unit to be responsible for network and information security. In case of a network and information security incident, the civil servant/unit must immediately document and report it to the administrative manager and the National Response Center for Network and Information Security Incidents at the Administrative Bodies Information Systems. The civil servant/unit periodically (not less than twice a year) reports to the head of the administrative body on the status of the network and information security (Appendix 2 to the Ordinance).According to Art. 19, paragraph 3 of the Cybersecurity Act (draft) the operators of essential digital services shall immediately notify the relevant Computer security incident response team of all incidents, including those that have a significant impact on the continuity of the essential services.	500 up to BGN 3,000 in case of a violation of network and information security measures, committed or admitted by civil servants. In case of repeated violations the fines increase and shall range from BGN 1,000 up to BGN 5,000. Article 28 and Article 29 of the Cybersecurity Act (draft) provide for administrative fines ranging from BGN 30, 000 up to BGN 150,000 in case of failure to perform the reporting obligations under this Act. In case of a repeated violation the fines increase and shall range from BGN 150,000 up to BGN 300,000. Liability for other violations of the Act is also foreseen.	developing and implementing the functions of a National Information Security Incidents Response Center in the event of accidents affecting the information security, as well as in carrying out the state policy in the field of network and information security. The Directorate coordinates the performance of the network and information security policies, related to the e-government functioning. At the level of the administrative bodies the Head of the particular body is directly responsible for the network and information security. The Cybersecurity Act (draft) provides for establishment of a system of competent authorities in the field of network and information security, clearly defining their obligations and responsibilities.	provider falls under the jurisdiction of the EU Member State in which it has its main establishment.	the legislation for compliance with the NIS Directive has been completed until now and a detailed analysis will be prepared. As of now, the analysis of the Bulgarian law is finalized and the second stage is the comparative law analysis of foreign legislation with respect to the implementation of the NIS Directive. Currently, the implementation process is almost complete as there is a draft of Act approved by the government, but on the other hand there is no clarity as to when it will become effective.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			operators of essential digital services as well as the essential services themselves. It is foreseen that the administrative bodies shall use networks and information systems that comply with the requirements of the Cybersecurity Act (draft).	Digital service providers shall also inform without undue delay the operators for any incident that has a significant impact on the essential services they provide.				
Croatia	The NIS Directive has not yet been adopted in Croatia. The National Cyber Security Council adopted at its session on 18 May 2017 a decision on the establishment of a Council working group for the implementation of the NIS Directive. As per information we were provided by the National Cyber Security Council, draft of the implementation act was made by their working group and was available for the public consultation until mid-February 2018. The draft was confirmed by the Government which passed it to the Parliament. The first round of	N/A	N/A	N/A	N/A	N/A	N/A	According to National Cyber Security Council the NIS Directive will be implemented in Croatian legislative system by way of passing the new act which will transpose the provisions of the directive. First draft of the new act will be publicly available by the end of January 2018, when the public consultations on provisions of the act will commence. The final version of the act is expected by the end of March, which will leave enough time for the act to be adopted by the Croatian Parliament until deadline prescribed in the NIS Directive.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
	legislative procedure before the Parliament was finished on 10 May 2018. All of the opinions, suggestions and amendments proposed on that session shall be included for the second (and final session) before the Parliament. The second session has to be held in 6 months period, however, it is expected that the implementation act will be adopted before the Parliament's summer break. The draft is still subject to amendments in accordance with accepted changes which will be proposed by the Parliament members during the Parliament stage of the implementation.							
Cyprus	The NIS Directive has been implemented in Cyprus on 5 April 2018	Network and Information Security Law of 2018 (Law 17(I)/2018)	No identification of the operators of essential services has been made yet. According to Article 2 (1) of the Draft Law, operators of essential services means a	Operators must notify the competent authority without undue delay of any incident having a substantial impact on the provision of the services. Providers of	Section 15 of the Draft Law provides that any person who prevents any employee of the competent authority to fulfil his duties is guilty of an offence	The Cyprus Digital Security Authority is an independent authority which is competent for the information security at national level, including the	Operators of critical infrastructures are subject to Cyprus law if the infrastructure is located in Cyprus.	

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			public or a private entity of a type referred to Annex II of the Directive which meets the below criteria: (a) the entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information system and (c) an incident would have significant disruptive effects on the provision of that service.	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.	and subject to imprisonment of up to 6 months and / or to a fine of up to EUR 8,000. Section 16 of the Draft Law provides that any person who breaches the 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 8,000. Section 29 of the Draft Law provides for administrative fines of up to EUR 8,500 for violations of the Law or the decisions of the competent authority. The fine referred to Article 15 and Article 16 of the Law is up to EUR 10.000 and not up to EUR 8.000. Article 30 of the Law provides for administrative fines of up to EUR 8,500 for violations of the Law or the decisions of the competent authority	prosecution and repression of administrative fines.		
Czech Republic	Czech NIS Directive Implementation Act, in effect as of 1 August 2017.	The Act No. 205/2017 Coll. (Collection of Acts part 74) amends Act No. 181/2014 Coll. on Cyber Security, as	Pursuant to Art. 5 of the NIS Directive, the Czech legislator has specified the criteria to identify operators of the following	Certain authorities and persons (listed in Section 3(b)-(f) of the CSA) are required to report cyber-security incidents in their	Section 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 200,000, in particular	The National Cyber and Information Security Agency is the central authority competent for the cyber security on a	Providers of digital services are subject to the CSA if: • Their seat is located in the Czech	The key requirements set out in the NIS Directive ("Directive") have already been part of the Czech Cybersecurity Act as

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
		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.	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(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.	significant network, the Critical Infrastructure Information System, Critical Information Infrastructure Communication System, Basic Service Information System, or Significant Information System, without delay after detection (Section 8(1) of the CSA). They either report the cyber security incidents to the national CERT or the National Cyber and Information Security Agency (Section 8(2),(3) of the CSA). Authorities and persons not listed in Section 3 of the CSA can report to either the national CERT or the National Cyber and Information Security Agency (Section 8(6)). 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	in the following cases: • 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. • Providers of digital services does not introduce/carry out security measures. Section 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 40,000, in particular in the following cases: • Providers of electronic communication services, entities operating an electronic communication network or authorities	national level (Section 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 (Sections 17 and 20 of the CSA).	Republic (Section 33 of the CSA); or • Their seat is located outside of the EU, but their representative is located in the Czech Republic (Section 3a of the CSA)	of 1 January 2015. The changes required 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.,:

