DIGITALEUROPE

8 APRIL 2020

Response to the pre-consultation on the Polish draft law implementing the EECC

Executive summary

DIGITALEUROPE wishes to thank the Polish Ministry for Digital Affairs (the "**Ministry**") and its Telecommunications Department for organising a pre-consultation about a new draft Polish law (the "**draft Law**") implementing the European Electronic Communications Code (EECC)[1]. DIGITALEUROPE sets out its observations in this document.

Our observations have been drafted in English. We thank you for your understanding as well as for your further follow-up and consideration of our observations. We also note that our observations are based on a machine-based translation of the draft Law and therefore apologize in advance for any possibly irrelevant requests for clarification that we make in the below document.

From the topics concerned to which comments have been invited by April 10, 2020, our comments below cover:

- Registration requirement (Article 5 of the draft Polish Law)
- Security of networks and services (Article 40, Article 41 of the draft Polish Law)

We look forward to submitting comments on other topics in accordance with the relevant timelines communicated by the Ministry.

[1] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast).

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

Registration requirement (Art. 5 draft Law)

DIGITALEUROPE understands that the registration requirement in Art.5(1) of the draft Law applies to "*telecommunications activity*" conducted by "*telecommunications entrepreneurs*". Neither of these terms appear to be defined; in particular, it is unclear whether the reference to telecommunications entrepreneurs is to a "*telecommunications undertaking*"[2] and/or an "*electronic communication entrepreneur*"[3] (as defined in Art. 2(38) and Art. 2(39) respectively.

In addition, DIGITALEUROPE notes that the draft Law not only includes requirements to submit a registration with the "*register of telecommunications entrepreneurs*" under Art.5(1), but with the "*register of territorial self-government units conducting activities in the field of telecommunications*" under Art.5(2) in certain circumstances as well. (*See also* Arts.6-10.) Pursuant to Article 12 and Recital 43 EECC, however, there should be a single notification framework and no additional or separate notification processes should be imposed, whether by territorial self-government units or otherwise.

Above all, DIGITALEUROPE considers that it should be expressly clear that, consistent with the position in Art. 12 EECC, the registration requirements in Art. 5 and related obligations that may arise from registration (such as requirements to pay levies/fees) do not apply to number-independent interpersonal communications services ("**NI-ICS**")[4] as defined in the EECC[5].

---

[2] "telecommunications undertaking" - an undertaking or other entity entitled to conducting business activity on the basis of separate regulations, who conducts business activity consisting in the provision of a telecommunications network, provision of related services or provision of telecommunications services, whereby a telecommunications entrepreneur, entitled to
a) the provision of telecommunications services, is called 'service provider of telecommunications."
b) the provision of public telecommunications networks or related services, is called 'operator'; (Art. 2(38) draft Law).

[3] "electronic communication entrepreneur" - a telecommunications entrepreneur and an entity providing interpersonal communication service not using numbers; (Art. 2(39) draft Law).

[4] 'number-independent interpersonal communications service' means an interpersonal communications service which does not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which does not enable communication with a number or numbers in national or international numbering plans; (Art. 2(7) EECC).

[5] This has also been confirmed in the Q&A document published by the European Commission on 24 September 2019: "**Question**: "*Article 12(3) Can NI-ICS not be obliged to notify themselves to a Member States under the rules of the Code? Can Member States therefore not impose notification requirement on NI-ICS even for the purpose of monitoring compliance of those providers with the national obligations (stemming from the EECC or regarding legal interception in the broad sense)? Could such notification be justified on another legal basis than Article 12(3) (General*

DIGITALEUROPE also notes that some of the registration requirements go beyond the scope of Article 12 of the EECC, such as e.g. the condition in Art. 6 (1), 8° of the draft Law to indicate the "*area*" in which the telecommunications activities will be carried out, the '*criminal liability declaration*' foreseen in Art. 6 (2) of the draft Law, or the waiting period foreseen in Art. 8(2) of the draft Law. In the interest of harmonizing the digital single market, DIGITALEUROPE requests the Polish authorities to better align the notification process with the exhaustive conditions of the EECC and the BEREC guidance.

