

Implementing the European Electronic Communications Code

Brussels, 11 December 2018

EXECUTIVE SUMMARY

DIGITALEUROPE welcomes the adoption of the new European Electronic Communications Code. In consolidating the existing four Directives constituting the European regulatory framework for electronic communications into one single piece of legislation, and in further harmonising certain elements thereof, the Code has the potential to offer a more easily accessible and more single market–friendly set of rules to bring the European telecommunications market into the digital age.

For the Code to live up to its potential, it is however crucial that it is incorporated into Member State law not only in a timely manner but also in a way that is true to its spirit and its overall political goals: a) to create incentives for the substantial infrastructure investments required to achieve 5G rollout and gigabit connectivity; and b) to create a genuine single market for innovation and the development of new digital communications services.

In this position paper, DIGITALEUROPE highlights some areas where national implementation should not diverge from the Code. The Code provides sufficient flexibility for competent authorities to apply the rules in a targeted and proportionate manner in accordance with national and local market situations, without the need for further flexibility to be introduced in national legislation. DIGITALEUROPE urges Member States to use this flexibility with caution and limit additional provisions to those instances where there is a genuine, demonstrable national circumstance in the market.

Furthermore, whilst generally fully harmonising end-user rights provisions, the Code does leave significant areas where Member States can deviate from the Code. Electronic communications services are no longer national in nature; diverging from the single European rulebook will cause fragmentation in the Digital Single Market, which will hinder innovation and limit the services available to European users.

INVESTMENT

DIGITALEUROPE shares the objectives of the Code, which are to:

- Encourage investment in new networks in line with the 2025 broadband objectives, with particular emphasis on Very High Capacity Networks (VHCNs), i.e. wholly fibre, fibre-to-the-distribution-point and 5G networks;
- Enable such investment by lowering the cost of network deployment through enhanced sharing of civil infrastructure;

- Create incentives to invest through lighter regulatory obligations for co-investment and wholesale-only networks, inspired by some successful models in Europe;
- Increase regulatory stability and facilitate network investment and business planning, with five-year market review cycles carried out by national regulatory authorities (NRAs) as opposed to the current three-year limit;
- Assure more predictability for the deployment of new generations of mobile technologies by guaranteeing a minimum licensing duration of twenty years for regionally harmonised spectrum and more transparency in the renewal of rights; and
- Facilitate the rollout of denser mobile networks through a simplification of administrative rules for the deployment of small-area wireless access points.

It is of utmost importance that the national laws transposing the EECC fully implement these new objectives and the accompanying regulatory tools.

To keep Europe in the 5G race, spectrum availability at reasonable prices prior to 2020 as well as harmonised and simplified rules for rolling out dense urban networks are of paramount importance. DIGITALEUROPE is worried that provisions in the Code that are subject to national interpretation will lead to a fragmented assignment of the suitable 5G frequencies in the Member States, and in some cases to a delay in the deployment of 5G networks. For successful deployment and operation of 5G in Europe, DIGITALEUROPE urges rapid assignment of the identified 5G pioneer bands in the necessary contiguous carrier bandwidth in order to enable full 5G service offerings, while also considering the needs of vertical industrial players regarding harmonised, dedicated spectrum for their own local purposes.

Furthermore, to ensure speedy progress towards fixed gigabit connectivity, DIGITALEUROPE encourages a national implementation that fully follows the new step-by-step approach to market analysis and significant market power (Title II, Chapter III). If the EECC is to succeed in its objectives to increase incentives to invest and to foster more infrastructure-based competition, national transposition has to pay close attention to the new signals embedded in the reform. The aim of these new signals is not to limit NRAs' powers or toolkit but to ensure a more targeted and step-by-step approach whereby the market has regulatory predictability – only when less costly remedies have been proven not to work should NRAs move to impose additional obligations. This in particular concerns the preference for access remedies to civil engineering ahead of access to specific network elements and associated facilities (Arts. 72 and 73).

DIGITALEUROPE also urges that the procedure around the granting of a lighter regulatory treatment for co-investment be implemented in a clear and predictable manner. Whilst we warmly welcome that NRAs should not regulate networks when they find that co-investment offers comply with the necessary conditions, significant uncertainty remains as to how this rule will be implemented nationally and whether additional conditions can be imposed. We urge national decision-makers to refrain from imposing any such additional conditions as those contained in the Code already provide significant safeguards to ensure sustainable competition (Art. 76 and Annex IV). We also urge national decision-makers to ensure that the commitments procedure to be introduced in accordance with Art. 79 is transparent and efficient and that decisions taken under this procedure are based on solid data and market evidence.