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
				Information Security Agency (Section 8(1)). 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 (Section 8(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 (Section 8(8) of the CSA). The type, category and assessment of the significance of the cyber security incident's impact, as	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. • 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			•Asset assessment rules (impact of intrusion of information security on individual assets) •Risk assessment rules (impact, threat and vulnerability assessment) •Overview of vulnerabilities and threats •Rules for data erasure and technical media disposal methods •Content rules regarding contracts concluded with significant suppliers of obligated persons •Requirements for individual security roles within the Cyber Security Committee and their competencies

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
				well as the requisites and means of reporting the cyber security incident shall be set out in implementing legislation (Section 8(7)).	and information. • 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. • Administrators or operators of the information or communication systems of critical information infrastructure do not notify the entities operating an electronic communication network. • 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			

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
					and information; or - do not destroy copies of data, operating data and information. • Authorities or persons operating a significant network do not report a cyber security incident. • 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. • Administrators or operators of the information or communication systems of a critical information infrastructure,			

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
					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. • 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. • 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			

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
					cyber security incident; or - do not fulfil its obligation to inform the public imposed by the National Cyber and Information Security Agency. • 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. Section 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 8,000, in particular in the following cases: • Operators of the information or communication systems of critical information infrastructure: - do not hand over data, operating data and information; or			

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
					- do not allow administrators to supervise the destruction of data, operating data and information. Section 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 400, in particular in the following cases: • 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.			
Denmark	12 new acts have come into force. Further, one bill is being processed for approval.	**Act no. 2017/1 LSF 135** Proposal for a Law on Security in Network and Information Systems in the Transport Sector Ministry of Transport, Building and Housing	Each of the acts are defining operators of essential services in each sector.	Each act sets out its own reporting scheme.	Breaches will generally be sanctioned by way of fines, unless the breach in question is so serious that another more stringent legislation applies to the specific situation.	Ministry of Transport, Building and Housing Ministry of Defence Ministry of Health and Elderly	Operators of digital services are generally subject to Danish law, if the headquarter or a representative is located in Denmark. However, each act will regulate this in	N/A

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
		Act no. 437 OF 08/05/2018 - In force Law on security in network and information systems for operators of major internet exchange points, etc. Ministry of Defence **Act no. 440 of 08/05/2018** - In force Law on safety requirements for network and information systems in the health sector Ministry of Health and Elderly **Act no. 436 OF 08/05/2018** - In force Law on network and information security for domain name systems and certain digital services (NIS Act) Ministry of Commerce **Act no. 441 of 08/05/2018** - In force Law on security in network and information systems in the transport sector Ministry of Transport, Building and Housing **Executive order no. 461 of 09/05/2018** - In force				Ministry of Commerce Ministry of Environment and Food Ministry of Energy, Supply and Climate	detail.	

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
		Executive Order amending the Executive Order on Management and Management of Banks, etc. Ministry of Commerce **Executive order no. 457 of 09/05/2018** - In force Declaration of Event Reporting for Operators of Essential Services Ministry of Commerce **Executive order no. 454 of 08/05/2018** - In force Executive Order on Security in Network and Information Systems for Operators of Essential Internet Exchange Points Ministry of Defence **Executive order no. 453 of 08/05/2018** - In force Executive Order on Security in Network and Information Systems for Operators of Essential Services in the Domain Name Area Ministry of Commerce						

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
		Executive order no. 452 of 08/05/2018 - In force Executive Order on Network and Information Security for Certain Digital Services Ministry of Commerce **Executive order no. 429 af 04/05/2018** - In force Executive Order on Requirements for Safety in Networks and Information Systems of Certain Water Supply (NIS Order) Ministry of Environment and Food **Executive order no. 425 of 01/05/2018** - In force Executive Order on IT Preparedness for Electricity and Natural Gas Sectors Ministry of Energy, Supply and Climate **Executive order no. 424 of 25/04/2018** - In force Executive Order on Preparedness for the Oil Sector Ministry of Energy, Supply and Climate						

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
Estonia	The NIS Directive has been implemented in Estonia by the Cybersecurity Act (CSA) that came entered into force on 23 May 2018.	The directive is implemented by the Cybersecurity Act (CSA).	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: 1) certain railway companies, 2) aviation (international aerodrome operators, providers of air traffic control), 3) certain port operators, 4) communications companies providing cable service to more than 10 000 end users; 5) 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; 6) family physician upon providing general medical care 7) certain domain name register administrators, 8) provider of communications, maritime communications and operational radio network of critical importance, 9) Estonian Public	Service providers 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	Section 18 of the CSA provides for fines in misdemeanour procedure of up to EUR 20,000, in case of not following requirements imposed on implementing security measures as set out in section 7(1)-(3) of the CSA.	The Estonian Information System Authority that operates under the Ministry of Economic Affairs and Communications shall have the roles of the competent authority referred to in Article 8 (1) of Directive and the single contact point referred to in Article 8 (3) and the computer incident response team referred to in Article 9 (1).	"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	

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			Broadcasting. The CSA specifies, that a 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 45	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 contingency of the digital service in another state, the competent authority will notify the affected state. No report is required if the provider has no sufficient access to information that are necessary to evaluate the impact and severity of the security incident.			representative in Estonia."	

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			vital services listed by law, but the list of providers of the vital services is not publicly available. According to the information on the website of Ministry of the Interior, there are currently 167 vital service providers.					
Finland	In April 2017, a working group of the Ministry of Transport and Communications of Finland published a closing report (9/2017) regarding their proposals for guidelines on how to implement the NIS Directive. The official government proposal on the implementation of the NIS Directive was given to the parliament on 19 December 2017 and was accepted in the parliament on 10 April 2018. The laws modificating the existing laws (no new law was proposed) came into force on 9 May 2018.	The necessary changes were made to existing sector specific acts. Altogether twelve Finnish acts were modified: the Information Society Code, 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.	According to the working group, the most functional way to determine the operators of essential services would be to regulate / specify the criteria in legislation. 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	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.	No proposed new sanctions; existing sanction regimes provided in the sector specific laws may apply.	Sector specific authorities will have competence for the supervision: The Energy Authority, the Finnish Transport Safety Agency, the Financial Supervisory Authority, the National Supervisory Authority for Welfare and Health, the Centre for Economic Development, Transport and the Environment and the Finnish Communications Regulatory Authority.	Not specified in the proposed modifications. The existing provisions on jurisdiction in the sector specific laws apply.	N/A

