Council of European National Top-Level Domain Registries

Brussels, Belgium
26 March 2019

CENTR Comment on the Proposal on e-Evidence

Introduction

CENTR is submitting the following comment on the proposal for a Regulation of the European Parliament and of the Council on the European Production and Preservation Orders for electronic evidence in criminal matters (COM/2018/225 final - 2018/0108 (COD) (hereinafter the Proposal).

CENTR is the association of European country code top-level domain (ccTLD) registries. All EU Member State and EEA country ccTLDs (such as .de, .no, and .nl) are members of CENTR.

CENTR members represent the industry that is at the core of the public internet, safeguarding the stability and security of the internet as we know it today. The majority of European ccTLDs are SMEs or non-profit organisations, providing an internet infrastructure service in the interest of and in close cooperation with their local internet communities (i.e. registrars, end-users, rightsholders but also in cooperation with CERTs and law enforcement authorities).

The Proposal directly concerns the data held by ccTLD registries that, according to the European Commission in its relevant Explanatory Memorandum to the Proposal, "[...]may be of relevance for criminal proceedings as **they can provide traces allowing for identification of an individual or entity involved in criminal activity**[emphasis added]" (Recital 18 of the Proposal). Article 2(3)(c) of the Proposal enlarges the scope of "service providers" affected by the Proposal to include domain name registries.

ccTLD registries maintain a registration database that is used to collect and access the contact information of domain name holders. In addition, Domain Name System (DNS) operators such as ccTLD registries are responsible for the resolution of domain name queries when a respective website in their domain name zone is requested. Based on the Proposal and the data categories held by service providers, as introduced by the European Commission, the data held by ccTLDs can thus be classified as "subscriber data" (i.e. registration data) and "access data" under the overarching category of "non-content" data (Recital 20 and 21 of the Proposal).[1]

As "Internet infrastructure providers" who are directly affected by the Proposal and the obligations within, CENTR members ask legislators to take into consideration and adequately assess the impact of the proposed legislation on ccTLD operators, who form the core of the public internet and are referred to as "operators of essential service" in

[1] It is noteworthy, however, that the type of activities that ccTLDs operators are performing cannot be generally described by the terminology used in the Proposal, as ccTLDs do not operate with the terms such as "subscribers".

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium

Phone: +32 2 627 5550
Fax: +32 2 627 5559
secretariat@centr.org

www.centr.org

the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

CENTR members would like the co-legislators to address the following areas of concern in the Proposal.

Areas of concern

1. Involvement of national authorities

The Proposal establishes a framework for a cross-border European Production Order (EPOC) and a European Preservation Order (EPOC-PR) to be issued by an authority in one Member State to access data held by a service provider in another Member State. The data ordered through an EPOC(-PR) from one Member State should be provided directly to the authorities ***without the involvement of national authorities in another Member State***.

Hereby, it is important to note that the Proposal does not foresee any appropriate safeguards for the verification of these foreign data access requests, leaving service providers to rely on their limited capacity to adequately respond to such requests, from potentially all EU Member States. ccTLD operators have well-established information channels to their local law enforcement authorities, meaning that the mutual trust is established by a long-standing practice and network-building. It is a disproportionate burden on ccTLD operators to assume that they can verify all possible judiciary, competent prosecutor, and any other competent authorities as defined by all issuing Member States that could approach a ccTLD operator with an EPOC(-PR) to hand out personal information on individuals.

It is, therefore, essential to make sure that the burden of verification of competent authorities does not lie on the internet infrastructure providers, whose main business activity lies in providing a stable and secure service, rather than responding to foreign data access requests.

CENTR believes that the list of competent authorities should be significantly shorter than proposed by the European Commission and should **be strictly limited to competent judiciary authorities (including courts)** in order for ccTLD operators to effectively respond to the EPOC(-PR) in the proposed time limits.