Consistent national implementation in the above-mentioned areas is crucial for all of Europe to progress towards the 2025 connectivity targets. In this respect, the BEREC guidelines will influence the impact of major provisions, including: what constitutes a VHCN; what can qualify for regulatory relief for co-investment; the

criteria for symmetric access obligations; and how geographical surveys of network deployments will be conducted to enable state-aid funds where there is insufficient private investment. Most of these guidelines are slated for adoption over the course of 2020. Only legal certainty, market consistency and predictability will promote customer choice, network innovation and investment. DIGITALEUROPE looks forward to engaging in a dialogue with NRAs and BEREC's working groups and to providing input to support these shared objectives.

EXTENSION OF UNIVERSAL SERVICE OBLIGATIONS TO AFFORDABLE ADEQUATE BROADBAND

DIGITALEUROPE fully supports the extension of the universal service obligation to affordability as a key challenge to support basic broadband connectivity. However, we urge national decision-makers to implement this through direct support to the identified groups of consumers rather than by imposing an obligation on internet access service providers to offer such services on conditions outside normal commercial conditions (Art. 85). The extension is an important social policy measure which will provide considerable socioeconomic benefits to those directly affected and society as a whole. As such, it should be funded through the Member States' general budget as any other social policy measure.

RULES GOVERNING THE PROVISION OF COMMUNICATIONS SERVICES

DIGITALEUROPE is pleased to see a relatively targeted scope towards regulation of new communications services, while regretting that the Code was not used as an opportunity to significantly rewrite telecoms legislation and reflect the single market nature of many of these services. In what follows we will delve into areas where consistency in national implementation will be key in order to protect choice and innovation in the Digital Single Market.

1. Transposition of key definitions

Lessons learnt from the implementation of the 2002 Telecoms Package show the importance of consistent transposition in this area. While the definition of 'electronic communications service' (ECS) was laid down 16 years ago, the parameters of the definition are still being debated in at least two ongoing CJEU cases.¹

The new, layered definition of ECS is much more expansive (in part to reflect this) and future conflict around it could at least be minimised if Member States transposed the definition consistently. This includes national transposition of the recitals that seek to elaborate on the intended scope of the respective categories of ECS. This in particular concerns the recital clarifying the use of a number that is intended to qualify as number-based interpersonal communications service (NB-ICS) and the use of a number that is intended to qualify as number-independent interpersonal communications service (NI-ICS).

¹ C-142/18 and C-193/18.

Recital 18

Those number-based interpersonal communications services comprise both services to which end-users' numbers are assigned for the purpose of ensuring end-to-end connectivity and services enabling end-users to reach persons to whom such numbers have been assigned. The mere use of a number as an identifier should not be considered equivalent to the use of a number to connect with publicly assigned numbers and should therefore, in itself, not be considered sufficient to qualify a service as a number-based interpersonal communications service.

This could furthermore be an area where BEREC guidelines could be useful to provide a convergent interpretation of the types of services falling under the different definitions.

2. General authorisation and information obligations

We welcome the introduction of an exhaustive list of information that can be required as part of the notification procedure of an NB-ICS and look forward to BEREC's guidelines for a common template as soon as possible.

Regulators will have powers to request information from both those ECS that are and those that are not required to seek general authorisation, to ensure compliance with the general authorisation (Art. 21) and to ensure compliance with the Directive (Art. 20) respectively. Considering that new services which will become subject to the Code are online, cloud-based services that in most cases are offered today on a cross-border basis, the lack of detail, in particular for the latter article, on how such information request will work in practice and what kind of information will be expected of new ECS players creates significant uncertainty and potential high levels of duplicative administrative efforts for such providers. DIGITALEUROPE looks forward to working with BEREC and national regulators to ensure coherence and proportionality in the type of information required.

We would like to take the opportunity to stress that the capacity of NI-ICS to provide such information may be limited by their technical ability to collect and provide it, for example in light of end-to-end encryption.

3. Technical feasibility assessments for providing access to emergency

NB-ICS must in principle provide access to emergency calling under the Code. This is, however, subject to the 'technical feasibility' of the different types of NB-ICS, notably of network-independent providers of those services. On the basis of this technical feasibility, Member States can make further determinations as to which NB-ICS are to provide this access.

Considering that the language clarifying the conditions under which access to emergency calling for NB-ICS apply is only contained in the recitals, it is crucial to pay particular attention to transposing these recitals in a consistent manner.

Recital 284

Providers of number-based interpersonal communications services have an obligation to provide access to emergency services through emergency communications. In exceptional circumstances, namely due to a lack of technical feasibility, they might not be able to provide access to emergency services or caller location, or to both. In such cases, they should inform their customers adequately in the contract.

Recital 286

Where the number-based interpersonal communications service is not provided over a connection which is managed to give a specified quality of service, the service provider might not be able to ensure that emergency calls made through their service are routed to the most appropriate PSAP with the same reliability. For such network-independent providers, namely providers which are not integrated with a public communications network provider, providing caller location information may not always be technically feasible. ... Where such standards and the related PSAP systems have not yet been implemented, network-independent number-based interpersonal communications services should not be required to provide access to emergency services except in a manner that is technically feasible or economically viable.