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			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.					
France	French NIS Directive Implementation Act has come into effect on 27 February 2018. A decree has been issued on the 23 May 2018.	Act n° 2018-133 of 26 February 2018 relating to implementation of EU provisions in the field of security. Decree n°2018-384 of 23 May 2018 relating to security of networks and information systems of essential service operators and digital service providers	A ministerial decree dated 23 May 2018 had identified the following sectors as essential services: a) Civil activities of the State. b) Judicial activities. c) Military activities of the State. d) Food. e) Electronic, audio-visual and information communications. f) Energy. g) Space and research. h) Finance. i) Water management. j) Industry. k) Health. l) Transport. Article 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	According to Article 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. According to Articles 7 & 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 once a year to the ANSSI an update of that list. The operators also need to keep this information at the disposal of the ANSSI in case of	At the moment, Article 9 of the Act provides for three criminal fines for the operators of essential services: - 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 €100,000; - directors that do not comply with their reporting obligation in case of an incident shall be punishable with a fine of €75,000; - directors that obstruct an investigation shall be punishable with a fine of €125,000. Article 15 of the Act provides for three	Article 8 of the Act provides that the National Agency for the Security of Information Systems (ANSSI) is competent to investigate and to issue formal demands asking to comply with the set of security rules.	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 (Article 11),	

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			decree of June 2006 according to article 5§2 of the bill. Article 2 of the decree provides that the operators 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	inspection.	criminal fines for the digital service providers: - 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 €75,000; - directors that do not comply with their reporting obligation in case of an incident shall be punishable with a fine of €50,000; - directors that obstruct an investigation shall be punishable with a fine of €100,000.			

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			service; - where applicable, sectoral factors. According to Article 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 ANSSI.					
Germany	German NIS Directive Implementation Act, coming into effect on 30 June 2017. The provisions on providers apply since 10 May 2018.	Implementation Act (Federal Law Gazette, BGBl. I 2017 of 29 June 2017, p. 1885) amends the Act on the Federal Office for Information Security ("FOIS Act"), Atomic Energy Act, Energy Industry Act, Social Insurance Code V,	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	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	Section 14 of the FOIS Act provides for administrative fines of up to EUR 50.000, in particular in the following cases: Operators of critical infrastructures wilfully or negligently - fail to properly	The FOIS is competent for the information security at national level, including the prosecution and repression of administrative offences (Section 1 and 14 para. 3 of the FOIS Act). The FOIS operates under the	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	The key requirements set out in the NIS Directive ("Directive") have already been part of the German 2015 IT Security Act ("ITSA"). Accordingly, the ITSA had a front-runner role for the Directive. In light of the ITSA, the changes required to

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
		and the Telecommunication Act.	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).	led [might lead] to a failure or significant impairment of the operability of the critical infrastructure (Section 8b para. 4 of the FOIS Act). Providers of digital services must immediately report to the FOIS any security incident that has significant impact on the provision of the digital service provided the EU (Section 8c para. 3 of the FOIS Act). The term "significant" is in particular determined by the implementing acts pursuant to Art. 16 para. 8 of NIS Directive. No report is required if the provider has no sufficient access to information that are necessary to evaluate the impact of the security incident.	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 technical and organisational measures to tackle risks for the security of the network and information systems - fail to properly report as described above. 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) where it has no establishment in another EU member state, has	authority of the German Federal Ministry of the Interior.	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 Germany (provided, of course, that information security in Germany is concerned, see "competent authorities").	German law resulting from the Directive were relatively small.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
					appointed a representative there and offers the digital services in that EU member state. Further, the Implementation Act amends the sanction rules under the Atomic Energy Act, Energy Industry Act, Social Insurance 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 Insurance Code V; and - up to EUR 500.000 under the Telecommunication Act.			
Greece	NIS Directive has not been implemented yet in Greece	-	-	-	-	-	-	-

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
Hungary	The provisions of the NIS Directive have been implemented into the Hungarian legal system.	The main implementing legislation are: - "Act 134 of 2017 on modifying certain interior related tasks and corresponding laws" and - "Government Decree 394/2017 (XII.13) on modifying government decrees related to Act 134 of 2017 on modifying certain interior related tasks and corresponding laws".	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.	Providers of registration-obliged services (online marketplace, cloud computing services, online search engine; jointly "Digital Services") must immediately report significant incidents in relation to network and information systems that have significant effects on their services offered within the EU to the General Directorate for Disaster Management of the Ministry of Interior ("Directorate"). The reporting obligation must be fulfilled primarily electronically or in exceptional cases by any other available method. The reporting must include at least the (i) description and status of the incident, (ii) the extent of the disruption, (iii) contact details of the incident response person appointed by the provider, (iv) the aspects that define the effect of the incident.	Annex 1 of Government Decree 410/2017 (XII.15) 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 notify the Directorate about significant incidents. The amount of the statutory fines are rather low compared to other EU members states and depend on the type of breach. The amount of the administrative fine ranges between HUF 50,000 (~ EUR 165) and HUF 5,000,000 (~ EUR 16,500). The amount of fine may not exceed HUF 5,000,000 even in case of multiple breaches, however fines may be imposed for the same breach multiple times every two months. Section 9 (2) of Government Decree 65/2013 (III.8) specifies the amount of administrative fines	**Directorate** Responsible for (i) receiving incident reports of providers of Digital Services, (ii) ensuring that providers of Digital Services comply with applicable regulations and (iii) imposing fines on providers of Digital Services. **Special Service for National Security** Serves as the national competent authority on the security of network and information systems as defined in Art 8 (2) of the NIS Directive and as the governmental incident response authority.	**Providers of Digital Services** The provisions of Act 108 of 2001 on e-commerce and information society services (the act being applicable to providers of Digital Services, "**E-commerce Act**") specifies that the E-commerce Act is applicable 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 members 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 in the territory of Hungary.	N/A