Security of Networks and Services (Art. 40 draft Law)

DIGITALEUROPE notes that the requirements to take technical and organisational measures to ensure the security of networks or services in Art. 40 onwards of the draft Law, apply to '*telecommunications undertakings*'. DIGITALEUROPE would welcome clarification whether this is intentional or whether this is an oversight with regard to the obligation in Article 40 EECC which applies to providers of public electronic communications networks[6] or providers of publicly available electronic communications services (as defined under the EECC).

Should the current security provisions in the draft Law be extended to NI-ICS, it is important that, in accordance with Article 40 EECC, such obligations are applied only to the extent these are appropriate and proportionate. For example, NI-ICS should not be subject to provisions concerned with network aspects, given that NI-ICS do not tend to control the networks over which their services are provided.

At a general level, DIGITALEUROPE takes this opportunity to urge the Ministry to ensure that the positions taken in the draft Law regarding transposition of the security

---

Authorisation) and included in national legislation on ICS?" **Reply**: "*As explained in the answer referred to on your question, Member States cannot subject NI-ICS to general authorisation or to any other prior authorisation or any other requirement having equivalent effect. As a consequence, they may not require the providers of these services to submit a notification under the General authorisation regime. Drawing on these notifications, the data-base maintained by BEREC will hence not include providers of NIICS.The provision of NIICS is not subject to general authorisation, and by consequence to notification obligations. In addition, Article 4 of the e-Commerce Directive 2000/31/EC prohibits Member States to subject the taking up and pursuit of the activity of an information society service provider to prior authorisation or any other requirement having equivalent effect. Paragraph 2 of the same provision states that this is without prejudice to authorisation schemes covered by the framework for general authorisations and individual licences in the field of electronic communications services. [ ]*"

[6] 'public electronic communications network' means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services which support the transfer of information between network termination points; (Art. 2(8) EECC).

of networks and services provisions in Art. 40 EECC do not undermine the preference for end-to-end encryption expressed in the EECC.

DIGITALEUROPE has the following comments regarding specific aspects of the security provisions in the draft Law:

Security measures and reporting/managing incidents

- Art. 40(3): provides the Minister for Computerisation to issue a regulation regarding the various measures listed in Art. 40(1) of the draft Law. In view of this possible regulation, DIGITALEUROPE wishes to emphasise the importance of harmonised rules because of the cross-border nature of new services.[7]
- Art. 42(3): contains certain additional criteria to those in Article 40(2) EECC for assessing whether or not a security incident has a "significant impact". The provisions in Art. 42(3) should instead be harmonized with those in Article 40(2) EECC.
- Art. 42(4): contains a wide obligation to inform about security best practices in general. For example:
  - Art. 42(4)(1) refers to potential risks associated with the use of telecommunications services.
  - Art. 42(4)(2) refers to recommended protective measures and the most popular ways to protect telecommunications terminal equipment against malware and to increase the security of the content of individual messages that users can take for the safety of the use of services, including the associated costs; and
  - Art. 42(4)(3) refers to the exemplary consequences of lack of or inadequate protection of telecommunications terminal equipment.
- The above requirements go beyond those set out in Article 40(3) EECC, which is limited to an obligation where there is a *particular and specific* threat of a security incident to inform users potentially affected by such a threat of any possible protective measures or remedies which can be taken by the users.
- Art. 42(5): requires a telecommunications undertaking to publish information about a security incident and its impact on the availability of services, if *in its opinion*, it has a significant impact on the services provided. DIGITALEUROPE appreciates the inclusion of the purported qualification that this should only be made available where this is required in '*its*' i.e., the

[7] See in particular the ENISA report on Security Supervision under the EECC, available at: https://www.enisa.europa.eu/publications/supporting-the-implementation-of-the-european- electronic-commmunications-code-eecc/

provider's opinion. DIGITALEUROPE considers that the current wording of Art. 42(5) goes beyond the requirement in Article 40(2) EECC which instead establishes an obligation to notify the competent authority.

