DIGITALEUROPE

29 NOVEMBER 2022

Improving Member States' approaches to number-independent services in light of the EECC

Introduction

This paper outlines some of the main findings from Member States' implementation of the European Electronic Communications Code (EECC)[1] to date, pertaining specifically number-independent interpersonal communications services (NI-ICS).

So far, 25 out of 27 Member States have fully transposed the EECC. Much work has been done by the majority of Member States in seeking to ensure that their national transposition reflects the nuanced positions taken with regard to NI-ICS in the EECC.[2] This paper illustrates how the provisions of several transpositions risk conflicting with the level of harmonisation provided in the EECC.

[1] Directive (EU) 2018/1972. This document does not include observations relating to Croatia, Latvia, Ireland, Poland, Portugal and Slovenia. Transposition by Croatia, Latvia, Portugal and Slovenia has only recently been completed and we are still in the process of analysing the texts. Ireland and Poland are yet to fully transpose the EECC. Also, this document is strictly limited to provisions pertaining to MI-ICS and does not cover other aspects relating to EECC enactment in Member State laws.

[2] As defined in Art. 2(7) EECC.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

- Introduction 1
- Table of contents..... 2
- Definitions (Art. 2 EECC) 3
- General authorisation (Art. 12 EECC)..... 3
- Security of networks and services (Art. 40 EECC) 4
- Security of networks and services: implementation and enforcement (Art. 41 EECC)..... 7
- End-user rights: information requirements for contracts (Art. 102 EECC)..... 7
- Quality of service related to internet access services and publicly available ICS (Art. 104 EECC)..... 8
- Access to emergency services and single european emergency number (Art. 109 EECC) 9
- Public warnings (Art. 110 EECC) 10

Definitions (Art. 2 EECC)

Notwithstanding our general observation that most Member States' definitions seek to reflect the substance of Art. 2 EECC, Member States such as Denmark and Germany have varied from the EECC's exact text. This could cause confusion or lead to different Art.icles being applied based on a difference in definitions, resulting in legal and regulatory uncertainty. Moreover, this undermines the EECC's principle of seeking to achieve an increased level of harmonisation across Member States.

- **Denmark**: Denmark defines NI-ICS separately from electronic communications services (ECS).[3]
- **Germany**: The definition of 'access' is more comprehensive in Germany, and the German Telecommunications Act does not use the term 'provision' of an electronic communications network (ECN) but rather 'operator' of an ECN.[4]

General authorisation (Art. 12 EECC)

While the EECC specifically exempts NI-ICS from general authorisation and registration requirements, at least one Member State (Spain) has implemented transposing laws that do apply certain registration and notification requirements on NI-ICS. This regulation on NI-ICS risks leading to an approach in practice that would contradict the EECC, depending on the scope of the notification concerned and its practical effects. In any event, it creates unnecessary additional regulatory and administrative burdens.

- **Spain:** The Spanish transposition law requires NI-ICS services to be 'communicated' to the Spanish telecoms regulator CNMC, ostensibly for 'purely statistical and census purposes.'[5] However, much of the information required from NI-ICS services providers is the same or similar to that required under the Spanish general authorisation regime.[6] We understand that the Spanish telecoms regulator CNMC is yet to publish a template for making such communications. We would urge that the information requested from NI-ICS be strictly limited to what is necessary for purely statistical and census purposes and not

[3] Act. 128 of the Law of 7 February 2014 on electronic communication networks and services.

[4] Telekommunikationsgesetz of June 2021, as modified in July 2022.

[5] Art. 6(6), General Telecommunications Law No. 11/2022 of 28 June 2022.