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
				Whether the incident is significant must be determined based on several aspects including the number of affected users, the duration and geographical scope of the incident, the level of disruption in the services and its economical/social effects (in line with Art 16 (4) of NIS). Operators of essential services must immediately report extraordinary incidents to the Directorate and to other competent authorities as defined by Hungarian laws and regulations.	that may be imposed on operators of essential services for breach of any obligations defined by the applicable laws. The amount the administrative fine ranges between HUF 100,000 (~EUR 330) and HUF 3,000,000 (~EUR 9,900).		The provisions of the E-commerce Act regarding providers of Digital Services are not applicable to micro and small enterprises.	
Ireland	The Irish NIS Directive implementation bill has not yet been published and a date for publication is not currently available. The Irish Department of Communications, Climate Action & Environment (a government department) published a consultation paper on the proposed approach to take on	According to the Irish Government's Spring / Summer 2018 legislative programme it is intended that the Cyber Security Bill (not yet published) will transpose the NIS Directive. The legislative programme cites that preliminary work is currently underway on the Bill.	No official information has been made publicly available at the date of preparation of this report. However, the Department of Communications, Climate Action & Environment has noted that those entities likely to be formally designated as operators of essential services (OES) once the legislation is in place have been informed	N/A	N/A	The competent authority will be the National Cyber Security Centre, which is an office of the Department of Communications.	N/A	The consultation paper is helpful in providing indicative terms that may appear in the legislation, once enacted.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
	the NIS Directive in November 2017, with the deadline for submissions having closed on 20 December 2017.		as such.					
Italy	On February 8, 2018, a scheme of a legislative decree which implement the NIS directive has been approved by the Italian Government and submitted to the scrutiny of the Parliament. On May 16, 2018 the Italian Government has approved the scheme, but the final text (with some small amendment coming from the Parliament) has not yet been published.	The final version of the implementation act has not yet been published. However, the scheme of legislative decree approved on 8 February 2018 should contained a large part of the definitive text.	There is not yet an Italian criteria for the determination of "operators of essential services" in the Italian landscape, which should be identified by the deadline of November 9, 2018. However, the scheme of the Legislative decree refers to the definition provided by the NIS Directive.	Operators of essential services must immediately report to the Italian CISRT, and for information to the competent NIS Authority, the incidents which have a significant impact on the provision of the essential services provided. Digital Service Providers also, in case of incidents which have a relevant impact on the provision in EU of a digital service included between those indicated in annex 3 to the NIS directive, must immediately report to the Italian CISRT, and for information to the competent NIS Authority.	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 € 12,000 to a maximum of €150,000.	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	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.	

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
						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		
Latvia	The Ministry of Defence in	The provisions of the NIS Directive will	The draft of the amendments to the	The Law On the Security of	The Committee has the right to enforce its	The Draft Law defines the	In case that a digital service provider or its	The Draft Law, although supposed to

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
	cooperation with the Security Incidents Response Institution has proposed a transposition of the NIS Directive provisions into national law. The amendments to the applicable law were passed for discussion at the Cabinet of Ministers on May 3, 2018 and as of now, the implementation is still in progress.	amend the 2010 Law On the Security of Information Technologies as well as separate Cabinet regulations.	Law On the Security of Information Technologies (hereinafter - the Draft Law) stipulates the criteria for an essential service provider and an essential service. It provides that: 1) the service provider is a state or local government institution, or a private legal entity; 2) it carries out an economic activity in Latvia; 3) it provides a service in the European Union in a particular sector; 4) the service provided by it is essential for social or economic activities; 5) the providing of this service is dependent on network and information systems; 6) a safety incident may cause a significant interference with the providing of the service.	Information Technologies already provides 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 is left to discretion. The Draft Law adds 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 will determine the criteria for materiality of a security incident both to essential service providers and digital service providers.	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, Article 21 of the NIS Directive on sanctions is being implemented.	Committee as the competent authority under the NIS directive. In relation to it, the law 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.	representative is seated in or providing its services in Latvia, the Latvian law will apply.	implement the NIS Directive provisions on May 9, 2018, is still in the reviewing phase in the Cabinet of Ministers, and as provided to us by state officials on a no-name basis, will be finalised in August 2018 the soonest.
Lithuania	The Ministry of National Defence has submitted the draft amendment to the Cybersecurity	NIS directive will be implemented into Lithuanian law by amendments to the Cybersecurity Act	Article 2 (6) of the draft amendment to the Cybersecurity Act defines Operator of Essential Services as	Article 11 (1) para. 3 of the draft amendment to the Cybersecurity Act entails that subjects	N/A	Article 4 of the draft amendment to the Cybersecurity Act lists the competent authorities for	N/A	As the amendments to the Cybersecurity Act are yet to be approved by the Parliament, the

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
	Act, which is pending approval by the Parliament.	and the Code of Administrative Offenses.	a person managing a system of essential information infrastructure. According to Article 2 (5), essential information infrastructure is a communications or information system, a part of it, or a group of such systems in which a cybernetic incident could have a significant negative impact on national security, state economy or interests of the state or its society. The following sectors are considered to be essential by the Government of the Republic of Lithuania: (i) energy; (ii) information technology and electronic communications; (iii) water supply service; (iv) food production; (v) healthcare; (vi) finance; (vii) transport and mail; (viii) public security and legal order; (ix) industrial sector, chemical and nuclear sub-sectors; (x) state administration; (xi) civil safety; (xii) environmental; (xiii)	of cybernetic security (entities managing state information resources; operators of essential services; providers of public communications networks or electronic communications services; providers of electronic information hosting services and digital services) must, in accordance with the procedures laid down in the National Cybernetic Incident Management Plan, inform the National Cyber Security Center about cybernetic incidents that occurred in communication and information systems managed or handled by them. Article 11 (1) para. 4 obliges subjects of cybernetic security to inform the State Data Protection Inspectorate (in accordance with the procedure established by this authority) about cybernetic incidents related to personal data security violations that occurred in		cybersecurity in Lithuania: - The Government of the Republic of Lithuania, which sets out the strategic goals and priorities of the cybersecurity policy as well as the measures necessary to achieve them; - Ministry of National Defence of the Republic of Lithuania, which shapes the cybersecurity policy and organises, controls and coordinates its implementation; - The National Cyber Security Center, which implements the cybersecurity policy and is involved in the formation of cybersecurity policy; - The State Data Protection Inspectorate, the Police and other institutions whose functions are related to cybersecurity are involved in implementing the cybersecurity policy. Detailed tasks and powers of the competent authorities for cybersecurity in Lithuania are		provisions related to the implementation of the NIS Directive are not final. It was proposed that while implementing the NIS Directive, the list of entities subject to administrative liability in accordance with the Code of Administrative Offenses for infractions related to communication systems should be widened by: - establishing administrative responsibility for all cyber security entities for non-compliance with organizational and technical cybersecurity requirements; - establishing administrative responsibility for all cybersecurity entities that are obliged to provide information on the cybersecurity statutes and fail to do so. There is no publicly available information about the status of this proposal.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			national defence; (xiv) foreign affairs and security.	communication and information systems managed or handled by them, or, in communication and information systems used for electronic communications services, electronic information hosting services and digital services. According to Article 18 of the National Cybernetic Incident Management Plan, operators of essential services, providers of public communications networks or electronic communications services as well as providers of electronic information hosting services must seek help from the National Cyber Security Center in cases where they conclude that they will not be able to self-manage a cybernetic incident within permissible time deadline.		described in Articles 5 - 10 of the draft amendment to the Cybersecurity Act.		
Luxem-bourg	NIS Directive has not been implemented yet in Luxembourg. There are preparatory works that are	-	-	-				

