



2 MAY 2023 • Brussels, Belgium

# CENTR feedback to the Global Digital Compact

## Summary of CENTR's recommendations

- CENTR urges governments to refrain from introducing unnecessary and disproportionate barriers to the domain name registration process via national and international legislation, as well as promote balanced and evidence-based policymaking, in order to retain the universal accessibility of essential digital infrastructure, such as the DNS.
- To ensure balanced and evidence-based policymaking, we strongly encourage greater dialogue between policy-makers and the technical internet infrastructure community.
- All stakeholders should support and respect the multistakeholder governance of the DNS, which facilitates the development of common open standards and protocols supporting global interoperability (e.g., standard-setting in the IETF).
- Given the cross-border nature of the technical infrastructure, governments should ensure that data protection regulations are non-conflicting, and that there is no need nor justification for the lowering of data protection standards.
- All stakeholders should recognise that the technical internet infrastructure is not an appropriate point for intervention on content-related issues. Addressing societal problems with purely technical solutions, including through interventions via the technical internet infrastructure, should be avoided.

## Introduction

CENTR is the association of European country code top-level domain registries (hereinafter ccTLDs). All EU member state and EEA country ccTLD registries (such as DENIC administering .de for Germany and NORID managing .no for Norway) are members of CENTR. Together, CENTR members are responsible for over 70% of all registered domain names worldwide.

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.

CENTR members are at the core of the public internet, safeguarding its resilience, stability and security. The majority of European ccTLD registries 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, law enforcement, data and consumer protection authorities, as well as governments).

Notably, ccTLD registries only hold information enabling users to navigate the internet but do not host, store, transmit or control any content online. This is not their expected role; domain name holders are primarily responsible for the use of the domain name and for any related services, such as websites associated with the domain name.

CENTR welcomes the opportunity to participate in the preparatory phase for the Global Digital Compact. As a key member of the European technical community, CENTR would like to outline the following key areas for maintaining an “open, free and secure digital future for all”.

## Connect all people to the internet, including schools

### a) Core principles

The Domain Name System (DNS) is integral to the functioning of the internet. It performs the essential task of translating IP addresses to human-readable domain names that are used by all connected devices and online services (browsers, e-mail exchanges, streaming services, smartphones and laptops), as well as more invisible infrastructure roles that the internet relies on.

The DNS is a flexible, resilient and scalable infrastructure. It is not linked to a particular device (e.g., an IP address might change, but the domain name remains the same), and ensures reliability via decentralisation and built-in redundancy (i.e., if one server is unreachable, several alternatives can be queried). The DNS is built to withstand heavy workloads, and its underlying technical components have been refined and optimised for over 40 years.

The Global Digital Compact should take into consideration the importance of essential technical infrastructure, such as the DNS, for the stability, resilience and security of the internet.

A domain name is also crucial for establishing one’s identity online, as well as being the foundational piece of infrastructure on which to build a business, develop a product or offer an e-government service.

European ccTLDs invest greatly in ensuring that domain names are accessible, at a reasonable cost. The domain name registration process is globally organised as per the “first come, first served” principle, which allows domains to be accessible to all internet users without discrimination. Recent regulation in the intellectual property (IP) space has sought to subvert this principle, by disproportionately privileging certain groups (e.g., via alert systems for IP rightsholders) over other legitimate beneficiaries. The imbalances introduced by such attempts erode the trust that users have in the DNS and their ability to participate fully on the internet. Furthermore, such imbalances may be disruptive for the competitiveness of smaller national infrastructure actors that are faced with more stringent legal requirements, as opposed to bigger global actors.

Hence, to ensure balanced and evidence-based policymaking, which takes into account the technical reality and potential impacts on the accessibility of essential digital infrastructure, such as the DNS, CENTR strongly encourages greater dialogue between policy-makers and the technical internet infrastructure community.

The Global Digital Compact should strongly emphasise that universal access to essential infrastructure, such as domain names, is the central tenet of a free, inclusive and open internet.