[6] Including: name and surname or, where appropriate, corporate or business name and nationality of the provider; details of entry in the commercial entry or similar public registry and tax identification number; registered office and address for notification purposes; provider's website associated with the provision of ECS, if any; name, surname, national identity card or passport number of its representative and of the person appointed for notification purposes, including, in respect of the latter, the email address and mobile telephone number for notification purposes; and brief description of the services provided.

otherwise constitute a veiled authorisation requirement. This risks conflicting with the clear position in Art. 12(2) and Recital 44 EECC, whereby NI-ICS should not be subject to a general authorisation or equivalent requirement.

Security of networks and services (Art. 40 EECC)

As the EECC does not prescribe definitions for 'significant impact' and 'undue delay' for security incidents in Art. 40(2), Member States have adopted diverging approaches and definitions.

In some instances (e.g. the Netherlands) the transposing law does not provide specific definitions of the terms; in other instances, it provides vague definitions (e.g. Austria). The thresholds for 'significant impact' in terms of the number of impacted users and duration of the incident also vary.[7] These security incident reporting obligations may also be duplicative of, and even in conflict with, separate outage reporting obligations contained elsewhere in Member States' laws.[8]

Efforts to harmonise definitions and thresholds would improve compliance, comparison of impacts across Member States, and EU-wide understanding of the security of networks and services. We would also urge for continued engagement with ENISA and its role in developing guidance for both NI-ICS and competent authorities on this issue.

We provide some examples of deviations in approach across Member States below:

- **Austria**: The term 'significant impact' is defined in §44(5) Telekommunikationsgesetz (TKG) 2021 and in more detail in §3(2) TK-NSiV.[9] In line with the EECC, the TKG 2021 uses the term 'unverzüglich' ('without undue delay'). While the term is not defined in the TKG 2021, §2(8) TK-NSiV defines 'unverzüglich' differently as 'without culpable hesitation' ('ohne schuldhaftes Zögern').

[7] For example, applying the 50,000 affected-end-user threshold in the Danish transposition to large NI-ICS providers would result in an incident of just a few minutes needing to be notified to the relevant competent authorities.

[8] Many Member States have reporting obligations for service outages, which have different thresholds, deadlines for reporting, and notification requirements, and are reported to an entirely separate regulatory authority. This creates ambiguity regarding whether and to whom a particular incident must be reported. National laws often define 'security incidents' as any incident having an impact on the 'functioning' or 'availability' of the service, which if interpreted broadly could also include service outages. Thus, even in Member States such as Belgium and the Netherlands that have reporting obligations solely for 'security incidents,' clarity is needed regarding whether such incidents include any impact to the functioning or availability of the service, or only when such impact results from a security breach.

[9] Telecom network security ordinance 2020, which was issued on the basis of the former TKG (2003).

- **Belgium**: The Belgian implementation uses the term 'onverwijld'/'sans délai,' signifying an immediate duty to notify.[10] A significant impact shall be assessed in accordance with the same criteria determined in Art. 40(2) EECC. The Belgian telecoms regulator (BIPT) is allowed to specify what can be considered to have a 'significant impact.' The BIPT considers this is the case when one or more of the thresholds are reached; however, such thresholds are tailored towards traditional ECN rather than to NI-ICS.[11]
- **Denmark**: §8–9 of Executive Order no. 258 on information and notification obligations concerning security in networks and services further defines what constitutes a security breach with 'significant impact.' The obligation to report such security incidents follows from §7 of the Executive Order.[12] §7(3) triggers the notification obligation when the provider becomes aware that the security incident has had a significant impact on the operation of networks or services. The notification shall be made without undue delay through the common digital solution for reporting to public authorities. 'Undue delay' has not been further defined in the legislation and it is therefore difficult for NI-ICS providers to predict how this will be applied in practice and what their precise compliance obligations will be.
- **France**: The French implementation uses the terms 'as soon as the provider is aware of the breach' to define 'undue delay.'
- **Germany**: The German implementation in §168(1) TKG uses the term 'unverzüglichliche Mitteilungsplicht' ('immediate duty to notify'). According to §121 of the German Civil Code (BGB) this is understood as neither intentionally nor negligently delaying the relevant action. A

[10] Art. 107(3) §2, Electronic Communications Act (ECA).