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
	taking place with respect to the implementation of this directive, in particular with the Financial Supervisor (CSS) and with the Telecom Regulator (ILR)							
Malta	The final draft of the Order that will implement the NIS Directive into Maltese law has been completed by a specialised unit within the Maltese Ministry for Home Affairs and National Security and has been published after having undergone public consultation. It should be finalised in the near future. It is being assumed that the Draft Order will be implemented into Maltese law by means of a Legal Notice.	Draft Order entitled "Measures for high common level of security of network and information systems Order" (hereafter referred to as the 'Draft Order').	It is the CIIP unit (the competent authority) that shall establish the criteria for the identification of Operators of Essential Services ('OES'). Operators of Essential Services shall be established from the sectors and sub-sectors listed in the Second Schedule of the Draft Order, namely: Energy, Transport, Banking, Financial Market Infrastructure, Health Sector, Drinking water Supply and Distribution and Digital infrastructure.	OES will be obliged to report any events/ incidents disrupting the delivery of their services to the competent authority, namely the CIIP unit.	Details regarding the administrative fines which can be imposed under the provisions of this Order, once it is made law, have not been published in the Draft Order.	The 'competent authority' responsible for the NIS directive will be the “Critical Information Infrastructure Protection (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.	N/A	It is worthy to note that local laws transposing EU Directives are generally implemented into Maltese law by means of a Legal Notice issued under the relevant Act. Although in this case the draft law is being referred to as an 'Order', in all likelihood it will nonetheless be implemented through a Legal Notice once it is finalised. This is however yet to be seen. The finalised law should be published in the coming days.
Nether-lands	In the Netherlands, the NIS Directive will be implemented by the Security Network- and Information Systems Act, which currently exists in	Draft "Security Network- and Information Systems Act".	The draft implementation act states that essential operators will be appointed from the most of the same sectors as named in Annex II to the NIS-	Operators of essential services are obliged to immediately notify the following events to the National Cyber Security Centre (Article 10 of the draft	The draft implementation act provides for the following administrative fines: 1. up to EUR 5 million	The following authorities have been appointed as the competent authorities: - For the sectors	According to the draft implementation act, operators of essential services can be either private or public entities, but the draft does not contain a determination with	In addition to essential operators, an obligation to notify will exist for other 'vital providers', which will be appointed from (as a minimum) the sectors Nuclear

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
	the form of a draft. The draft was adopted by the House of Representatives on 29 May 2018 and will now be presented to the Senate, which is generally not able to make further amendments to the Act. The draft is expected to be adopted by Parliament this summer. The operators of essential services are expected to be designated before the deadline of 9 November.		Directive, namely Energy, Transportation, Banking, Infrastructure for the financial market, Supply of drinking water and Digital infrastructure. However, the government has repeatedly stated it is not planning to designate any operators from the healthcare sector as essential operators, because it considers the healthcare sector not sufficiently "high risk", as it is largely decentralised. A motion to designate healthcare operators as essential was submitted by a member of the House on 24 May 2018. This motion is currently being held to be dealt with at a currently unknown time. The essential operators will be appointed by governmental decree at a currently unknown date.	implementation 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 Cyber Security Incident Response Team and the competent authority (Article 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	for any breach of the draft implementation act by essential service operators or DSPs; 2. a maximum of EUR 1 million for failing to cooperate with a request for further information from the National Cyber Security Centre; and 3. a maximum fine of EUR 1 million for failure to adequately cooperate with supervisory authorities exercising their competencies.	Energy and Digital Infrastructure: the Minister of Economic Affairs and Climate Policy; - For the sectors Banking and Financial Market Infrastructures: the Dutch National Bank ("DNB"); - For the sectors Transport and Drinking water supply and distribution: the Minister of Infrastructure and Water Management; and - For the sector Health: the Minister of Health, Welfare and Sports. The Minister of Economic Affairs and Climate Policy has been appointed as the competent authority for DSPs. The competent authorities will (at a currently unknown date) appoint sectoral supervisory authorities.	regard to the territorial scope. However, departing from a related governmental decree (see under "Remarks"), application of the implementation 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 draft implementation act if their main establishment or representative is located in the Netherlands.	and Weirs. These other vital operators will be appointed by governmental decree. As of now, it looks like there will not be any supervision or sanctions for violation of the notification requirement by vital operators which are not classified as operators of essential services However, the parliamentary history of the draft implementation act specifically mentions that it might be decided that supervision and sanctions will be applied. N.B. The draft act implementing the NIS-Directive is antedated by a national law containing a notification duty (which entered into force on 1 January 2018) and is to be withdrawn as soon as the act implementing the NIS-Directive comes into force. Under this national law, there is no supervision and no sanctions apply to any breaches. Additionally, under the national law, vital operators (which

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
				consequences for the continuity of the digital service in question.				include operators from the sectors in Annex II of the NISD) have been appointed by decree. However, the selection of vital operators differs from the list of essential operators of the Directive, leaving, for example, the entire Healthcare sector out. It is to be expected, however, from the parliamentary history of the national law, that the list of essential operators and other vital operators to be appointed under the act implementing the NIS-Directive will be inspired by this selection.
Poland	The proposal of the National Cyber Security System Act (NCSA) is still work in progress (on the Parliament level), and there is no date of enactment set yet.	The National Cyber Security System Act - the text of the bill has been published on 30 April 2018, but may change during the works in the Parliament.	The Act states that essential operators will be appointed from the same sectors as mentioned in Annex II to the NIS-Directive, namely Energy, Transportation, Banking, Infrastructure for the financial market, Healthcare, Supply of drinking water, and Digital infrastructure. Essential operators will be appointed by the competent	Operators of critical infrastructure 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 Defence), CSIRT NASK (Computer Security Incident Response Team run by Academic Computer Network - National Research	Article 73 of the draft 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 critical infrastructure - fail to implement a security management system, ensuring in particular: management of	The competent authorities for cybersecurity are the ministers competent for the sector in which the given operators of critical infrastructure operate.	Operators of critical infrastructure are subject to Polish law and the NCSA if they have an organizational unit within the territory of Poland. The provision of digital services is subject to Polish law if the digital service provider has its registered seat in Poland (Article 17.1. of the draft NCSA).	The requirements set out in the NIS Directive have already been addressed in the National Strategy of Cyber Security of the Republic of Poland for the years 2017-2022. One of the main objectives of the Strategy is implementation of the NIS Directive.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			authority according to the criteria listed in the regulation issued by the Council of Ministers.	Instituteor), CSIRT GOV (Computer Security Incident Response Team led by the Head of the Internal Security Agency), Article 11.1.4) of the draft NCSA. Providers of digital services must immediately, but within no more than 24 hours, report a significant incident to the CSIRT NASK (Article 18.1.4) of the draft NCSA).	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; - fail to classify security incidents; - fail 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 critical infrastructure persistently violates the Act, causing: 1) a direct and serious threat to cybersecurity for defence, state security, public safety and order, or human life and health, 2) the threat of serious damage to property or serious difficulties in			

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
					providing key services - the competent authority will impose a penalty of up to PLN 1,000,000 (EUR 230,000).			
Portugal	According to non-official information of the National Cyber Security Center transcription for implementation is ongoing .Yet in stage of legislative procedure - the government approved the law proposal on 15 March 2018.	Legal Regime of Cyber Security" ("Regime jurídico da segurança do Ciberespaço") - the text of the project of Law is public but may not yet be final.	No final elements available yet but the project of Law includes Finance, Insurance, Health, Transportation and traffic, Energy, Water, IT & telecoms on the list of essential services.	No final elements available yet but the Project of Law states that (i)The Public Administration and critical infrastructures must notify the National Cybersecurity Center of incidents with a relevant impact on the security of networks and information systems and (ii) 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: a) the number of users affected; b) the duration of the incident; c) the geographical distribution, with regard to the area	No final elements available yet. Project of Law states that: (i) Very serious administrative offenses are punishable by a fine of EUR 1250 to EUR 2500, in the case of a natural person, and EUR 2500 to EUR 5000, in the case of a legal person (ii) Serious administrative offenses are punishable by a fine of EUR 250 to EUR 500, in the case of a natural person, and EUR 500 to EUR 1000, in the case of a legal person.	No final elements available yet. The Project of Law foresees that the National Center for Cybersecurity (CNCS), as the National authority for the Cybersecurity has regulatory, supervisory, enforcement and sanctioning functions and the power to issue cybersecurity instructions and to define the national level of cybersecurity alert.	No final elements available yet but Project of Law states that the Law will be applicable to digital service providers who have their headquarters in Portugal or, not having it, if they have designated a representative established in Portugal, considering that they provide digital services there.	From consultation of official websites of key sectors it is expected that Finance, Insurance, Health, Transportation and traffic, Energy, Water, IT & telecoms are on the list of essential services. The project of Law states that the provisions related with Security Requirements, Incident Notification and Enforcement will only come into effect six months after the implementation of the Law.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
				affected by the incident.				
Romania	In May 2018, the Romanian Parliament adopted the Law for ensuring a high common level of security of network and information systems which transposes the NIS Directive. On 24 May 2018, the law was transmitted for promulgation to the Romanian President. The Law will enter into force after the promulgation by the Romanian President, which is expected to take place in the next 20 days (under normal course of legislative process). The text of the law as approved by the Parilament is available here http://www.cdep.ro/pls/proiecte/upl_pck2015.proiect?cam=2&idp=17075	N/A	The law provides that, by 9 November 2018, the essential operators will be identified by the relevant Romanian authority (i.e.the Romanian National Center of Response to Cyber Security Incidents - CERT-RO) for the following sectors of activity: a) energy, b) transport, c) banking, d) financial market infrastructures, e) health, f) drinking water supply and distribution, g) digital infrastructure.	According to the law, the essential service operators and providers of digital services 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 Article16 of the NIS Directive. The notification procedure will be detailed in a technical norm which shall be adopted by CERT-RO.	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.	The Romanian National Center of Response to Cyber Security Incidents (CERT-RO).	The provisions of the law are applicable to (i) essential service operators which have the head office, branch, subsidiary, working point or any other form of representation in Romania and (ii) providers of digital services headquartered in Romania, or in other non-EU country which has a representative office in Romania (non-EU entities offering relevant services in Romania have to designate a Romanian representative). The security and notification requirements shall not apply to (i) undertakings providing public communications networks or publicly available electronic communications services which have special or exclusive rights for the provision of services in other sectors in Romania or another EU Country and (ii) to trust service	N/A

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
							providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.	
Slovakia	Slovakia implemented INC Directive by the Act No. 69/2018 Coll. On cybersecurity effective as of April 1, 2018.	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 April 1, 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 concreto the Act No. 145/1995 Coll. on Administration Fees as amended; the Act No. 73/1998 Coll. on	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	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	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	National Security Authority is responsible for cyber security sphere 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.	In case, that a digital service provider or its representative is seated in or providing its services in Slovak Republic then the Slovak laws are binding (Sec. 23).	It is clear that every company moving doing business in critical sectors and providing targeted services will need to reflect in their systems and processes the requirements of the NIS as well as the new law. 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.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
		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.	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	voluntary reporting of security incidents (Sec. 26).	of committing it, the duration, consequences and circumstances in which it was committed (Sections 30 and 31).			