It is well-established in global internet governance that differences are allowed between the policy arrangements of ccTLDs and gTLDs, and amongst ccTLDs, in particular, informed by national particularities or needs. This model shows that digital autonomy and global interoperability are not mutually exclusive. Bridging these accepted differences, ccTLD registries voluntarily share their experiences amongst peers in different fora - including ICANN, CENTR or Regional Internet Registries (e.g., RIPE NCC) - to contribute to overall online safety.

CENTR members support their local communities' digital presence and connectivity. Some notable examples cover responses to the Covid-19 pandemic and education programmes for marginalised communities.

At the beginning of the Covid pandemic, an initiative co-founded by DNS Belgium, the registry behind .be, [provided young people with 12.000 refurbished laptops](#), to facilitate home-schooling and bridge digital divides. In addition to this, NOMINET, who runs the .uk ccTLD, invests in [sustainable data poverty initiatives](#) to make internet access free for people on very low incomes. CIRA, the registry administering .ca, awards grants to [fund locally-led connectivity initiatives](#) in rural, Northern and Indigenous communities in Canada, in support of innovative solutions to overcome natural hurdles to infrastructure. In their [Digital Town Awards](#), the .ie Domain Registry similarly rewards digital achievements within local communities. The Portuguese registry, .pt, has set up the '[Rampa Digital](#)' training and digital literacy programme, aimed at accelerating economic recovery through digital technology, training and mentoring for SMEs, with a differentiated focus on marginalised individuals. Similarly, SK-NIC, who runs .sk, funds many projects which foster digital inclusion, such as [a recent initiative supporting digital literacy among children with disabilities](#), via a custom-made app. CZ.NIC, the registry administering .cz, is one of four organisations that run the [Safer Internet Centre of the Czech Republic](#), an education and prevention centre to make the internet safer for children and young people, as well as their guardians. The registry responsible for .me also leads digital literacy campaigns for children and young people, such as [programming competitions](#). EURid, who runs .eu, likewise supports digital literacy programmes in collaboration with schools and universities.

## b) Key commitments

- Governments should prioritise balanced and evidence-based policymaking in the digital area, being mindful of its impact on the accessibility of essential digital infrastructure, such as the DNS.
- Governments should refrain from introducing unnecessary and disproportionate barriers to the domain name registration process via national and international legislation, in the interest of ensuring a level-playing field for all infrastructure actors, irrespective of their size.
- The technical community shall continue exchanging good practices of abuse mitigation within their technical remit in order to contribute to overall safety online.
- Technical infrastructure actors, such as ccTLDs, support, where necessary, their local communities' digital presence and education, through information sharing and outreach programmes.

## Avoid internet fragmentation

### a) Core principles

In order to have a meaningful conversation on the avoidance of internet fragmentation, the challenge of defining what it means must first be overcome. CENTR expects that the Global Digital Compact will build on prior work in differentiating between various manifestations of internet fragmentation, foremost the recent [framework](#) developed by the Internet Governance Forum's Policy Network on Internet Fragmentation. As guardians of the technical internet infrastructure, CENTR members would like to emphasise the difference between two areas of internet fragmentation.

First, fragmentation in the internet's technical layer should be avoided. At present, the technical underpinnings of the internet remain global and uniform. However, as soon as there is interference in the technical stack, including the DNS, interoperability of the free and open internet is jeopardised. The Global Digital Compact should emphasise deference to multistakeholder internet governance processes, designed to avoid fragmentation of the DNS at a technical level.

Second, legislative interventions in the operation of the DNS may result in unwanted consequences, such as conflicts between policies and standards set by the global internet governance community and national legislation. In doing so, fragmentation emerges in terms of conflicting legal requirements which technical operators, such as TLD registries, must adhere to. Even well-intentioned legislative interventions in (supra-) national jurisdictions may undermine global voluntary commitments and create technical conflicts (e.g., [recent legislative efforts on Geographical Indicators in the EU](#), and the [Sony v Quad9 case](#)). Therefore, the Global Digital Compact should stress the need for national legislation to carefully assess the level of its interference with voluntary protocols and standards, by making sure that the technical community's expertise and feedback is dutifully taken into consideration when new legislation is drafted and negotiated.