[11] The incident has been lasting for at least one hour and is affecting at least 25,000 end-users; the incident has an impact on the network and is affecting access to emergency services via the network; the incident has an impact on the interconnections located in Belgium, thus affecting other operators in Belgium or abroad; and the incident has an impact on a network component considered by the operator as critical for the operation of its networks and services.

[12] According to § 7(1), providers of NI-ICS and public ECN/ECS shall notify the Danish Centre for Cybersecurity of security incidents that have had a significant impact on the operation of networks or services in terms of damage to the availability of these networks and services, stored or transmitted or processed data or the related services offered by or accessible via those networks or services, as referred to in §8. According to §7(2), providers of NI-ICS and public ECN/ECS shall notify the Danish Centre for Cybersecurity of security incidents that have had a significant impact on the operation of networks or services in the form of an event that has had an actual negative impact on the ability of networks and services to withstand actions that are detrimental to the confidentiality, integrity or authenticity of those networks and services, the data stored or transmitted or processed, or the related services offered by or accessible through those networks or services, as referred to in §9.

significant impact shall be assessed in accordance with Art. 40(2) EECC pursuant to §168(2) TKG on the basis of several criteria.[13]

- **Italy**: According to the Decree of the Ministry of Economic Development of 12 December 2018, security incidents are considered significant – and as such have to be reported within 24 hours to the competent authority –following criteria that are tailored towards traditional ECN rather than NI-ICS.[14] Starting from January 2022, the Decree 81/2021 of the President of the Council of Ministers requires providers of essential services (including telecommunications services) to notify the Italian Computer Security Incident Response Team (CSIRT) of any incident concerning the malfunctioning, interruption or inappropriate use of the network, information and/or informatic systems directly managed by ECS providers that may result in a breach of the Italian national security.[15]
- **Netherlands**: Art. 11a.2 paragraph 1 of the Dutch Telecoms Act (DTA) only specifies that security incidents with a significant impact and undue delay must be notified. In the explanatory notes to the implementation of the EECC, the Dutch government specifies that security incidents now also relate to confidentiality and authenticity, but no further guidance is provided on the terms 'significant impact' and 'undue delay.'[16]
- **Greece**: The Greek transposition appears to require providers of a public ECN or publicly available ECS to notify the Hellenic Authority for Communication Security and Privacy (ADAE) of any security incident that has had a significant impact on the security of networks/services or poses a 'particular risk' to them.[17] This goes

[13] The number of users affected by the security incident, the duration of the security incident, the geographical extent of the area affected by the security incident, the extent to which the telecommunications network or service is affected, the extent of the impact on economic and social activities. No further information is given as to how to weigh these criteria, creating legal and regulatory uncertainty for NI-ICS providers.

[14] These are: duration of more than one hour and the percentage of affected users exceeding fifteen percent of the total national users of the service concerned; duration of more than two hours and the percentage of affected users exceeding ten percent of the total national users of the service concerned; duration of more than four hours and the percentage of affected users exceeding five percent of the total number of domestic users of the service concerned; duration of more than six hours and the percentage of users affected exceeding two percent of the total national users of the service concerned affected; duration of more than eight hours and the percentage of users affected being greater than one percent of the total amount of national users of the service concerned.

[15] This must occur: (i) within six hours from the moment they became aware of it (if it is not a 'particularly serious' breach according to Annex A of Decree 81/2021; or (ii) within one hour from the moment they became aware of it (if it is a 'particularly serious' breach). Following the introduction of Decree 81/2021, no amendments have so far been made to the decree of the Ministry of 12 December 2018, which remains unaffected.

[16] https://zoek.officielebekendmakingen.nl/kst-35865-3.pdf, pg. 20

[17] Art. 40(2), Law No. 4727/2020.

beyond the provisions in Art. 40(2) EECC, and imposes a disproportionate requirement.

