28 FEBRUARY 2022 • *Brussels, Belgium*

CENTR Board Statement on the call for evidence on an EU Toolbox against counterfeiting

Summary of CENTR key recommendations

- For the sake of consistency with existing EU legal framework, and to maintain legal clarity when it comes to targeted action against counterfeiting, CENTR members recommend maintaining the proportionality standard established in the CPC Regulation.
- It is essential to provide a legal basis for actions at DNS level, alleviating concerns in cases of wrongful actions and ensuring the right to remedy. Therefore, in the case of counterfeiting, only public competent authorities should be able to mandate action from ccTLDs.
- Where appropriate and depending on local jurisdiction, European ccTLDs should be able to continue carrying out voluntary measures to contribute to the overall safety of their domains.
- European ccTLDs are ready to share their practices with other TLD operators to contribute to creating a safer online environment.
- Competent authorities should remain the main point of contact for any personal data disclosure request targeted at ccTLDs to ensure consistency with the overarching data protection legislation.
- Any "Know-Your-Customer" (KYC) requirements should be in line with the basic data protection principles, such as purpose limitation and data minimisation, enshrined in the EU GDPR.

Introduction

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

CENTR members are at the core of the public internet, safeguarding the stability and security of the internet. The majority of European ccTLDs are non-profit organisations or SMEs, providing an internet infrastructure service in the interest of and in close cooperation with their local internet communities (e.g. registrars, end-users, rightsholders, CSIRTs, law enforcement authorities).

ccTLDs are responsible for operating and maintaining the technical Domain Name System (DNS) infrastructure for their top-level domain. The DNS is a well-established network protocol at the heart of the internet infrastructure – commonly thought of as the "phone book of the internet". It provides a navigation function to map user-friendly domain names to numeric IP addresses. ccTLDs only hold information enabling users to navigate the internet but do not store, transmit or enhance any content online.

CENTR welcomes the European Commission's call for evidence in the context of the EU Toolbox against counterfeiting and wishes to submit the following recommendations to **support fact-based and informed policymaking**, in line with the principle of proportionality.

The role of ccTLD registries

ccTLDs are only one of several internet infrastructure actors that enable users to reach content or send emails. ccTLDs enable domain names to point to an IP address on which these services (e.g. a website or an email server) are hosted. Furthermore, ccTLDs maintain a registration database that contains the names and contact details of domain name holders. Elements of this registration database are publicly accessible via the so-called WHOIS. In addition, ccTLDs, as technical operators of the internet infrastructure, are considered to be 'operators of essential services' under Directive 2016/1148 [NIS Directive]) and 'essential entities' under the upcoming revision of the NIS Directive (NIS 2 Directive).

Each ccTLD maintains the authoritative name server for the specific top-level domain(s) managed by that ccTLD. Every authoritative name server managed by a ccTLD provides information about all the delegations and complete DNS information of registered domain names.

A domain name and its management are distinct from, and cannot be equated with the content of any services related to the domain name, that are provided by other intermediaries (such as web hosting companies, mail service providers etc.).

CENTR welcomes the general objective of the EU Toolbox against counterfeiting to set out a coherent, effective and coordinated action against counterfeiting, both online and offline. However, it is worth pointing out that in addition to being coherent, effective and coordinated, any **action targeting intermediaries lower in the internet stack and further away from the content, such as ccTLD registries, needs to be necessary and proportionate**.

ccTLDs do not have the technical capacity to directly target unlawful content online. They can only suspend the underlying technical infrastructure, i.e. the domain name, that will disrupt the functioning of all associated services (such as website or email hosting). However, this drastic measure does not remove illegal content from the internet: the unlawful content remains reachable through other means (e.g. directly typing the IP address in the browser).

The existing legal framework in the area of consumer protection clearly establishes a certain proportionality standard when action at ccTLD level can be mandated. According to the Consumer Protection Cooperation

Regulation[1], the deletion of a fully qualified domain name can only be considered as a potential measure available to competent authorities "where no other effective means are available to bring about the cessation or the prohibition of the infringement[...] and in order to avoid the risk of serious harm to the collective interests of consumers" (Article 9(4)(g)). In addition, any action at ccTLD level can only be mandated "when appropriate" and when contacting other intermediaries closer to the content has not brought about any results.