- Art. 42(6): contains a provision whereby telecommunications undertakings "*may inform other telecommunications undertakings and entities forming part of the national cyber security system*" about incidents. DIGITALEUROPE believes it is important that should this provision remain in the draft Law, that this remains a possibility i.e., "*may*" rather than an outright obligation.
- Art. 44: DIGITALEUROPE notes that there is no equivalent provision on this issue (which appears to be aimed towards contingency planning) in Article 40 EECC. We therefore consider that it ought to be deleted. Should this provision nonetheless remain in the draft Law, DIGITALEUROPE considers that NI-ICS should be excluded from application of this requirement, particularly given that NI-ICS do not tend to control the underlying networks over which their services are provided. The same should apply to network independent NB-ICS providers.
- Art. 45(2): contains a list of potential restrictions that may be imposed on a telecommunications undertaking, in the event of particular threats. This provision seems to apply regardless of significance of both threats and services/networks. DIGITALEUROPE notes that there is no equivalent provision on this issue in Article 40 EECC and thus this provision goes beyond the scope of the EECC. Should this provision remain in the draft Law, DIGITALEUROPE considers that it is important NI-ICS and network-independent NB-ICS should be excluded from application of this requirement, for similar reasons to those stated above regarding Art. 44. Moreover, given the cross-border nature of NI-ICS, a potential limitation of scope or area (under Art.45(2)(b)) would be unduly restrictive and fundamentally undermines the basis on which such services are provided. Finally, DIGITALEUROPE considers it important that any purported restrictions reflect the provisions in EU's Open Internet Regulation (Regulation 2015/2120) and associated BEREC guidelines.

Law enforcement

As a general comment, DIGITALEUROPE considers that certain of the law enforcement requirements in Art. 46-48 of the draft Law disproportionate and/or not adapted to the specific nature of NI-ICS.

Generally speaking, DIGITALEUROPE does not consider it appropriate for the Polish legislature to introduce new lawful intercept requirements for cross-border NI-ICS providers via electronic communications legislation, or to extend existing intercept rules under Polish criminal or other laws to those providers without due consideration of the specific features of those providers' operations. The application of rules designed for fixed and mobile network providers established in Poland to cross-border NI-ICS would lead to conflicts with other Member State laws and restrict the

freedom of NI-ICS providers established in another Member State to provide cross-border NI-ICS in Poland.

DIGITALEUROPE also sets out the following specific comments on Art. 46 of the draft Law:

- Art. 46(6)[8] provides that telecommunications undertakings may prescribe the conditions applicable to lawful interception interfaces, including in respect of technical implementation and the location of the interfaces. DIGITAL EUROPE encourages [the Ministry] to address Poland's lawful interception requirements instead through consultation and dialogue with our members. Prescriptive technical requirements could disproportionately restrict the freedom to provide services from another Member State as envisaged by the EECC, and may not be the most effective way to achieve [the Ministry's] requirements given the features of our members' products and our members' obligations under both the EECC and other Member State laws to which they are subject. s.
- Art. 46(7): DIGITALEUROPE invites [the Ministry] to clarify the nature of the "*access...without the participation of employees*" envisaged under this draft Article. Any arrangements for lawful interception handover must have regard to applicable standards, our members' obligations under the EECC and the EU Charter, and other EU and Member State laws (be it in the criminal law area or in the privacy/human rights sphere), as well as the specific characteristics of the services at issue. . In particular, the draft Law must not undermine the position in the EECC which contains a presumption in favour of end-to-end encryption services[9].

Data retention

- Art. 52: contains an obligation on an "*operator of a public telecommunications network and the provider of publicly available telecommunications services*" to store retained data locally, on Polish territory. DIGITALEUROPE

[8] Complemented by Article 50 (2) of the draft Law.

[9] Art. 40(1) EECC: "Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Having regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. *In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services"*; and recital (97) EECC: "In order to safeguard security of networks and services, and without prejudice to the Member States' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences, *the use of encryption for example, end-to-end where appropriate, should be promoted and, where necessary, encryption should be mandatory* in accordance with the principles of security and privacy by default and by design." (emphasis added)

understands that this provision does not apply to NI-ICS. As a general comment, DIGITALEUROPE considers that the requirement to store data locally is disproportionate and risks undermining free movement of data and establishment of a Digital Single Market. Notwithstanding this, DIGITALEUROPE respectfully requests that should this provision remain in the draft Law, services provided on a cross-border basis from establishments, or using infrastructure in, another Member State are explicitly excluded.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice
Senior Policy Manager for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

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 Membership

Corporate Members

Airbus, Amazon, AMD, Apple, Arçelik, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Epson, Ericsson, Facebook, Fujitsu, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Qualcomm, Red Hat, Ricoh Europe PLC, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Xerox.

National Trade Associations

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