Security of networks and services: implementation and enforcement (Art. 41 EECC)

Art. 41 EECC requires Member States to ensure that competent authorities can ask ECN/ECS providers to provide information (including security policies) needed to assess the security of their networks and services, and to submit to a security audit by a qualified independent body or a competent authority. In order to implement this article, Member States have imposed varying requirements to appoint a security officer and register security documentation. While the EECC specifically references security documentation requirements, it does not mention requiring a security officer, and variance in obligations creates additional regulatory burden and challenges in compliance.

- **Austria**: According to §163(3) TKG 2021, public ECS providers (including publicly available NI-ICS) are obliged to have a security concept for the processing of personal data in place. Non-publicly available ECNs are not subject to these obligations. It is unclear why public ECS providers, and specifically NI-ICS, are subject to elevated regulatory burden given that these services do not tend to control the public ECNs over which their services are delivered.
- **Germany**: A security officer must be appointed and security documentation registered for NI-ICS providers, but not for non-public ECN providers.
- **Netherlands**: Both public ECN operators and public ECS providers have the obligation to appoint a security officer and to have a security plan. Public ECN operators and public ECS providers must also designate a Netherlands-based contact for telecoms security breach reporting and provide their securitry officer's contact details to the Radiocommunications Agency.

End-user rights: information requirements for contracts (Art. 102 EECC)

While the ECC's includes laudable measures to ensure equivalence of access for end-users with disabilities, diverging Member State approaches in this sphere undermine the principle of maximum harmonisation in Part III, Title III EECC. These divergences could lead to increased regulatory burden and compliance costs, which could especially discourage smaller NI-ICS providers from providing services for fear of risk of non-compliance with stricter local laws.

Furthermore, requiring that information is always provided in an accessible format could lead to documentation that is lengthier or actually more difficult for users without disabilities, by restricting the use of non-text content such as photos.

- **Austria**: While there is an exemption for NI-ICS in Sec 6 Abs 1 TKG 2021, if providers do not surpass 350,000 end users, general terms and conditions (GTCs) must be notified to the regulatory authority. Furthermore, certain non-discrimination and transparency obligations create additional burden for implementation (e.g. notification of changes to terms and conditions must be made two months in advance unless beneficial for the end-user).
- **Germany**: There is the additional information obligation for NI-ICS providers to provide a product information sheet pursuant to §1–2 of the Telecoms Transparency Regulation (TK-TransparenzV).
- **Italy**: Art. 98 of the Italian transposition law states that the required information shall always (and not only upon request) be provided in an accessible format for end-users with disabilities.

Quality of service related to internet access services and publicly available ICS (Art. 104 EECC)

Art. 104 EECC only applies quality of service (QoS) publishing obligations to 'publicly available interpersonal communications services … to the extent that they control at least some elements of the network either directly or by virtue of a service level agreement to that effect.' Some Member States (e.g. France, Germany and Italy) do not take into account this exemption related to control of the network, directly contradicting the understanding in the EECC that ICS providers without control of the network are fundamentally different from ICS providers that do control such elements. This distinction is essential, as providers without network control cannot provide any guarantees or necessarily remedy any issues regarding the QoS provided.

- **France**: NI-ICS providers are required to publish QoS information. Pursuant to Art. 36(6) of the French Code des postes et des communications électroniques, the French telecoms regulator ARCEP shall specify the rules concerning the content and procedures for making available to the public complete, comparable, reliable, easy-to-use and up-to-date information on the availability, quality and coverage of ECN/ECS, including information on measures taken to ensure equivalent access for disabled end-users, and the determination of the indicators and methods used to measure them. ARCEP has not yet issued rules regarding, amongst others, the content and modalities for making available information on the

availability, quality and coverage of services. DIGITALEUROPE urges ARCEP to make clear in those rules that NI-ICS providers that do not control relevant network elements should be exempted, in line with the EECC.