For the sake of consistency with the existing EU legal framework, and in order to maintain legal clarity for ccTLD registries when it comes to targeted action against counterfeiting, **CENTR members recommend maintaining the proportionality standard established in the CPC Regulation**, when discussing new legislative initiatives in the area of Intellectual Property rights (IPR) enforcement. Any conflicting obligations run the risk of having disproportionate and undesirable effects on the internet's infrastructure.

The role of competent authorities

Due to the technical role of ccTLDs and their role as essential service providers, it is crucial to ensure that **a close cooperation between ccTLD registries and competent public authorities is maintained** when any action at DNS level is mandated (in response to targeting the availability of illegal content online). The qualification of the (il)legality of content depends on the local legal framework and, except for cases when content is illegal beyond any doubt, should be assessed as such by competent authorities. This is especially the case in the area of IPR infringements, that not only require specialised knowledge and insight, but also a balancing act with other public interests involved (e.g. in the area of copyright exceptions). A ccTLD registry does not have a special authority to effectively judge over the legality of content that is put online.

As counterfeited products and their risk to consumers may legitimately fall into the area of consumer protection, it is necessary to **ensure that already existing competent authorities, such as consumer protection authorities, are adequately equipped and resourced to address consumer protection infringements online, including counterfeited products**. Additionally, the CPC Regulation already establishes the minimum powers available for consumer protection authorities to take in response to serious infringements online.

Furthermore, due to the risk of inflicting collateral damage on the lawful use of services when action at DNS level is mandated, it is in the interest of legal clarity and proportionality that **an appropriate assessment of the illegality of content is done by a competent authority before addressing ccTLD registries**. Moreover, it is worth pointing out that suspension of domain names cannot be considered as an interim measure that can easily be reversed. As a result, **any action at DNS level in response to illegal content available through associated services (such as websites) can only be considered when the illegality of the content has been appropriately assessed and if possible, established by competent authorities**. A proper legal basis for any action mandated at DNS level will help to alleviate any concerns with potential liability claims in case of wrongful action. An appropriate legal basis is also needed to ensure that affected individuals and other rightsholders can effectively

1 Regulation (EU) 2017/2394 on the cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004

exercise their right to remedy, in cases where they are deprived from accessing a fundamental digital infrastructure as a result of a wrongful action.

The relevant legal expertise available to rightsholders can be streamed into the process by making sure **there is an effective way for rightsholders to flag counterfeited material to competent authorities** who can then perform the necessary assessment and mandate action from appropriate intermediaries.

Voluntary cooperation mechanisms with authorities

In order to be able to assess the necessary level of regulatory intervention in the area of IPR infringement online, an appropriate impact assessment is needed to provide neutral and objective data on the size of the problem (e.g. any quantitative and qualitative analysis on the scale of trademark infringements in the EU); and the breakdown and analysis of the types of intermediaries whose services and infrastructure are used to commit trademark infringements (e.g. hosted websites within specific TLDs, online marketplaces, social media platforms etc).

When it comes to the DNS level and specifically with regard to potential illegal activity associated with domain names, the recent DNS Abuse study[2] unfortunately does not provide enough analysis linking counterfeiting activities to the misuse of domain names. The statistics that are predominantly cited within the study refer to general reports and figures that do not reflect the size of the problem in connection to particular ccTLDs but concern IPR infringements taking place all over the internet ecosystem, including online marketplaces and social media[3]. Furthermore, the authors of the study have pointed out that "further studies would be needed to analyse and assess extensively the economic and societal impact of DNS abuse and its various types on EU citizens and businesses and the sectors which are more exposed to such phenomenon". Limited information from the WIPO UDRP statistics, as evident from the DNS abuse study, shows that counterfeiting in cybersquatting cases did trend down slightly in the period of 2018-2021[4].

In the absence of compelling evidence of a widespread problem with counterfeiting within European ccTLDs, it may be assumed that the existing good practices and voluntary measures taken by ccTLDs to tackle any illegal content online are sufficient in keeping abuse out of European ccTLDs. ccTLDs would gladly share their practices with other TLDs to contribute to a safer online environment.