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			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 recognised.					
Slovenia	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.	Act on Information Security (Official Gazette of the RS, No. 30/18; hereinafter: ZInfV).	Pursuant to Art. 5 of the NIS Directive, the draft bill specifies the criteria to identify operators of the following essential services: a) energy, b) digital infrastructure, c) water management and distribution, d) healthcare, e), transportation f) banking, g) financial markets	Pursuant to the draft bill, 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	Article 37 of the ZInfV provides for fines in misdemeanour 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:	“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	Pursuant to Article 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	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.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			infrastructure, h) food supply and i) 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 to be adopted in 6 (six) months following the adoption the ZInfV; to this day the Government has not adopted the said Ordinance); (ii) meet the criteria set out in Article 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 Government Ordinance to be adopted in 6 (six) months following the adoption of ZInfV (to	services. The draft bill also foresees the same obligation for the providers of digital services that provide such services in the EU and state administration authorities.	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. Article 38 of the ZInfV provides for fines in misdemeanour 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	authorities´ CSIRT. The Slovenian Information Security Administration operates under the authority of the Ministry of Government Administration. Slovenian Information Security Administration shall begin operating as of January 1. 2020, while the other authorities shall begin operating as of January 1. 2019.	social and economic activities in the Republic of Slovenia. ZInfV contains no other jurisdictional provisions, except in one case: According to Article 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.	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 January 1. 2020, when the Slovenian Information Security Administration shall begin operating, as the ZInfV proposes.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			this day the Government has not adopted the said Ordinance) and (iiii) are designated as such by the Government of Republic of Slovenia.		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. Article 39 of the ZInfV provides for fines in misdemeanour 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.			
Spain	The NIS Directive has not been implemented in	Not yet.	Pursuant to Article 2 of the draft this law	Pursuant to Article 18 of the draft, essential operators and digital	Article 36 of the draft law includes a set of assumptions where	Pursuant to Article 9 of the draft law, competent authorities	Pursuant to Article 2 of the draft the law	The Spanish legislator will have to coordinate the new

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
	Spain yet. Last 21 December 2016, the official public consultation period about the transposition of the mentioned Directive into the Spanish law ended. During a period of 21 days interested parties were able to send their comments about the transposition to the Spanish Ministry of Energy, Tourism and Digital Agenda (see the document here: http://www.minetad.gob.es/telecomunicaciones/es-ES/Participacion/Documents/consulta-previa-def.pdf). To date, we are not aware that next legislative steps have been carried out by the Spanish Government. The Spanish Government is currently working on the transposition of the NIS Directive which it is expected to come up in May 2018. Last 8 January, 2018 a public hearing period ended.	There is a draft law was made available to the public in early December 2017. Our input is based on this draft therefore this information may change.	will apply to: (i) Essential services dependent on networks and information systems present in the following sectors: Transport, Food, Financial and tax system, Administration, Space, Nuclear industry, Chemical industry, Research facilities, Water, Energy, Health and Information and Communication Technologies (TIC) and; (ii) Digital services that are online markets, online search engine and/pr cloud computing services.	service providers must notify the competent authority of any incidents that may have significant effects on their services. Notifications may also refer to events or incidents that may affect the networks and information systems used to provide the services, but that have not yet had a real adverse effect on that. Notifications will refer also to incidents that affect the networks and systems of the information used in the provision of the services indicated, whether it is own networks/services as if they are from external suppliers, even if they are providers of digital services subject to this law. The operators should make a first notification of the incidents without undue delay. In addition, operators should make other intermediate	infractions are deemed to exist under law. Infringements are divided into very serious, serious or minor infringements. A very serious infraction would be, e.g., the repeated breach of the obligation to report incidents. A serious infraction would be, e.g., the breach of the obligation to report incidents with significant impact on services. A minor infringement would be, e.g., the breach of the obligation to report incidents without significant impact on services. The draft includes the following penalties that should apply in case of an infringement (Article 37): (i) fines of EUR 500,001 to EUR 1,000,000 for very serious infringements; (ii) fines of EUR 100,001 to EUR 500,000 for serious infringements, and warnings of fines of up to EUR 100,000 for minor infringements.	in the field of security of networks and systems of information are the following: a) For operators of essential services: - 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. b) For digital service providers: the Secretary of State for the Society of Information and the Digital Agenda, of the Ministry of Energy, Tourism and Digital Agenda.	will apply to: (i) Essential services established in Spain. It will be understood that an essential services operator 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) Digital service providers 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	obligations 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.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
				notifications to update the information on the incidents and a final notification after the resolution of the incident.	The sanctioning body will determine the sanctions based on criteria established in the draft, such as the degree of culpability, number of users affected or the volume of billing of the offender.		European Parliament and the Council of 6 July 2016.	
Sweden	There is a proposition (Prop. 2017/18:205) regarding the implementation of the NIS Directive. The law which is proposed will, if the bill passes through parliament, enter into force on August 1, 2018.	Act (2018:000) on information security for certain operators of essential services and digital services providers Ordinance (2018:000) on information security for certain operators of essential services and digital services providers	Pursuant to Art. 5 of the NIS Directive, the proposed bill has defined essential services as 'a service that is important to maintain critical social or economic activity.' (freely translated). The Swedish Civil Contingencies Agency (MSB) specified the criteria to identify operators of the following essential services: a) energy, b) transportation, c) banking), d) financial markets infrastructure, e) health care, f) water management and g) digital infrastructure. MSB:s report establishes detailed assessment material to assist operators of essential services in deciding whether the directive is applicable to their service. MSB	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 a 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.	If the relevant authority finds that the supplier does not comply with the act or ordinance they can instruct the supplier to take actions. The request can be combined with a penalty fine. Further, the relevant regulatory authority shall decide on administrative fines from 5,000 SEK up to 10,000,000 SEK for not complying with the security requirements or incident notification.	Swedish Civil Contingencies Agency (MSB) is appointed CSIRT-unit. The regulatory authorities will be specified in a 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	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.	N/A

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			will present a catalogue of the identified criteria through a regulation, when the bill has been passed. Operators of essential services will without delay be obliged to report to the supervisory authority.			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		
United Kingdom	UK NIS Directive will be implemented into national laws on 9th May 2018. The Department for Digital, Culture Media & Sport commenced a public consultation in relation to the implementation on 8 August 2017 and published the Government's response to the public consultation in January 2018.	To be implemented into UK law on 9 May 2018 through section 2(2) of the European Communities Act.	In accordance with Art. 5 of the NIS Directive, the UK Government has proposed criteria to identify operators of the following essential services: a) Drinking water supply and distribution, b) Energy (including electricity, oil and gas), c) Digital Infrastructure, d) Health Sector, e) Transport (including air, maritime, rail and road) (all identified in Annex 1 of the Government Response to Public	All NIS incidents should be reported to the competent authority. Competent authorities will calculate incident reporting thresholds for each sector and/or sub sector and will publish such thresholds before May 2018. In order to define incident thresholds, competent authorities must determine what a significant impact would be in their sectors. The UK Government has stated that as a	The Government proposes that the penalty regime for the NIS Directive will include a maximum financial penalty of £17m, which will cover all contraventions, such as (for example) failure to cooperate with the competent authority, failure to report a reportable incident, failure to comply with an instruction from the competent authority, failure to implement appropriate and proportionate security measures.	The UK Government intends to take a multi authority approach to designating competent authorities to supervise each 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	The territorial scope of the UK's implementing legislation is expected to adopt 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	“The UK Cyber Security Strategy” was published on 1 November 2016, which sets out how the UK will address cyber security challenges over the next five years. The UK Government is working closely with the Devolved Administrations on the strategy’s application to Scotland, Wales and Northern Ireland. The UK Government considers its strategy is amongst the most comprehensive cyber strategies within the