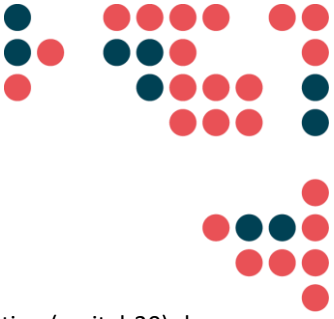
This requirement will also be more consistent with the Proposal that already envisages the judiciary validation of the competent authorities, in case these are involved in the criminal proceedings (Article 4 of the Proposal). It is, therefore, more consistent with the purpose of the Proposal to make sure that only competent judiciary authorities may issue EPOC(-PR)s, leaving the verification burden to the authorities whose main responsibility is to follow and ensure the appropriate application of rule of law.

In addition to this limitation, it is essential to ensure that the efforts of verification of these cross-border competent authorities that issue EPOC(-PR) are also made either by national law enforcement authorities (as the closest to the service provider) or in coordination with the Member States' law enforcement authorities (e.g. Europol), through trusted and secure communication channels between authorities and ccTLD operators.

2. Type of data

As indicated above, ccTLD operators process "subscriber" and "access" data that are referred to as "non-content" data in the Proposal. The "non-content data" is treated differently from the so-called "content" data that has a higher level of authoritative oversight in the context of EPOC(-PR), according to the Proposal. For "non-content data" the EPOC(-PR) can also be issued by a prosecutor, in addition to the competent judiciary authorities. For "content data", on the contrary, EPOC(-PR) can only be issued by competent judicial authorities.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org



According to the reasoning of the Proposal, the "non-content" data is considered less sensitive (recital 30), hence different conditions are imposed for obtaining subscriber and access data on the one hand, and transactional and content data on the other.

Given the differentiation between types of data in the Proposal, according to which "transactional and content data are the most relevant as probative material" (Recital 23), it is disproportionate to put the burden of approving access to personal data of individuals within the proposed strict deadlines (i.e. 6 hours in the case of emergency) on ccTLD operators. Furthermore, when the type of data requested from service providers is not even assessed to the same level of relevance for investigators, there is no justification for such stringent obligations and deadlines to be put on internet infrastructure providers for issuing access to "subscriber" and "access" data.

Hereby, it is worth reiterating that the reasoning of the Proposal to categorise "subscriber" and "access" data differently, based on a lesser interference with fundamental rights, is not entirely convincing. Both categories are described as a means to "provide traces allowing for identification of an individual" according to the Proposal and are thus considered to be "personal data" that is governed by the respective data protection rules.

The claimed lesser probative quality of "subscriber" and "access" data for the investigators cannot be considered an adequate reasoning for lowering the standards of data protection in the European Union, and especially at the expense of operators of essential services like ccTLDs.

CENTR members ask the co-legislators to **treat all personal data according to the respective data protection rules** as enshrined in the General Data Protection Regulation (GDPR). A proper **impact assessment of the different types of service providers needs to be conducted** before any decisions are made, especially in relation to personal data, that has little probative quality for investigators.

3. Transmission of data

According to Article 9 of the Proposal, all addressees of the EPOC are obliged to ensure that the requested data is transmitted to the authorities at the latest within 10 days upon receipt of the EPOC. In emergency cases the addressee shall transmit the requested data without undue delay, at the latest within 6 hours upon receipt of the EPOC.

The Proposal gives little clarification as to how the personal data of individuals shall be transmitted to the authorities, ensuring its security, integrity and confidentiality. Proper verification mechanisms need to be put in place, especially in light of the increased number of foreign authorities requesting personal data from the operators. Operators need to be able to trust foreign data access requests as legitimate, as well as be able to securely transmit the requested data back to competent authorities.

The emergency deadline of 6 hours essentially entails a 24-hour service from ccTLD operators, that are primarily SMEs or non-profit organisations. Considering the fact that the data held by the registries is of low probative quality for the investigators and can only be used as supportive evidence to malicious activity, it is a disproportionate burden on ccTLD registries to mandate a 24-hour service to respond to cross-border data transmission requests.

CENTR members therefore ask legislators **to take into consideration the size of an operator and probative quality of requested data**, as well as adequately **re-assess the plausibility of transmission of data within suggested deadlines**, without prejudice towards general data protection rules of all personal data.

4. Inability to comply with EPOC(-PR)

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

Article 9 and 10 of the Proposal give an opportunity for addressees to deny the EPOC(-PR) in case of a "force majeure or of de facto impossibility not attributable to the addressee[...]or the data has been deleted before receiving the EPOC".

It is notable that in regard to the EPOC(-PR) the obligation to issue and preserve data for a particular amount of time might be in direct conflict with data minimisation and anonymisation efforts conducted under the GDPR. It is therefore essential to make sure that activities carried out by service providers to comply with their data protection obligations are explicitly considered as part of the de facto impossibility not attributable to the addressee in the meaning of Article 9 and 10.

In addition, the technical impossibility to revert the automated deletion of particular data needs to be reflected in the text of the Proposal. It is therefore essential **to include the reference of "technical impossibility" to comply with the EPOC(-PR) as a legitimate basis for withdrawing the EPOC(-PR).**

5. **Other practical issues**

The proposed EPOC(-PR) templates are a welcome step towards outsourcing the burden of translation of cross-border data access requests away from service providers, the majority of which are SMEs (in Europe) and which do not necessarily have the capacity to provide services in all EU official languages.

Furthermore, these templates do not provide enough means for service providers to be able to verify that the provided information is valid and correct. Therefore, it is essential to make sure that the **verification of unfamiliar foreign authorities is done by a competent authority trusted by the service provider, either in connection to the local law enforcement and judiciary authorities or on a more coordinated level through Europol.**

The templates also do not provide an opportunity to provide any additional information about the request, beyond the details of the request itself. It might be beneficial to attach any supporting documentation for the service providers to be able to assess the validity of a foreign data access request. However, one needs to bear in mind that even if this additional documentation were provided, the service provider might also not be in a position to adequately assess this information, mainly due to the challenges derived from the need for translation. Hereby, it is worth reiterating that ccTLDs are predominantly non-profit organisations and SMEs, serving their local internet communities according to the specific local jurisdictions, with well-established communication channels with the local law enforcement authorities. This means that ccTLDs operate within national restrictions, including in terms of language.

Recommendations

- CENTR calls for co-legislators to shorten the list of competent authorities. This list should be strictly limited to competent judiciary authorities (including courts) in order for ccTLD operators to effectively respond to the EPOC(-PR) in the proposed time limits.
- CENTR calls for co-legislators to ensure that the verification of unfamiliar foreign authorities is done by a competent authority trusted by the ccTLD operator, either in connection with the local law enforcement and judiciary authorities or on a more coordinated level through Europol.
- CENTR asks co-legislators to treat all personal data according to the respective data protection rules as enshrined in the General Data Protection Regulation. Proper impact assessments on different type of service

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org

providers need to be conducted before any decisions are made, especially in relation to personal data, that has little probative quality for investigators.

- CENTR asks co-legislators to take into consideration the size of an operator and probative quality of the requested data, as well as adequately re-assess the plausibility of the transmission of data within the suggested deadlines, without prejudice towards general data protection rules of all personal data.
- CENTR asks co-legislators to ensure the safeguards for personal data of individuals to be transmitted to the authorities in a secure and confidential way. Proper verification mechanisms need to be in place, especially in light of the increased number of foreign authorities requesting personal data from operators
- CENTR asks co-legislators to make sure that activities carried out by ccTLD operators to comply with their data protection obligations under GDPR are explicitly considered as part of de facto impossibility in the meaning of Article 9 and 10.

About CENTR

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 54 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries. Full membership is open to organisations, corporate bodies or individuals that operate a country code top level domain registry.

CENTR vzw/asbl · Belliardstraat 20 (6th floor) · 1040 Brussels, Belgium
Phone: +32 2 627 5550 · Fax: +32 2 627 5559 · secretariat@centr.org · www.centr.org