Impact of Cybersecurity Regulations on ICT Companies in the European Union

Access Partnership

May 2020

Contents

Impact of Cybersecurity Regulations on ICT Companies in the European Union

Executive summary

Cybersecurity requirements imposed on Information and Communication Technology ("ICT") entities in the European Union mainly come from two regulatory frameworks. It is often the responsibility of ICT entities to assess which framework applies to their services so they can provide reliable and secure services to customers in line with compliance requirements.

The first is an electronic communication framework adopted by the European Commission in 2002 with the aim of harmonising the EU electronic communication sector. The framework had several objectives, including ensuring privacy and confidentiality of personal data in the electronic communications sector.[1] This framework was later amended to ensure the security and integrity of services and networks. However, the necessary measures only applied to telecommunication providers, and did not affect non-telecommunication ICT entities.

The second framework was adopted by the European Commission in 2016 in the form of a Network and Information Systems Directive (NIS Directive). Its aim was to regulate security measures that apply to critical infrastructure sectors and that have enhanced ICT activities, as they play a crucial role in the wellbeing of people and society. The activities of companies currently affected by the NIS Directive had previously not been covered by the electronic communication framework, and affected entities had to evaluate to what extent provisions applied to their services. The framework distinguishes between operators of essential services (including digital infrastructure) and digital service providers. The NIS Directive imposes different obligations on them but specifically excludes telecommunication and trust service providers from its requirements.

The purpose of this paper is to provide an overview of these two frameworks, highlight the differences between them, examine what type of entities could be affected, and identify when and under what conditions one framework may exclude the other. Additionally, due to the different implementation of the NIS Directive in EU Member States, we will demonstrate "mixed" cases where one entity could potentially be considered a digital service provider in one EU member state, and an operator of essential services in another. In addition, we will discuss "mixed" cases where certain services could fall under the electronic communication framework and the NIS Directive, highlighting that affected entities must closely evaluate their services to determine which framework applies to each of their services.

This paper will also examine new requirements imposed under the recently adopted EECC Directive. The directive broadens the definition of telecommunication providers, potentially encompassing entities that are currently subject to the NIS Directive, and amends security obligations that apply to telecommunication providers. Finally, this paper will briefly assess whether provisions of the General Data Protection Regulation apply if an entity is already subject to one of the above-mentioned frameworks.

[1] It should be highlighted that in 1995 the EU data protection directive was issued which required data processors and controllers to take certain measures to protect personal data. The directive was later repealed by the General Data Protection Regulation.

Introduction

Access to the Internet and other electronic communication services has become a basic utility in todays globalised world. However, our digital dependence extends far beyond the use of electronic communications services to make phone calls, send messages, and surf the web. Daily, we use different applications and platforms to order goods and services. We also rely on the Internet at work for communication and storing data in the cloud, including sensitive data. It has therefore become crucial to protect the ICT industry against failures which may affect the wellbeing of people and disrupt a country's infrastructure and jeopardise its security.

Considering these risks, the European Commission adopted several directives in 2002 which aimed to harmonise the EU electronic communication sector. One of the objectives of harmonisation was to ensure privacy of personal data in telecommunications. The Commission later amended the framework, adding a requirement to ensure the security and integrity of services and networks to avoid disruptions of services. In both cases, telecommunication providers[2] were supposed to notify national authorities of the security breaches so that they could address the challenges and risks this caused and take rectifying measures.[3]

Non-telecommunication activities mostly fell outside of EU regulatory framework,[4] and Member States often either had only sector specific or no security rules to face the pending challenges to ensure cybersecurity protection in other sectors. It should be emphasised that obligations were placed on controllers and processors of personal data[5] first under the EU Data Protection Directive,[6] and then under the General Data Protection Regulation (GDPR).[7] The GDPR has effectively created a cybersecurity framework for the handling of personal data in the EU. However, these requirements were limited only to handling personal data and did not cover other activities critical to the functioning of the state and its people. Recent cybersecurity attacks on critical infrastructure from organised crime units, individuals, and even foreign governments undermines the infrastructure of EU states and served as a wakeup call to EU stakeholders to act.

As a result, the European Union adopted the Network and Information Systems Directive ("NIS Directive")[8] which required Member States to adopt a national strategy on the security of network and information systems, harmonise cybersecurity[9] standards, and ensure transparency and cooperation between different stakeholders in Member States and increased regional cooperation within the EU. The NIS Directive has also required Member States to extend cybersecurity obligations

---

[2] EU regulatory framework refers to providers of public communications networks (PECN) or publicly available electronic communications services (PECS), for convenience this paper will use notion "telecommunication providers" and unless indicated differently should mean both PECN and PECS.

[3] For example, in recent press release ENISA has reported that 157 telecom outages were reported by the 28 EU member states and 2 EFTA countries, in 2018 as part of the requirement imposed on telecommunication providers to report security incidence.

[4] It should be mentioned that the European Council has issued a Directive 2008/114/EC "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection". However, this directive was mostly limited to the energy and transport sectors, requiring Member States to determine entities of critical infrastructure within those sectors, and did not provide the same scope of application similar to the recent NIS directive.

[5] This paper will only briefly review requirement applicable to controllers and processors of personal data as there has been plenty of material written on this subject.

[6] EU Data Protection Directive" 95/46/EC which has been repealed by General Data Protection Regulation.

[7] General Data Protection Regulation (EU) 2016/679.