The Global Digital Compact must acknowledge the role of the multistakeholder model in developing global internet infrastructure. CENTR expects the Global Digital Compact to maintain and strengthen respect towards the key principles of the free and open internet, which are also at the core of global internet governance and prevent fragmentation. The core principles underpinning the technical and operational stability of the internet include interoperability, common open standards and protocols. Respect for these principles by all stakeholders, from governments to businesses, is quintessential. The coexistence of two parallel streams of governance, at the national/regional and multistakeholder levels, should be avoided at all costs, where these core principles are concerned. The Global Digital Compact should therefore support the multistakeholder fora in which the core principles of the free and open internet are negotiated (e.g., IETF, ICANN).

At the same time, regional and national particularities are already reflected in the way national ccTLDs are operating and setting their terms and conditions. While ccTLDs operate based on global standards at a technical level, they set their own policies and procedures according to national rules and needs. ccTLDs participate in regional organisations, such as CENTR for Europe, to promote and participate in the development of a high standard of ccTLD management for the benefit of their local internet community and the global internet.

CENTR members are committed to maintaining the resilience, stability and security of the DNS infrastructure via national initiatives, such as [PTSOC](#), which serves as the Portuguese national cybersecurity cooperation forum between .pt, governmental authorities and the user community. Further, to deepen and expand European ccTLDs' long-established collaboration in the security field, CENTR acts as an Information Sharing and Analysis Centre (ISAC), by creating a secure environment for exchanging security-related information, data and collaboration on good practices. In the face of cybersecurity threats, ccTLD registries have adopted a variety of practices, which reflect that uniformity is not necessary, and that there is strength in diversity. As a result, there is no single point of failure.

CENTR expects the Global Digital Compact to recognise different manifestations of internet fragmentation, and that differences between TLDs' policy arrangements are a feature, not a bug.

### **b) Key commitments**

- Policymakers must take into account the multistakeholder model when drafting national/international legislation concerning internet infrastructure, due to the global and universal nature of the internet.
- All stakeholders should support and respect the multistakeholder governance of the DNS, which facilitates the development of common open standards and protocols supporting global interoperability (e.g., the development of standards in the IETF).
- ccTLD registries should be able to adopt policies and procedures which meet local needs, while safeguarding the common technical core of the DNS. Diverging policies do not automatically equate to fragmentation, when the technical underpinnings remain universal and interoperable.
- CENTR members continue their collaboration efforts to strengthen cybersecurity and contribute to the resilience, safety and stability of the DNS infrastructure.

## **Protect data**

### **a) Core principles**

ccTLD registries maintain a domain name registration database. This database contains the contact information of domain name holders, as well as technical and administrative data that is necessary to provide DNS services. 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). Access to registration data is inter alia governed by relevant data protection and information security rules, as per national and regional legislation.

Even before the conception of the EU GDPR, European ccTLDs had developed best practices to adhere to data protection principles, such as the use of clear and transparent policies, as well as data minimisation, to guarantee that only data that is strictly necessary for the performance of their essential functions is collected and processed.

CENTR members are committed to protecting domain name holders' data. There is high demand for accessing domain owners' personal or financial information, primarily for law enforcement purposes. Access requests for

domain name holders' registration data must be rooted in clear legal bases and respect due process. There is no need nor justification for lowering data protection standards for domain name registration data.

A clear example is the above-mentioned data minimisation. In general, the DNS requires no personal data to function. For administrative purposes (e.g. invoicing) a minimal dataset is maintained for these specific contractual purposes. Demands for the collection of more personal data do not only breach the principle of data minimisation, but also enlarge the risk of data breaches.

CENTR expects the Global Digital Compact to support the establishment of a global consensus on minimum data protection standards, applicable to internet infrastructure operators, such as TLD registries, to support universal respect for the right to privacy, while balancing the needs to access domain name registration data for reasons of public interest, based on due process.