- **Germany**: According to §52(1) Nr. 4 TKG, every ICS (including NI-ICS) is required to publish QoS information.
- **Italy:** Under Art. 98 of the Italian transposition law, the Italian Authority for Communications (AGCOM) may require providers of internet access services and publicly available ICS to publish QoS information. Similar to the French situation, AGCOM should reflect the position in Art. 104 EECC, subjecting only those providers that control at least some elements of the network to these obligations.

Access to emergency services and single european emergency number (Art. 109 EECC)

Art. 109(2) EECC specifically states that it only applies to publicly available number-based ICS (NB-ICS) where they allow end-users to 'originate calls to a number in a national or international numbering plan.' Many Member States (including France, the Netherlands and Spain) do not explicitly exclude NI-ICS from the scope of emergency service requirements, which could lead to confusion. An express exclusion, including by way of secondary legislative measures and guidance from the national regulators, would improve legal certainty.

- **Belgium:** While NI-ICS are not subject to emergency services obligations, they are also not explicitly excluded.[18]
- **Germany:** While NI-ICS are not subject to emergency services obligations, such obligations arise when NI-ICS offer so-called 'emergency call apps.' DIGITALEUROPE understands this to refer to apps that enable direct communication to the locally competent emergency call answering points. In this articular case, NI-ICS have to ensure that the data required to determine the emergency location are transmitted.
- **Italy**: Art. 98-vicies bis of the Italian transposition law, establishing obligations to ensure access to emergency services, only applies to NB-ICS. In order to comply with transparency obligations under Art. 98-quindecies, Annex 9 establishes that NI-ICS are in any case required to publish information if (and eventually, the extent to which) access to emergency services can be guaranteed.

[18] The requirement in Belgium explicitly applies to: (i) non-publicly available ECN that allow calls to be made to public networks; and (ii) NB-ICS providers that allow end-users to make outgoing calls to a number in a national or international telephone numbering plan.

Furthermore, it is vital for Member States to recognise the fundamental technical differences of nomadic, cloud-based NB-ICS that rely on the networks of fixed and mobile line operators to connect to the public switched telephone network (PSTN).

For example, as inherently nomadic services, network-independent NB-ICS cannot rely on a fixed service address for the purposes of routing to the appropriate public-safety answering point (PSAP), nor can they obtain dynamic network-based location information to route based on the caller's location. Furthermore, many network-independent NB-ICS provide one-way, outbound-only VoIP-to-PSTN connections; as a result, there is often no phone number associated with the user making the emergency call, nor inbound calling service available to facilitate call-back capabilities in the event an emergency call is disconnected.

To ensure seamless and ubiquitous access to emergency services, we strongly encourage Member States to identify a single PSAP for routing when emergency caller location is not available and, where necessary on the basis of technical infeasibility, provide limited exceptions and alternative means for network-independent NB-ICS to comply with emergency service obligations.

Public warnings (Art. 110 EECC)

Art. 110 EECC only applies to mobile NB-ICS, unless Member States 'determine that public warnings be transmitted through publicly available electronic communications services other than [mobile number-based ICS] or through a mobile application relying on an internet access service, provided that the effectiveness of the public warning system is equivalent in terms of coverage and capacity to reach end-users, including those only temporarily present in the area concerned, taking utmost account of BEREC guidelines.'[19]

Some Member States (e.g. France)[20] have already extended Art. 110 to apply to NI-ICS without sufficient analysis of whether the services are equivalent in light of BEREC guidelines.

[19] https://www.berec.europa.eu/sites/default/files/files/document_register_store/2020/6/BoR_%2820%29_115_BEREC_Guidelines_on_PWS.pdf

[20] Art. L. 33(1) Code des postes et des communications électroniques.

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 98 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Banco Santander, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Eli Lilly and Company, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nemetschek, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK