Council of European National
Top-Level Domain Registries

Brussels, Belgium
29 April 2021

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

Introduction

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

CENTR is the association of European country code top-level domain registries (ccTLDs).

CENTR members are 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 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).

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. ccTLDs are primarily responsible for operating and maintaining the technical DNS infrastructure for their top-level domain. 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).

As an "entity providing domain name services" who are directly referenced in Article 6, CENTR members ask the Cybercrime Convention Committee (T-CY) to adequately take into consideration the impact of the proposed text on ccTLD operators.

Recommendations

As per CENTR previous submission in the 5th round of stakeholder consultations, CENTR would like to reiterate a few key recommendations, to increase legal clarity for domain name registries, competent public authorities and data subjects affected by the provisions in Article 6.

1. Balancing test with proportionality

Article 6 requires each Party to adopt "such legislative and other measures as may be necessary" to empower its competent authorities to issue registration data access requests to entities providing domain name services in the territory of another Party.

It is worth recalling that domain name registration data is considered personal information and is therefore protected under the respective data protection framework of EU primary and secondary law. The member States of the Council of Europe and the other State Parties to the Convention on Cybercrime that are not governed by the EU General Data Protection Regulation must nevertheless comply with any applicable national or international law with respect to privacy and data protection.

Any data access request directed at domain name registries with regard to data that is not publicly available ought to be considered an interference with individuals' fundamental rights, namely the right to respect for private and family life (Article 8 of the European Convention on Human Rights), and data protection (Article 8 of the Charter of Fundamental Rights of the EU). Any interference with fundamental rights needs to be based on a clear legal basis, considering it is also necessary and proportionate 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.

It is, therefore, necessary to reference the principle of proportionality directly in Article 6(2): "Each Party shall adopt such legislative and other measures as may be necessary to permit an entity in its territory to disclose such information in response to a request under paragraph 1, **subject to reasonable and proportionate conditions provided by domestic law, including a clear legal basis.**"

2. Minimum requirements of data access requests

Article 6(3) includes a list of requirements for domain name registration data access requests subject to this provision. While this list is helpful in limiting the scope of domain name registration data requests, it should be considered as a minimum level of necessary requirements for such data access requests. In addition, the requesting authority should clearly state the legal basis under the respective data protection framework (i.e. Article 6 of EU General Data Protection Regulation - GDPR) it is using to seek such access. As domain name registries can be considered data controllers/processors in relation to domain name registration data, they are subject to respective obligations under the EU GDPR. International treaties, such as the Budapest convention, together with its additional protocols, cannot have the effect of prejudicing the constitutional principles of the EU treaties (as pointed out by the European Data Protection Board in its respective statement on the matter in question).

Article 6(3) should be amended to include a statement on the applicability of a clear legal basis under domestic legislation, including the overarching data protection framework.

3. Verification of data access requests

Cross-border 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 domain name registries to respond positively to the respective data access requests. In light of European Court of Justice (CJEU) case-law, the type of requesting authorities who may issue such requests should be limited to an independent prosecutor, a judicial authority or another independent authority.

Article 6 must be amended to ensure an appropriate involvement of independent national competent authorities, including an adequate judiciary review of cross-border data access requests, to abide by the principles of accessibility and foreseeability in criminal law and offer a measure of protection against arbitrary interferences by public authorities. Domain name registration data can be considered a subset of subscriber data, and there is no adequate justification why it should be treated according to lower data protection standards.

4. Additional procedural safeguards

CENTR welcomes the ability for domain name registries to refuse to cooperate with the requesting foreign competent authority in Article 6. However, this cannot be considered as a sole appropriate safeguard against the potential abuse of fundamental rights, as it puts a disproportionate burden on technical operators such as domain name registries to conduct the necessary human rights impact assessment.

It is necessary to include additional proper procedural safeguards for cross-border 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, at the same time, would not deprive ccTLD registries from their obligation to respect the laws of the country where they are established.

Article 6 must include an explicit reference to appropriate safeguards pursuant to Articles 13 and 14 of the protocol, including grounds for objection to provide relevant information to foreign authorities if the safeguards in Article 13 and Article 14 are not met.

Article 6 should be amended to include that "**the information disclosed in response to a request under paragraph 1 shall be subject to appropriate safeguards pursuant to Article 13 and 14 of the additional protocol**".

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 53 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.