Therefore, **ccTLDs should be able to continue carrying out voluntary measures, where appropriate,** in the context of fraudulent activity linked to a domain name, depending on the local jurisdiction. These voluntary measures could include additional cooperation agreements with law enforcement authorities[5] and consumer

[2] Study on Domain Name System (DNS) Abuse, written for the European Commission, January 2022.

[3] See for example, EUIPO 2020 Status Report on IPR Infringement that suggests that online marketplaces and social media are increasingly more abused by the criminal groups to engage in the sale of counterfeit products.

[4] Study on Domain Name System (DNS) Abuse, p.78.

[5] E.g. Nominet's (.uk) successful cooperation with the Police Intellectual Property Crime Unit (PIPCU) in Operation Ashiko to reduce the number of counterfeit sites: https://www.nominet.uk/record-low-for-number-of-uk-domains-suspended-by-law-enforcement/

protection authorities to ensure swifter actions[6]; and/or the exchange of statistical data and trends with like-minded partners[7], just to name a few.

Access to registration data

ccTLD registries maintain a domain name registration database. This database contains the contact information of domain name holders, technical and administrative data necessary to provide DNS services. Only part of these registration databases is publicly accessible within the limitations of national and regional legislation. Registration data can be queried by the general public using different protocols like the web, WHOIS and RDAP, each offering their own unique controls to comply with the EU General Data Protection Regulation (GDPR).

European ccTLDs have established various ways and methods to keep registration data accurate. Some ccTLDs make use of national eID schemes in the process of domain name registration[8], others perform additional registration data checks post-registration based on the internal tools available for screening new registrations[9]. Means and practices available for European ccTLDs vary depending on the national legal frameworks, and the availability of functioning eID schemes and other digital identification tools. Any 'Know-Your-Customer' (KYC) **requirements that may oblige ccTLDs to collect more personal information need to be in line with the limits of the EU GDPR, including purpose limitation and data minimisation**. It is also worth pointing out that a specific data accuracy obligation for the purposes of enhanced cybersecurity would be applicable to ccTLDs as part of the upcoming NIS 2 Directive. Any conflicting or duplicating obligations on data accuracy, including extensive KYC requirements as part of IPR enforcement discussions, are not justified, considering the low level of abuse within ccTLDs.

In addition, access to registration data is governed by the EU GDPR, and other national data protection frameworks. Access to registration data by law enforcement authorities is governed by the upcoming e-Evidence framework[10], and the NIS 2 Directive. Any data access request needs to meet the requirements of lawful access based on "legitimate interest", that includes **transmitting personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority** (EU GDPR, Recital 50). It is also worth pointing out that ccTLDs can provide non-public registration data details

[6] E.g. DNS Belgium's (.be) cooperation agreement with FPS Economy: https://www.dnsbelgium.be/en/news/fraudulent-websites-offline

[7] E.g. EURid's (.eu) collaboration with the International Anti-Counterfeiting Coalition: https://eurid.eu/en/news/eurid-and-iacc-team-up-to-fight-cybercrime/

[8] E.g. The use of NemID for verifying identities of individuals and businesses based in Denmark by DK Hostmaster (.dk); the Estonian Internet Foundation requires verification of .ee registrants with the use of Estonian eID solutions and also accepts the use of ID cards from Belgium, Latvia, Lithuania, Finland.

[9] E.g. the APEWS tool developed by EURid to screen for potentially abusive registrations; screening system developed by DNS Belgium to scan new registrations for incorrect registration data; machine learning tool used by SIDN (.nl) to identify potentially fake webshops.

[10] Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final - 2018/0108 (COD).

through dedicated WHOIS disclosure forms that are generally available for all interested parties that can demonstrate their legitimate interest.

Since competent public authorities, including law enforcement authorities, are the ones whose primary responsibility is to protect consumers from harm, and the transmission of personal data to these authorities in individual cases is clearly covered by the "legitimate interest" under the GDPR, these **competent authorities should remain as the main contact point for any personal data disclosure requests targeted at ccTLDs** in clear cases of consumer protection infringements. This is in line with the existing legal framework in the area of consumer protection (Article 9 of the CPC Regulation), and is within the provisions of the upcoming Digital Services Act (DSA)[e.g. Article 9 of the DSA proposal].