[8] NIS Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

[9] Recently passed Cybersecurity Act defines cybersecurity as *the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.*

to various stakeholders from operators of essential services in energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, and digital infrastructure to providers of digital services.[10] Digital services are services which most of us use for online shopping, online searches, sending emails, and storing data in the cloud. As a result, a great number of companies now fall under this regulatory framework and must comply with security requirements.

The European Commission has recently gone even further and established an EU-wide cybersecurity certification scheme via the Cybersecurity Act for ICT products, services and processes, aiming to harmonise cybersecurity standards to simplify compliance processes and ensure single standards apply throughout the EU.[11] The regulatory changes under this Cybersecurity Act and NIS Directive significantly broaden the types of activities which will now be subject to cybersecurity obligations.

The purpose of this paper is to provide more clarity about the current two cybersecurity requirements in the EU which may apply directly to telecommunication providers and other ICT companies covered under the NIS Directive, as well as to briefly review the upcoming changes to cybersecurity rules that apply to telecommunication providers under the recently adopted EECC Directive. Finally, this paper will analyse whether provisions of the General Data Protection Regulation apply if an entity is already subject to one of the two frameworks.

Both the electronic communications framework and requirements under the NIS Directive are meant to ensure cybersecurity, but have different addressees, impose different obligations and have different compliance procedures. This paper will explain that there is a significant risk that some entities may understand that they are covered under one regulatory framework, but actually be subject to a different framework with different requirements. Distinguishing between various obligations is key to ensuring compliance and the security and reliability of services.

This paper is divided into two sections. The first section analyses the types of services that could be covered under the NIS Directive by assessing cybersecurity requirements related to affected entities. It will then study how the directive has been implemented in Germany and the UK to evaluate similarities and differences. The second section analyses the regulatory requirements relevant to telecommunication providers, by assessing the services that could potentially be covered under the electronic communications regulatory framework. It then examines the regulatory requirements relevant to providers of such services to highlight the main obligations and the best way to navigate them to mitigate regulatory risks. The conclusion will provide a summary of regulatory obligations, as well as recommendations on how affected entities can mitigate regulatory risks and ensure compliance.

[10] In this paper only services of digital infrastructure and digital service providers will be reviewed.

[11] Cybersecurity Act.

Cybersecurity requirements based on the NIS Directive

The purpose of the NIS Directive was to create harmonisation for security requirements of network and information systems used by operators of essential and digital services in the EU, while at the same time allowing Member States to adopt and maintain rules which have higher requirements. The directive served as a catalyst in many EU Member States, paving the way for real change in the institutional and regulatory landscape regarding cybersecurity.[12] Nevertheless, NIS Directive implementation has significant inconsistencies, allowing for different classifications and entities affected, as well as different regulatory requirements. This section will highlight the requirements from the NIS Directive in relation to digital infrastructure operators and digital service providers. It examines how the directive has been interpreted in Germany and the UK to highlight some of the key issues that ICT companies should be aware of to avoid unnecessary regulatory risks.

The NIS Directive establishes security and notification requirements for operators of essential[13] and digital services. Operators of essential services are subject to more "burdensome" requirements compared to providers of digital services. It should be highlighted that security and notification requirements under this directive do not apply to telecommunication providers as those undertakings are subject to requirements from the electronic communication framework.[14] Before going into further detail about the relevant cybersecurity requirements, it is necessary to first provide a clear distinction between digital service providers (DSP) and operators of essential (OES) services.

Digital service providers (DSPs)

A digital service provider could be any legal person that provides digital services in one of the following categories:

- An online marketplace is a final place for the buying and selling of goods or services either on its website or on a trader's website that uses computing services provided by the online marketplace.[15] This category does not cover intermediaries or online services that only compare different prices of products or services and then redirect users to preferred traders. Online marketplace services are provided by enterprises such as eBay and Amazon.
- Online search engines allow users to perform searches on websites. This category does not cover search functions that are limited to a specific website and it also does not cover online services that compare prices of different products or services.[16] Online search engine services are provided by undertakings such as Google, Yahoo and Bing.
- Cloud computing services enables access to a scalable and elastic pool of shareable computing resources.[17] Cloud computing services are provided by undertakings such as Amazon Web Services, Microsoft Azure and Salesforce.

[12] Page 22 of the REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems.

[13] In this paper we will review only operators or digital infrastructure, other types of operators of essential services are outside of the scope of this paper. The directive does not apply in relation to trust service providers as those are covered under different framework. Trust service providers are outside of the scope of this paper.

[14] Article 1(3) of the NIS Directive for more information on security and notification requirements please see Cybersecurity obligations to telecommunication providers in this paper.

[15] For further information please see Recital 15 of the NIS Directive.

[16] For further information please see Recital 16 of the NIS Directive.

[17] For further information please see Recital 17 of the NIS Directive.

If the first two categories are relatively straightforward, then cloud computing services are much more ambiguously defined, encompassing a wide range of undertakings.

In the UK, the Information Commissioner's Office responsible for overseeing DSPs has provided its guidelines on the interpretation of cloud computing services and has concluded that "the term primarily, but not exclusively, includes the following types of cloud computing services":[18]

a) Software-as-a-Service (SaaS) providers: only to the extent that they provide a scalable and elastic pool of resources to the customer;

b) Platform-as-a-Service (PaaS) providers; and

c) Infrastructure-as-a-Service (IaaS) providers.