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			Consultation from the Department for Digital, Culture, Media and Sport dated January 2018). The consultation paper proposed a series of thresholds so that the enactment will apply only to "more important operators" in each sector. The consultation responses highlighted concerns that the thresholds required further clarity. As a result, Lead Government Departments have refined the thresholds so that companies can identify with certainty whether they are in scope of the requirements of the Directive. The revised thresholds are also identified in Annex 1 of the Government Response to the Public Consultation. When considering these thresholds, the UK Government has taken into account the requirements of Art. 5 and Art. 6 of the NIS Directive. The thresholds are	minimum, the following parameters will be used: a) the number of users affected by the disruption of the essential service; b) the likely or actual duration of the incident; c) the geographical area affected by the incident. In addition, competent authorities may also use the following optional parameters: (d) the dependency of other sectors on the service provided by the affected entity; and (e) the impact that incidents have, in terms of degree and duration, on economic and societal activities, public safety or national security. The UK Government has stated that operators must report an incident without undue delay and, where feasible, no later than 72 hours after having become aware of an incident. The UK Government proposes to encourage the voluntary reporting of	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. In addition, the maximum penalties should be reserved for the most severe cases, , and it is expected that mitigating factors (including steps taken to comply with the NIS Directive, actions taken to remedy any consequences) and sector specific factors will be taken into account by the competent authority when deciding appropriate regulatory response. 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	retain responsibility for their jurisdiction. The NCSC will have 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 proposed competent authorities is included in Annex 2 of the Government Response to Public Consultation from the Department for Digital, Culture, Media and Sport dated January 2018. The list is subject to final confirmation and a definitive list will be included in the NIS Regulations. Proposed	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 on 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 DPS 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.	“The UK Cyber Security Strategy” was published on 1 November 2016, which sets out how the UK will address cyber security challenges over the next five years. The UK Government is working closely with the Devolved Administrations on the strategy’s application to Scotland, Wales and Northern Ireland. The UK Government considers its strategy is amongst the most comprehensive cyber strategies within the EU and believes that it addresses most of the requirements of the Directive. Those requirements that are not covered by the current strategy can be addressed through a NIS specific addendum to the strategy.

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			not intended to identify the systems that are in scope of the Directive, only the operators of essential services. Identifying the systems that support the services will be the responsibility of the operators. Alongside essential operators, Digital Service Providers (DSPs) will be required to comply with the requirements of the NIS Regulation which implements the NIS Directive in the UK. Companies that "normally provide a service for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" will be categorised as DSPs and will be within scope of the Directive if they are operators of an online market place, an online search engine or a cloud computing service. Despite the definitions that have been given there still remains significant	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	proceedings, and appealable through the court system. It is also proposed that breach of the NIS Directive is cumulative with any GDPR sanction. There may be reason for an operator to be penalised under different regimes for the same event because the penalties might relate to different aspects of the wrongdoing and different impacts. However, the NIS Regulations will include text which will encourage competent authorities to work with regulators in the event of different regimes applying to determine what approach to take. 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 in Annex 2: •Drinking water supply and distribution: In England, Department for Environment, Food and Rural Affairs (Defra) supported by the Drinking Water Inspectorate; In Wales, Welsh Ministers supported by the Drinking Water Inspectorate. •Energy- Electricity: In England, Scotland and Wales, the Department for Business, Energy and Industrial Strategy (BEIS) and the Office of Gas and Electricity Markets (Ofgem). •Energy- Gas (downstream): In England, Scotland and Wales, the Department for BEIS and Ofgem. •Energy- Gas (upstream): In England, Scotland and Wales, the Department for BEIS supported by the Health and Safety Executive. •Energy- Oil (downstream and upstream): In England, Scotland and Wales, the Department for BEIS supported by the Health and Safety Executive. •Digital Infrastructure:		

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
			room for uncertainty as to whether you qualify as a DSP.	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 (a) online marketplace; (b) online search engine; or (c) 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		The Office of Communications (Ofcom). •Health Sector: In England, the Department of Health, supported by NHS Digita; in Wales, Welsh Ministers. •Transport- Air: Department for Transport (DfT), acting jointly with the Civil Aviation Authority (CAA). •Transport- Maritime: DfT. •Transport- Road: In England and Wales, DfT. •Transport-Rail: In England and Wales, DfT. •Digital Service Providers: Information Commissioner's Office. The competent authority in Northern Ireland will be confirmed by the Northern Ireland Government Departments. The Government is working with the Scottish Government to determine the best arrangements for competent authorities in respect of devolved functions in Scotland.		

Country	Current status of implementation	Implementation Act	Determination of operators of essential services (Art. 5 NIS)	reporting obligations	sanctions regime	competent authorities	Jurisdictional applications	Remarks (if any)
				of criteria set out in the draft NIS Regulation which implements the NIS Directive. Additionally the draft Regulation provides that a relevant DSP must also have regard to the following (a) (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; (b) the duration of the incident; and (c) the geographical area affected by the incident; (d) the extent of the disruption to the service provision; and (e) 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.				

Contacts

Germany

Dr. Alexander Duisberg
Partner, Tech & Comms

Tel: +49 (0)89 3581 6139
alexander.duisberg@twobirds.com

Dr. Benedikt Vogel, LL.M.
Associate, Tech & Comms

Tel: +49 (0)89 3581 6346
Benedigt.vogel@twobirds.com

Follow us

@twobirds / @twobirdsde

www.linkedin.com/company/318488

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 & Shanghai & Singapore & Stockholm & Sydney & Warsaw