### **b) Key commitments**

- All actors agree that there is no need nor justification for the lowering of data protection standards as they relate to domain name registration and the provision of the technical infrastructure.
- Given the cross-border nature of the technical infrastructure, governments should strive for global consensus on minimum data protection standards applicable to internet infrastructure actors, balancing the need to respect the right to privacy and supporting the rule of law.
- The technical community and industry actors shall respect and be mindful of data protection in the context of the provision of the essential technical infrastructure. Clear and transparent public policies must be set out on the purposes of data collection and use.
- CENTR members are committed to a high standard of protection for domain name holders' data and other legitimate rights within their technical remit, and legal requirements applicable to them.

## Apply human rights online

### **a) Core principles**

The Global Digital Compact should commit to the protection of the free and open internet, as a facilitator for the exercise of human rights.

In the past years, CENTR members have observed a trend for governments to push for intervention on illegal and harmful content via the internet infrastructure. However, societal problems and the technical internet infrastructure should be strictly separated. Anything else constitutes a threat to exercising one's human rights online (e.g. freedom of expression or fair trial/due process), as intervention on content via the DNS is inherently disproportionate as well as fundamentally misunderstanding its role as technical infrastructure.

First, DNS actors have no insight into or control over the content associated with the domains they register, but rather fulfil a purely technical, administrative function. Misconceptions of how the technical internet infrastructure works create unrealistic expectations on the part of policy-makers, which, in turn, creates a disconnect between legal rule and technical reality that may threaten respect for human rights.

Second, intervention via the DNS layer is a ‘nuclear’ option, given that illegal content cannot be surgically removed (as with an edit to a web page or deletion of an individual Tweet, for example). Rather, interventions at the DNS level remove entire domains, with a significant risk of collateral damage for access to legal content or unrelated services, such as e-mail services using the respective domain name. Such interventions are also inherently ineffective, as the DNS is an addressing system at its core; the illegal content is not deleted by deregistering an associated domain. Intervention on illegal content at infrastructure level can only be reserved for exceptional circumstances, following a clear legal basis and after an adequate assessment by the competent public authorities. In this context, CENTR members are committed to safeguarding internet users’ human rights by insisting on due process and transparency, when approached for content interventions.

Nevertheless, European ccTLD registries are committed to ensuring a high level of trust for all internet users when navigating to domain names within their respective TLD zones. European ccTLD registries have consistently been recognised as operators of TLD zones with the [least amount of abuse](#). This is done through a variety of different practices and policies, rooted within national context and consumer protection law regimes, among others. For example, there are a variety of registration [data accuracy practices](#) adopted by European ccTLD registries, that allow registries to take action (including suspending a domain name) based on inaccurate registration data, keeping registry action to its technical remit and information available to them. The crux of the strength of the European ccTLD space is diversity in data accuracy approaches. It allows flexibility and adaptability of national context, business model and regulatory needs.

The Global Digital Compact should insist that public authorities follow the rule of law, rooted in democratic process, when addressing illegal content and other forms of abuse online. Addressing societal problems with purely technical solutions, including through interventions via the technical internet infrastructure should be avoided.

Considering the inherent global nature of the internet, the Global Digital Compact should encourage inter alia the review of existing international multilateral mutual assistance agreements, as well as the efficiency of current processes available to law enforcement authorities for fulfilling their role efficiently within due process requirements.

## **b) Key commitments**

- All stakeholders should acknowledge that the technical internet infrastructure is not an appropriate point for intervention on content-related issues.
- All stakeholders should recognise, in addition, that intervention on content at the DNS layer is as ineffective as it is disproportionate. Human rights are jeopardised, if interventions in internet infrastructure threaten the free and open internet.
- ccTLD registries are not in the position to remove content. Any content-related intervention at the domain name level needs to be accompanied by a clear legal basis and assessment by competent authorities.
- CENTR members shall safeguard human rights by insisting on the tenets of the rule of law, transparency and due process.