The guidelines further emphasise that there are other types of companies and mixed services that could be covered under the cloud computing definition if their services enable access to a scalable and elastic pool of shareable computing resources. The European Commission has also studied the definition and has provided an overview of the above-mentioned services.[19]

NIS Directive requirements apply to all DSPs unless they employ less than 50 people, with an annual turnover and/or annual balance sheet total not exceeding EUR 10 million.[20] If a DSP is not established in a Member State, but still provides services in the European Union, it shall designate a local representative in at least one EU Member State where services are provided.[21] It is therefore the responsibility of the DSP to determine whether it is subject to the national cybersecurity framework and to identify which national authority its activities will be subject to.

It should be noted that if an undertaking is a DSP, then pursuant to the provisions of the NIS Directive it should be subject to the regulatory requirements based on where it has designated its representative or has its main establishment. The question is whether a DSP will only be subject to potential penalties for noncompliance in that jurisdiction. The NIS Directive does not provide a clear answer to that question and does not clarify which national regulatory framework will apply. Therefore, DSPs must assess how the Directive is adopted in each Member State in which they operate and whether penalties in other jurisdictions could apply. As will be explained below, penalties for noncompliance vary significantly and DSPs thus have a significant financial incentive to evaluate the various local implementations of the NIS Directive and potential consequences for non-compliance.

Finally, it should be highlighted that the regulatory approach of the EU Member States in defining DSPs has generally been harmonised, and as an example, neither Germany nor the UK have significantly deviated in defining DSPs during the transposition of the directive into their national legislation.

Operators of essential services (OESs)

Within the Digital Infrastructure sector, three service types have been identified in the NIS Directive to potentially be considered as OES:[22]

[18] For further information please see The guide to NIS - Digital service providers.
[19] European Commission and the Council COM (2017)476 final/2 - Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union pages 32-35.
[20] Article 18 of the NIS Directive together with Commission Recommendation 2003/361/EC.
[21] Recital 64 of the NIS Directive.
[22] For more information please see Art 4 (13-16) and Recital 18 of the NIS Directive.

- Internet exchange point (IXP) – is defined as a network facility which enables the interconnection of more than two independent autonomous systems, to facilitate the exchange of Internet traffic. IXP services are provided by undertakings such as DE-CIX, AMS-IX, LINX and Equinix.
- Domain name system (DNS) – is defined as a hierarchical distributed naming system in a network which refers queries for domain names. DNS services are provided by undertakings such as Euro DNS and Verisign.
- Top-level domain (TLD) name registry – is defined as an entity which administers and operates the registration of Internet domain names under a specific top-level domain. DNS services are provided by undertakings such as Verisign and Afilias.

The NIS Directive further provides a list of criteria for Member States to identity OESs.[23] However, the criteria is ambiguous and Member States are free to impose specific parameters to identify OESs. As a result, an undertaking could be considered an OES in one Member States and not in another. Additionally, Member States are free to expand the list of OES providers. For example, Germany extends cybersecurity requirements to services which are clearly not identified as OES under the NIS Directive.

As opposed to DSPs, Member States are required to identify OESs established in their jurisdictions. Unlike DSPs, however, establishment does not imply corporate establishment, but rather where the effective and real exercise of activity through stable arrangements takes place,[24] and as a result an entity could be identified as an OES in several EU Member States.

Finally, it should be highlighted that some EU Member States have adopted a top down approach where national authorities inform the operator of their classification as an OES, while others have adopted a bottom up approach, requiring operators to identify and notify themselves to the authorities.[25] [26] Before reviewing how OESs are defined and regulated in Germany and the UK to illustrate their individual national approaches, it is important to highlight the requirements imposed on DSPs and OESs by the NIS Directive framework.

What are the relevant regulatory requirements for DSPs and OESs?

DSPs must identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use to provide services within the EU. Being aware of the most current measures will ensure a level of security for network and information systems corresponding with the risk posed.[27]

In addition, DSPs must without undue delay report any incident that has a substantial impact on the provision of its services to the relevant authority. An incident that has a substantial impact on services

[23] Article 5(2) of the NIS Directive.
[24] For more information please see Recital 21 of the NIS Directive.
[25] Recital 25 of the NIS Directive.
[26] The European Commission has found that Member States have diverged significantly in their approaches to identifying OESs. They find part of this divergence may stem from some Member States putting the onus of identification on the affected entities, while others put the obligation to identify affected parties on the regulator. For more on this please see page 8 of the REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems.
[27] For further information and a list of other measures please see Article 16(1) of the NIS directive together with Regulation (EU) 2018/151 which further specifies the factors required to take into account when assessing risk management.

is specified by the Commission under Article 16 (4) and Regulation (EU) 2018/151.[28] It also describes factors that should be taken into account when managing risks and the parameters for determining whether an incident has had a substantial impact or not.

It should be emphasised that the NIS Directive recommends that national authorities take a light-touch approach to DSPs, aiming for ex post regulation only justified by the nature of services provided or their scope of operations. Unless provided with evidence that a DSP does not comply with the requirements, national authorities are generally not obliged to supervise DSP activities.[29]

OESs are subject to similar but more stringent obligations as DSPs are.[30] The NIS Directive, however, requires OESs to additionally show the security of their networks and information systems. For example, by conducting security audits. Following an assessment, the national authority has the power to issue binding instructions to the OES to remedy the deficiencies identified.[31] Additionally, while DSPs are only required to notify incidents where they have the necessary information to assess the impact,[32] this caveat does not apply to OESs.

Finally, the security and notification requirements apply to operators of essential services and digital service providers regardless of whether they internally maintain their network and information systems or outsource it.[33]

Germany

The main German authority handling cybersecurity is the Federal Office for Information Security. German legislation on cybersecurity is found in several acts and regulations. A key piece of legislation is the Act on the Federal Office for Information Security of 2015 (IT-Sicherheitsgesetz or BSI Act)[34] which was amended to add provisions pursuant to the NIS Directive. Important provisions are also found in the Basic IT Protection Catalogues,[35] developed by the BSI. Below we will review the types of services which are covered under the regulatory framework and provide an overview of obligations.

What services are considered critical infrastructure (OES)?

The BSI Act[36] casts a wider net than the NIS Directive, identifying a larger class of OESs, or operators of critical infrastructure as it is called in the German legislation. It also covers certain sectors which are not covered in the NIS Directive.

The BSI Act provides the Federal Ministry of the Interior the right to define activities which can fall under critical infrastructure requirements,[37] and with these powers the Ministry has issued an Ordinance to Identify Critical Infrastructures for the technology and telecommunications industry in which the following services are considered part of critical infrastructure:[38]

1) Voice and data transmission

[28] Regulation (EU) 2018/151.
[29] Article 17 and Recital 60 of the NIS Directive.
[30] For detailed information please see Article 14 of the NIS Directive.
[31] Article 15 of the NIS Directive.
[32] Article 16(4) of the NIS Directive.
[33] Recital 52 of the NIS Directive
[34] BSI Act (German) - BSI Act (English).
[35] BSI Basic IT Protection Catalogues.
[36] BSI Act (German) - BSI Act (English).
[37] Section 10(1) of the BSI Act.
[38] Section 5 of the Ordinance to Identify Critical Infrastructures under the BSI Act (BSI-KritisVO).

2) Data storage and processing

The Ordinance further provides clear identification criteria and lists information technology and telecommunication sector services, including the provision of a Content Delivery Network (CDN) or server farm services (hosting).[39] The critical infrastructure providers list is much broader than what was provided under the NIS Directive. This has two important outcomes:

Firstly, certain providers that are not subjected to the NIS Directive could be subject to German critical infrastructure provisions. Thus, they may need to comply with strict cybersecurity requirements in Germany, although they are not subject to any in other Member States. Secondly, providers which will potentially be subject to cybersecurity requirements as they are considered a DSP as cloud computing service providers (like for example CDN providers in the cloud) will also be subject to the more stringent requirements of an OES (operator of critical infrastructure) under German law. Therefore, undertakings may have to comply with cybersecurity requirements as a DSP in one Member State and an OES in another (Germany).

What are the regulatory requirements?

These considerations are important as operators of critical infrastructure are required to identify themselves to the Federal Office Information Security (BSI).[40] Such entities are required to take organisational and technical precautionary measures to avoid disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components and processes that are crucial to the functioning of the critical infrastructures they operate. Further, they must prove compliance with the requirements every two years by way of security audits, reviews or certifications, and grant BSI access to their business and operating facilities,[41] as well as provide a point of contact that has to be available at all times and must report security incidents.[42]

What are the enforcement actions in case of non-compliance?

Entities that fail to comply may be fined up to EUR 50 000. Should an entity fail to correct a cybersecurity effect following an order from the BSI, it may be fined up to EUR 100 000.[43]

United Kingdom

The UK has implemented the NIS Directive with The Network and Information System Regulations 2018 ("Regulations 2018").[44] The Regulations 2018 will not change materially for DSPs and OESs post Brexit due to The Network and Information System (Amendments etc.) (EU Exit) (No. 2) Regulations 2019 which aims to ensure that the Regulations operate effectively following the withdrawal of the UK from the EU.[45] The Office of Communications ("Ofcom") is responsible for overseeing OES within the digital infrastructure sector, and the Information Commissioner's Office ("ICO") oversees digital service providers.

Depending on the outcome of post-Brexit negotiations, DSPs that are established in the UK and provide services in the EU may be required to appoint a representative in an EU Member State.

[39] For the whole list and necessary criteria please see Annex 4 of the BSI-KritisVO.
[40] Section 8b(3) of the BSI Act.
[41] Section 8a of the BSI Act.
[42] Incidents which must be reported are specified in section 8b(4) f the BSI Act.
[43] Section 14 of the BSI Act.
[44] The Network and Information System Regulations 2018.
[45] The amending instrument does however change the relationship regulatory bodies in the UK have with other EU bodies, like for example the ENISA, by revoking the ENISA Regulation.

Similarly, EU based DSPs may need to appoint a representative in the UK if they wish to continue providing services. Therefore, digital service providers including IaaS, PaaS and SaaS must closely monitor the regulatory developments in this area to ensure they remain compliant with both British and EU Member State cybersecurity regulations.

What services are considered essential?

As opposed to the regulatory framework in Germany, Regulations 2018 does not significantly deviate from the provisions of the NIS Directive. Like the NIS Directive, the Regulations 2018 limits digital infrastructure services to three types of services and has similar definitions as the directive. However, the Regulations 2018 also has specific threshold criteria for what is considered a digital infrastructure OES in the UK.[46] The threshold criteria is detailed, providing clear instructions for entities to evaluate whether they are subject to OES requirements or not.

What are the relevant requirements for DSPs and OESs?

Operators of essential services within the digital infrastructure sector that meet the relevant threshold levels must comply with security obligations[47] and identify themselves to Ofcom.[48] However, OES which do not meet the threshold levels may still be designated by Ofcom as an OES covered by the Regulations 2018. The requirements for relevant DSPs mirror those of the NIS Directive.[49] However, while the directive does not require DSPs to be registered with national authorities, the Regulations 2018 require relevant DSPs to register with the ICO within three months after fulfilling the conditions to qualify as a DSP.[50] The security and incident report requirements for OESs in the UK largely mirror the requirements of the NIS Directive.[51] An OES which is reliant on a relevant DSP to provide essential services must immediately notify Ofcom[52] of any significant impact that an incident has had on the continuity of services.[53]

What are the enforcement actions in case of non-compliance?