In addition, BEREC and/or EENA guidance on this topic would be extremely useful, in particular their recommendations as to commonality of approach to caller location and call routing to (failover) PSAPs. This applies equally to the related area of public warning system obligations.

4. Security requirements and incident notifications

The security provisions represent an area where we believe a more harmonised approach could have been followed without any negative impact on security, as the requirements do not fundamentally differ depending on geography. We therefore hope that the EU implementing acts will constitute the main part of security requirements and urge Member States to only use their powers to adopt additional requirements in limited cases and when strictly necessary, e.g. for national security.

To ensure a more aligned approach across the single market, we also welcome ENISA's involvement in the development of the implementing acts and in facilitating coordination between Member States with regard to the obligations set out in Article 40. We reiterate the need for clarity in this area given the similar, overlapping obligations set out in the General Data Protection Regulation (GDPR) and the Directive on security of network and information systems (NIS Directive).

Art. 40(1), first subparagraph

ENISA shall facilitate in accordance with Regulation (EU) No 526/2013 the coordination of Member States to avoid diverging national requirements that may create security risks and barriers to the internal market.

Art. 40(5)

The Commission, taking utmost account of the opinion of ENISA, may adopt decisions detailing the technical and organisational measures referred to in paragraphs 1 as well as the circumstances, format and procedures applicable to notification requirements pursuant to paragraph 3. Those implementing acts

shall be adopted in accordance with the examination procedure referred to in Article 110(4). They shall be based on European and international standards to the greatest extent possible, and shall not prevent Member States from adopting additional requirements in order to pursue the objectives set out in paragraphs 1.

5. Consumer/end-user protection measures

Title III, setting out the end-user protections and transparency provisions, represents some helpful progress towards a single market approach. For the first time, the Code seeks to almost fully harmonise these provisions (Arts. 102-115) and to apply a targeted approach both in terms of the scope of services and by distinguishing between business and consumer contracts.

However, for this targeted approach to translate into practice, it is crucial that the national transposition pays close attention to the intended scope. We are in particular concerned that some of these provisions will be unduly burdensome to service providers if: (i) the scope of application remains unclear (just consumers or some businesses?); (ii) the requirements differ per Member State; and/or (iii) many Member States choose to utilise the extended transposition period set out in Art. 101(2).

Point (i) notably concerns Arts. 102, 105(1) and 107, which in the Code are limited to consumer contracts, micro and small enterprises and not-for-profit organisations. As regards point (ii), whilst the type of information required is now harmonised (Arts. 103 and 104), how and which providers need to comply is left to the Member States. We would like to see guidance and best practice in this area from BEREC to ensure a shared approach in order to facilitate compliance for cross-border and pan-European providers. Finally, concerning point (iii), we urge Member States to limit the use of the extended transposition period to where strictly necessary.

6. Public warning systems

DIGITALEUROPE members have ample experience in helping national governments and competent authorities establish public warning systems across the world, in ways to ensure efficiency and adequate levels of user engagement. Public warning systems, depending on the options chosen, can lead to important technical implementation requirements for ECS providers and device makers.

We therefore urge national governments and competent authorities to adhere to international standards and proven, established practices wherever possible. The adoption of very different solutions will lead instead to market fragmentation, resulting in unnecessary additional burden for industry players and confusion for travelling end-users. We therefore look forward to working closely with BEREC on the development of timely guidelines as established by Art. 110(2).

--

For more information please contact:

Alberto Di Felice, DIGITALEUROPE's Senior Policy Manager for Infrastructure, Privacy and Security
alberto.difelice@digitaleurope.org or +32 2 609 53 10

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total over 35,000 ICT Companies in Europe represented by 66 Corporate Members and 40 National Trade Associations from across Europe. Our website provides further information on our recent news and activities: <http://www.digitaleurope.org>

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, Arçelik, Bosch, Bose, Brother, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ	Germany: BITKOM, ZVEI	Slovakia: ITAS
Belarus: INFOPARK	Greece: SEPE	Slovenia: GZS
Belgium: AGORIA	Hungary: IVSZ	Spain: AMETIC
Bulgaria: BAIT	Ireland: Technology Ireland	Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Croatia: Croatian Chamber of Economy	Italy: Anitec-Assinform	Switzerland: SWICO
Cyprus: CITEA	Lithuania: INFOBALT	Turkey: Digital Turkey Platform, ECID
Denmark: DI Digital, IT-Branchen	Luxembourg: APSI	Ukraine: IT UKRAINE
Estonia: ITL	Netherlands: Nederland ICT, FIAR	United Kingdom: techUK
Finland: TIF	Norway: Abelia	
France: AFNUM, Syntec Numérique, TECH IN France	Poland: KIGEIT, PIIT, ZIPSEE	
	Portugal: AGEFE	
	Romania: ANIS, APDETIC	