Council of European National Top-Level Domain Registries

Brussels, Belgium
14 December 2020

CENTR response on the provisional draft text of the Second Additional Protocol to the Budapest Convention on Cybercrime

CENTR is submitting the following feedback on the provisional draft text of the Second Additional Protocol to the Budapest Convention on Cybercrime, namely the proposal for Article 6 - Request for domain name registration information (hereinafter the 'Proposal').

CENTR is the association of European country code top-level domain registries (ccTLDs). All EU Member State and EEA country ccTLDs (such as .de, .no, and .si) 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 CSIRTs and law enforcement authorities).

ccTLD registries maintain a registration database that is used to collect and access the contact information of domain name holders (via the so-called WHOIS protocol). In addition, Domain Name System (DNS) operators such as ccTLDs are responsible for the resolution of domain name queries when a website in their domain name zone is requested.

As an "entity providing domain name services" who are directly referenced in the proposal for Article 6 and the Draft Explanatory Report, CENTR members ask the PDP and the PDG to adequately take into consideration the impact of the proposed text on ccTLD operators.

CENTR recommendations

1. Legal clarity

The Proposal aims to ensure the availability of "legislative and other measures" for competent authorities to issue a request to an entity providing domain name services in the territory of another Party for information "for identifying or contacting the registrant of a domain name", without explicitly mentioning any involvement of national competent authorities, nor applying rule of law safeguards in the receiving Party.

It is unclear from the Proposal to what extent national competent authorities within the receiving Party can be involved, beyond adopting necessary "legislative and other measures". According to the respective Draft Explanatory Report, the information requests need to be issued "without requiring the authorities in the territory where the entity is located to act as an intermediary".

CENTR vzw/asbl
Belliardstraat 20 (6th floor)
1040 Brussels, Belgium
0885.419.166
RPR Brussel
Phone: +32 2 627 5550
secretariat@centr.org
www.centr.org

For the sake of legal clarity for the operators and national competent authorities, ***the explicit mentioning of limits within the national jurisdiction needs to be maintained in the Article: i.e., information requests are "subject to reasonable conditions provided by domestic law" (para. 2).***

Any data access request from a foreign competent authority needs to be subject to at least the same level of procedural safeguards as the data access request from a national authority. For foreign data access requests, the need for clear, predictable and consistent rules is even greater than with national competent authorities, as in the latter case trusted information channels are usually already in place between ccTLD registries and national competent authorities. This cannot be assumed for all potential "competent authorities" across the Parties, nor that each data access request can be appropriately assessed by ccTLD registries.

CENTR recommends to explicitly reference the principles of proportionality and necessity in a democratic society. According to the jurisprudence of the European Court of Human Rights (ECtHR), the Contracting Parties may not in the name of national security adopt whatever measures they deem appropriate, and adequate and effective guarantees against abuse must be in place.

The Draft Explanatory Report also recognises that domain name registration information may be personal data that may be protected under data protection regulation in the receiving Party. According to the Draft Explanatory Report, registration data collected by domain name registries contains information such as the name, physical address, email address and telephone number of a registrant. However, its disclosure may "be less intrusive than the disclosure of other categories of data" according to the Draft Explanatory Report. Hereby, it is worth mentioning that the concept of private life extends to aspects relating to personal identity, including a person's name. It covers personal information which individuals can legitimately expect not to be published without their consent (Article 8 of the European Convention of Human Rights [ECHR]).

The limits of interference with individuals' private life ***must follow the established rules and procedures in the receiving Party, including the respective data protection safeguards***. In jurisdictions where the personal information of private individuals is redacted via WHOIS due to data protection considerations, each registrant has a reasonable expectation that their personal information is not made publicly available. The situation where any competent authority across each Party can obtain this personal information in another Party creates a peculiar situation where such information can almost be considered public due to the almost infinite pool of parties able to query such information. In addition, a situation such as this creates a disproportionate overburden for technical operators such as ccTLDs, whose role is first and foremost to maintain and provide a stable and secure service, rather than responding to foreign data access requests.