In comparison to Germany, the UK has set exceptionally high penalties for breaches to cybersecurity obligations from the NIS Directive. The penalty for a material contravention[54] of the Regulations 2018, that is determined to have caused or could have caused an incident resulting in an immediate threat to life or significant adverse impact on the UK economy, may result in a fine not exceeding GBP 17 million. A fine of GBP 8.5 million may be imposed for a material contravention which Ofcom determines has caused, or could cause, an incident resulting in a disruption of services by the OES or relevant DSPs for a significant time period. A fine of GBP of 1 million can be imposed for any contravention which Ofcom believes could not cause a NIS incident.[55] DSPs should especially note these high penalties as, unlike OESs, they are only subject to penalties imposed by authorities in the jurisdiction of their main establishment.

---

[46] Schedule 2, Section 10 for digital infrastructure subsector of the Regulations 2018.

[47] For further information please see Section 10 of The Network and Information System Regulations 2018.

[48] Section 8(2) of The Network and Information System Regulations 2018.

[49] For more information on this please see Section 12 of The Network and Information System Regulations 2018.

[50] Section 14(4)(b) of The Network and Information System Regulations 2018.

[51] For specification on security duties and incident reporting please see section 10 and 11 respectively of The Network and Information System Regulations 2018.

[52] Guidance for Operators of Essential Services under the Network and Information Systems Regulations 2018.

[53] Section 12(9) of The Network and Information System Regulations 2018.

[54] "a material contravention" means a failure to take steps, or any adequate steps, within the stipulated time period to rectify a failing.

[55] Section 18(6) of The Network and Information System Regulations 2018.

Cybersecurity under electronic communication framework

In the previous section, the cybersecurity requirements that apply under the NIS Directive have been reviewed; however, the NIS Directive does not apply to telecommunication providers as these are subject to specific regulatory requirements applicable to them under the EU electronic communication framework. To an extent, requirements under the electronic communication framework are similar in nature, but different in substance, to the NIS directive requirements. Below is an overview of cybersecurity requirements that apply to telecommunication providers under the electronic communications framework. It is first important to determine what type of undertakings can be considered subject to these requirements, and then assess what obligations they are subject to.

Types of undertakings subject to electronic communication requirements

The electronic communications framework of the EU is harmonised by several directives enacted in 2002 and amended in 2009. To a certain extent, the framework was considered to regulate the so called "traditional" providers of telecommunication services, and did not specifically consider Over the Top providers, although their role in the telecommunications industry has significantly increased since these directives were adopted.

In the recent years, however, the electronic communication framework has gone through significant changes to catch up with the pace of technical change. The European Court of Justice recently had a case that significantly "expanded" the applicability of the electronic communications framework to Over the Top Providers (OTTs). It was decided that the SkypeOut application, which allows users to make phone calls via PSTN, should be considered a publicly available electronic communication service. As a result, Skype was required to comply with the regulatory requirements that apply to telecommunication providers.[56]

The recent European Electronic Communication Code (EECC) Directive ("Code"),[57] which was adopted in 2018 and will be transposed into national laws across the Union before 21 December 2020, aims to reform the "outdated" electronic communications framework. The Code has widened the definitions of electronic communication services and is including more non-traditional providers in its provisions. The Code defines an 'electronic communications service'[58] as:

A service normally provided for remuneration via electronic communications networks, which encompasses, the following types of services:[59]

a) Internet access service;

b) Interpersonal communications service;[60]

---

[56] Skype Communications Sàrl v Institut belge des services postaux et des télécommunications (IBPT), Case C-142/18.
For a comprehensive discussion on how ECJ caselaw has expanded the ECS/ECN definition, and the consequences to OTT connectivity providers please see Access Partnership's paper 'The Impact of EU Regulatory Frameworks on OTT Connectivity Providers'.

[57] Directive 2018/1972 on establishing European Electronic Communication Code.

[58] Article 2(4) of the Directive 2018/1972 on establishing European Electronic Communication Code.

[59] Services providing, or exercising editorial control over, content transmitted using electronic communications networks and services are outside of the scope of the Code.

[60] A service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

c) Services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting.

If the first and last points have not significantly deviated from the previous framework, the inclusion of 'interpersonal communications service' has notably expanded the definition of electronic communication services. This service could include all types of emails, messaging services and group chats.[61] This expansion could affect companies that have not previously been considered electronic communication service providers, but at the same time are regulated under the NIS Directive. It is important to highlight that one undertaking could fall under the electronic communication framework as a provider of telecommunication services, and under the NIS Directive if it provides DSP or OES services.[62] Therefore, it is crucial for every entity to determine which of its services could be considered under which framework as both frameworks exclude each other. Below we review examples of cases where services could be covered under the NIS Directive and at the same time be considered telecommunication providers.

Internet exchange points (IXP)

Internet exchange points (IXP) offer platforms where multiple networks can interconnect to exchange traffic. This allows networks to connect with all other networks present at the IXP. This creates improved network redundancy, lowers the cost of peering, and makes networks less dependent on transit. It is important to differentiate between operators who facilitate the exchange of aggregated Internet traffic being subject to the NIS Directive, and those who physically interconnect their networks effectively, providing services as telecommunication providers.[63]

Content Delivery Networks (CDN)

Traditionally, CDN providers operated servers that stored material from Content and Application Providers (CAPs) like Netflix and YouTube closer to end users for end users to have better and securer access to content. "Traditional" CDN providers would procure Internet connectivity for the transmission between its servers like any other CAP provider and would be outside of an electronic communication framework.

The situation will be different if CDN providers start extending the scope of their services by providing connectivity and can then potentially be classified as telecommunication providers. There is currently no harmonised approach to CDNs across the EU Member States. BEREC[64] has assessed[65] the extent to which CDNs could fall under telecommunication requirements by distinguishing between "core functionality" and "infrastructure based" models of CDNs. The latter operates infrastructure which connects to CDN servers, and thereby transmits CAP's content via this infrastructure. In this case, the CDN will likely be subject to telecommunication requirements. French[66] and Norwegian[67] authorities have also published similar studies which highlight one decisive factor for classification as ECS or ECN: the responsibility for the transmission of signal – even if merely between PoPs (servers) is a key indication that the CDN is classed a telecommunication provider.

[61] Section 2.1.2. of Review of the Electronic Communications Regulatory Framework.
[62] COM (2017)476 final/2 page 40.
[63] COM (2017)476 final/2 page 21.
[64] Body of European Regulators for Electronic Communications (BEREC).
[65] An assessment of IP interconnection in the context of Net Neutrality".
[66] Study related to the ECS/ECN term- ARCEP.
[67] Content Delivery Networks – regulatory assessment.

Considering the broad definition of cloud computing services, CDN providers, if their services are provided in the cloud, could potentially be classified as a DSP under the NIS Directive.[68] In addition, as was illustrated, "infrastructure based" CDN providers are likely to be classified as telecommunication providers.

Cloud computing services

The Code has expanded the definition of electronic communication service providers to interpersonal communications services, which could cover applications that enable the direct interpersonal and interactive exchange of information between a limited number of persons. These could mean that cloud computing companies which, for example, provide software as a service, such as online email or chat services, could potentially have their services be subject to the new electronic communication framework, and not to requirements under the NIS Directive. We now briefly review the cybersecurity obligations of telecommunication providers from the electronic communications framework.

Cybersecurity obligations of telecommunication providers

Under the EU electronic communication framework, telecommunication providers are obliged to comply with the provisions of two separate EU directives. The first is an ePrivacy Directive[69] which – among other requirements – places obligations on telecommunication providers to ensure an adequate level of privacy and confidentiality while processing personal data. The Framework directive[70] requires telecommunication providers to ensure the security and integrity of their services or network to minimise the impact of security incidents on users and other interconnected networks.

Requirements under ePrivacy Directive

Public electronic communication providers are required to take appropriate measures to secure their services, and together with providers of public electronic communication networks, ensure network security measures are appropriate in relation to possible risks.[71] If a personal data breach occurs, the public electronic communication provider, must notify the breach to the competent national authority immediately and in certain cases must also notify its subscribers or the affected individuals. This also applies if there is a risk of a significant breach.[72]

The EU Commission issued a Regulation[73] which set up a 24 hour timeframe for public electronic communication providers to notify their national authorities about a security incident and to provide the list of information that is required with such a notification. Depending on national requirements, such a notification may need to be submitted to the data protection authority – as is the case in the UK[74] - or to both the telecommunication regulator and the data protection authority, as is the case in Germany.[75]

---

[68] Also, Germany classifies certain CDNs as critical infrastructure providers, making them subject to additional requirements.
[69] Directive on privacy and electronic communications 2002/58/EC, as amended in 2009.
[70] Article 13a of the Framework directive 2002/21/EC, as amended in 2009.
[71] Article 4 (1) of the Directive on privacy and electronic communications further provides a minimum list of measures that needs to be undertaken.
[72] Article 4(2) and (3) of the Directive on privacy and electronic communications.
[73] Commission Regulation (EU) No 611/2013. Under EU law regulations are directly applicable in the Member States and do not require a separate implementation.
[74] For more information, please see Notification of PECR security breaches to Information Commissioner's Office.
[75] Germany framework requires submission of notification to the Federal Network Agency and to the Federal Commissioner for Data Protection and Freedom of Information. For more information, please see the relevant section of the Federal Network Agency's website.

In addition, the Regulation describes the conditions required to notify affected subscribers or individuals. However, such a notification would not be required if the provider has demonstrated, to the satisfaction of the national authority, that it has implemented appropriate measures to render the data unintelligible to any person who is not authorised to access it.[76] Therefore, to avoid "unnecessary" notification to customers or other affected persons, providers should consider implementing security measures making data unreadable to unauthorised peoples and coordinate these measures with national authorities.

To a certain extent, the provisions of the ePrivacy Directive overlap with GDPR requirements. However, if the ePrivacy Directive applies to telecommunication providers when processing personal data, the GDPR applies to all processors and controllers of personal data. Therefore, two frameworks could potentially apply when telecommunication providers are subject to GDPR provisions. To avoid conflict of frameworks, the GDPR specifies that it should not impose additional obligations on telecommunication providers when they are subject to the same obligations under the ePrivacy Directive.[77] As an example, telecommunication providers may only need to notify of a data breach under the ePrivacy Directive and not under the GDPR.[78]

In 2017, the EU Commission published a proposal[79] to repeal the ePrivacy Directive and replace it with a regulation which would serve as a *lex specialis* to the GDPR in relation to the processing of electronic communications data. It was carried out in connection with the provision and the use of electronic communications services. However, this proposal has still not been adopted, and there is no clear timeframe when or if it will be.

Requirements under the Framework Directive

The Framework Directive also requires telecommunication providers to take appropriate technical and organisational measures to ensure the integrity and security of their services and network, to prevent and minimise the impact of security incidents on users and interconnected networks.[80] The directive does not specify what measures will be imposed by national states to ensure the security and integrity of services and networks, leaving this for the national authorities to determine.

ENISA has prepared technical guidelines for minimum security requirements,[81] aiming to assist national authorities with assessing the measures taken by telecommunication providers pursuant to the regulatory framework of the directive. These guidelines aim to harmonise the minimum requirements to ensure the security and integrity of services and networks. However, they are not mandatory and EU Member States often adopt their own security measures.[82]

---

[76] Art 4(3) of the Directive on privacy and electronic communications in such case only notification to the national authority would be required.

[77] Article 95 of the General Data Protection Regulation 2016/679. For further information please see Opinion 5/2019 of the European Data Protection Board "on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities" see pages 12-16.

[78] Opinion 5/2019 pages 14-15.

[79] European Commission Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

[80] Article 13a(1) and (2) of the Framework directive 2002/21/EC, as amended in 2009.

[81] Technical Guideline for Minimum Security Measures.

[82] Germany has implemented its Catalogue of security requirements for the operation of telecommunications networks and data processing systems and for the processing of personal data (available in German). Please note that this catalogue provides requirements for protection of personal data as well as requirements (under e-privacy directive) to ensure security and integrity of services and network.
In the UK, telecommunication's regulator OFCOM has published its guidelines on the necessary measures to protect the security and resilience of their networks and services.

Similar to the ePrivacy Directive, the Framework Directive also requires telecommunication providers to notify national authorities "of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services". There is no EU wide definition of what activity could constitute a "significant impact", leaving individual EU Member States to decide. ENISA has published Technical Guidelines on Incident Reporting[83] where it gives recommendations on what constitutes a significant impact. However, as was the case with the technical guidelines, these are not legally binding guidelines.

Finally, as opposed to the ePrivacy Directive, the Framework Directive does not provide a timeframe for telecommunication providers to notify national authorities about a breach, leaving this to the national authorities to determine. This means it can significantly vary in different jurisdictions. Each Member State can therefore choose its own standards of what is considered a significant impact.

In Germany, if one of the following conditions are met it will be considered a "considerable security breach" and a notification must be immediately submitted to the Federal Network Agency and the Federal Office for Information Security:[84]

a) Affected participant hours (end users multiplied by number of hours) exceed 1 million;

b) Any impact on international interconnection points;

c) Impact on emergency calling; and

d) Exceptional IT failure.

In the UK, Ofcom differentiates notifications by different levels of urgency – within 3 hours of occurrence and reportable incidents or within 72 hours of occurrence – depending on the severity of the case and its impact on end users and society in general. Incidents attracting national media coverage or affecting critical public sector services are considered urgent.[85]

As was demonstrated in the German and UK examples, national authorities have different approaches to the framework. Notification and security requirements under the Framework Directive vary, making it the responsibility of telecommunication providers to assess and report incidents that have a significant impact. This contrasts with the more harmonised approach under the ePrivacy Directive, where regulatory discrepancies are less common.

Finally, it should be highlighted that the Code,[86] which must be implemented by December 2020 by all EU Member States, will repeal the Framework Directive,[87] making several changes that specify the provider's obligations by setting an expected security baseline. In particular, the Code highlights the need for encryption where appropriate to prevent and minimise the impact of security incidents,[88] as well as notifying national authorities without undue delay of a security incident that has had a significant impact on the operation of networks or services.[89]

[83] Technical guidance on the incident reporting in Article 13a.
[84] For more information please see Implementation concept of Notification in accordance with section 109 (5) of the Telecommunications Act.
[85] For more information please see Ofcom's guidelines on the necessary measures to protect the security and resilience of their networks and services.
[86] Article 40 of the Directive 2018/1972.
[87] However, the E-privacy directive will remain in force, and will not be affected by the Code.
[88] Article 40(1) Directive 2018/1972.
[89] Article 40(2) Directive 2018/1972.

The Code also adds that "in the case of a particular and significant threat of a security incident" telecommunication providers need to inform potentially affected users of the protective measures they can take, and when appropriate, also provide more detail about the threat itself.[90] The Code also requires more preventative action on the part of authorities, which are to instruct telecommunication providers on how to mitigate threats.

[90] Article 40 (3) Directive 2018/1972.

Conclusion

This paper has reviewed two cybersecurity frameworks relevant to ICT companies. Both frameworks can potentially overlap, meaning it is important for stakeholders to know which framework applies to their services so that they can mitigate unnecessary regulatory risks.

The first framework derives from the NIS Directive, which requires certain entities to take measures and notify national authorities if they experience a security incident. The directive distinguishes between operators of essential services and digital service providers. The identification and obligations of providers are significantly more harmonised across EU Member States, and subject to less stringent requirements compared to operators of essential services. Due to different identification processes of EU Member States, one entity may be considered an operator of essential services in several jurisdictions, or be considered as a digital service provider in one jurisdiction and an essential service (digital infrastructure) provider in another.