2. Verification of data access requests

Furthermore, the Proposal does not mention any means for verification of data access requests from foreign competent authorities. It is, therefore, not entirely clear which conditions such data access requests can be made on and under which circumstances.

According to the Draft Explanatory Report, "the form of implementation depends on the Parties' respective legal and policy considerations" and the article "is intended to complement current and future internet governance policies and practices". It is understandable that to be implementable in a variety of different jurisdictions and in a rapidly evolving area such as cybercrime, the Proposal cannot be too prescriptive.

However, there is a need to reflect a few principles for ensuring the rule of law, according to the ECHR, primarily Article 7.

According to Article 7 of the ECHR, "no one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed". This should be especially relevant in the context of cross-border (criminal) investigations.

Although, Article 7 of the ECHR does not address any "requirements as to the procedure in which those offences must be investigated and brought to trial", Article 7 of the ECHR guarantees "that criminal offences and the relevant penalties must be clearly defined by substantive criminal law". In essence, criminal law must be accessible and foreseeable in its effects, according to the respective case-law of the ECtHR.

The principle of foreseeability requires from the State that a rule "affords a measure of protection against arbitrary interferences by the public authorities".

Stemming from these principles, it is essential to reflect more on procedural guarantees in connection to cross-border data access requests, as there is a risk of losing sight of accessibility and foreseeability principles in criminal investigations.

Therefore, foreign data access requests should be ***subject to ex-ante or simultaneous checks by independent national competent authorities (incl. judiciary)***, at least for establishing a proper legal basis within the receiving Party and a confirmation of the offence punishable also under the receiving Party's jurisdiction. Such necessary checks by trusted national competent authorities will also give additional confidence to ccTLD registries to positively respond to the respective data access requests.

3. Specific criminal investigations and proceedings

The Proposal mentions that data access requests for domain name registration information need to be "for purposes of specific criminal investigations or proceedings".

It is necessary to make sure that any data access request from a competent authority directed towards ccTLD registries should only concern the information that is strictly necessary to achieve a legitimate purpose. Blanket, vague and broad data access requests directed towards domain name registries affect technical operators disproportionately, creating organisational overload and a burden on the technical operators.

CENTR, therefore, ***welcomes the attention that the Proposal gives to the need to "avoid broad requests for the disclosure of domain name information***" in the Draft Explanatory Report. This requirement needs to be maintained in the text of the Proposal.

Additionally, the Proposal also recognises that it is necessary for domain name registries to be able to object to data access requests by foreign competent authorities. Private parties, like ccTLDs, should be able to raise objections to data access requests by foreign competent authorities when the justification for the data access request is not sufficiently clear, and they should be able to require additional information to respond to the data access request.

The Proposal explicitly recognises the potential role for national competent authorities only in the event of non-cooperation by a private entity like a ccTLD registry. In this event, the requesting Party may seek consultation with the Party in which the entity is located.

Therefore, it is worth reiterating that despite it being a welcome step to involve national competent authorities at least at some point within the procedure, this is not a sufficient safeguard against potential abuse by State officials in the procedure for accessing and transferring personal information. This is especially relevant in the context of bulk data access requests, that are still possible under the Proposal and according to the Draft Explanatory Report, as these

might be necessary in the context of "specific criminal investigations". Accordingly, additional categories such as a balancing test between the seriousness of a crime and the burden on technical operators such as ccTLDs should be considered.

While ***CENTR welcomes the ability for domain name registries to refuse to cooperate with the requesting foreign competent authority***, according to the Proposal, it is still ***necessary to include additional proper procedural safeguards for foreign data access requests.*** This is in order to ensure that the receiving Party is not deprived of their fundamental responsibility to ensure the respect of fundamental rights on their territory and would, at the same time, not deprive ccTLD registries from their obligation to respect the laws of the country where they are established. The appropriate involvement of national competent authorities cannot be denied in this regard, nor be considered trivial.

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.