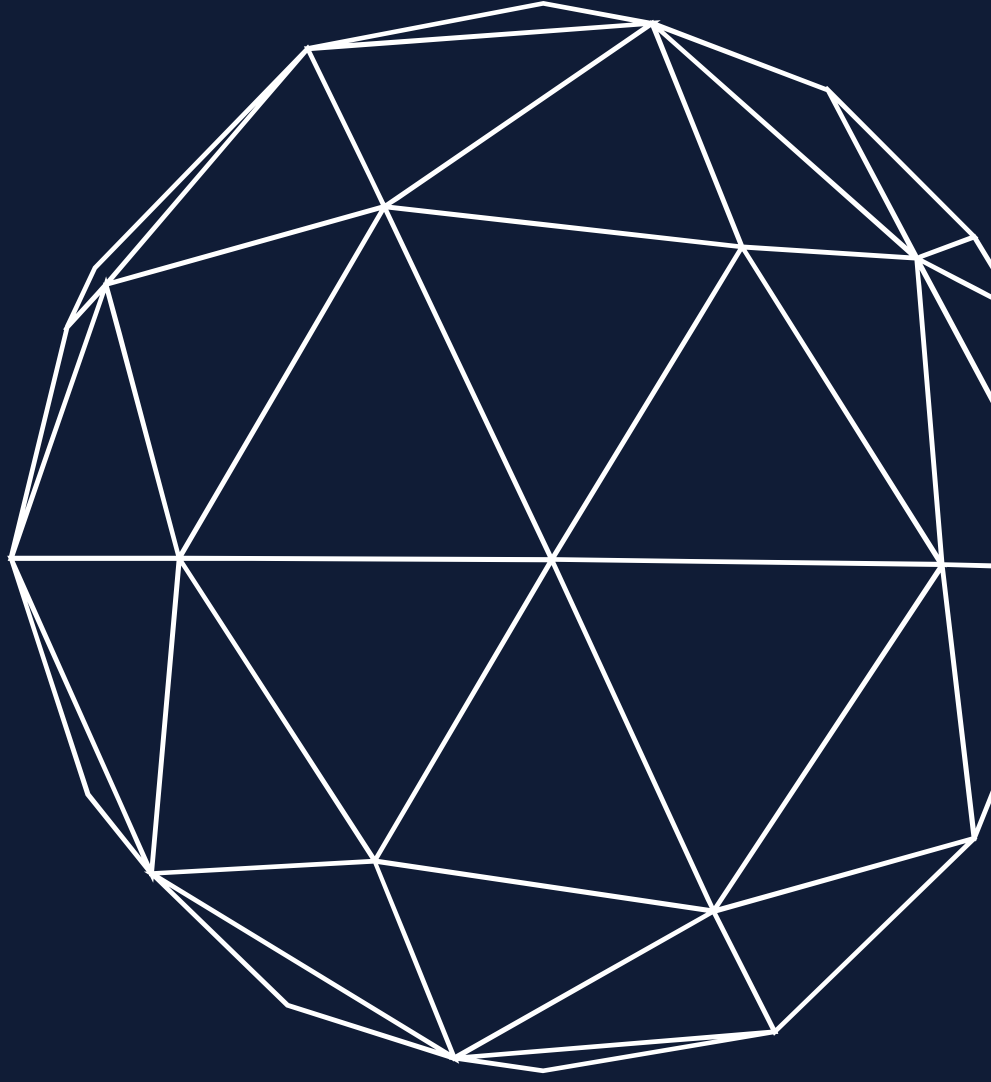
The second framework applies to telecommunication providers. One must distinguish between requirements to protect the privacy and confidentiality of personal data of end users under the ePrivacy Directive, and to ensure the security and integrity of services and networks so as to avoid disruptions of services under the Framework Directive. If an activity is subject to the electronic communication framework, then provisions of the NIS Directive should not apply.

Telecommunication requirements for the protection of personal data overlap with data protection requirements under the GDPR. This is the case although the GDPR should not apply to the extent that telecommunication providers are already covered under ePrivacy Directive.[91] For example, if an affected telecommunication provider is already obliged to notify under the ePrivacy Directive it may not have to notify the national authorities under GDPR provisions. Also, to avoid service disruptions, telecommunication providers must take the necessary security measures and report incidents to national authorities. Member States are free to determine when incidents are subject to notification. It should also be added that cases where a breach of personal data has resulted in the disruption of services – for example, if it was caused by outages – the telecommunication provider is likely to be required to separately notify the relevant authorities about the two incidents.

The recent EECC Directive significantly expands the definition of electronic communication service providers to include certain cloud computing companies whose services are currently subject to the NIS Directive. These entities will need to evaluate both frameworks to identify which of their services apply to which framework.

Finally, the COVID-19 pandemic has once again underlined the importance of the ICT industry and its services. Although networks have thus far been robust enough to handle the surge in traffic and the other challenges the pandemic has caused, this success demonstrates that cybersecurity obligations should not be considered a burden. Cybersecurity exists to ensure the security of services, avoid disruptions of daily services, and to protect the privacy of end users. Having implemented these measures, entities will not only mitigate and avoid regulatory risks, but also operational risks. Every ICT company should carefully analyse whether and to what extent its activities are subject to these regulatory frameworks.

[91] Please note that GDPR provisions should apply together with NIS directive, so if entity is covered under NIS Directive it does not exempt if from complying with any GDPR requirements.



We lead countries to fair tech

Access Partnership is the world's leading public policy firm that provides market access for technology. Our team uniquely mixes policy and technical expertise to optimise outcomes for companies operating at the intersection of technology, data and connectivity.

9th Floor, Southside
105 Victoria Street
London SW1E 6QT
United Kingdom
Tel: +44 (0) 20 3143 4900
Fax: +44 (0) 20 8748 8572

www.accesspartnership.com

AccessAlerts

AccessPartnership