



# Towards a Stronger Internet

## Principles for the Next Digital Decade

### Setting the scene

The year ahead will be a big year in EU digital policy, as 2024 will give EU policymakers the chance to set legislative priorities for the coming 5 years. It is clear that EU policymakers have ambitious goals, as demonstrated by long-term initiatives such as [Web 4.0 and virtual worlds](#), the [Declaration for the Future of the Internet](#), [Europe's Digital Decade](#), and the [Declaration on Digital Rights and Principles](#).

With these ambitions in mind **CENTR, the association of European country code top-level domain (ccTLD) registries, proposes principles to safeguard Europe's digital future in the upcoming decade.**

The Principles for the Next Digital Decade proposed by CENTR draw upon the experience of key internet infrastructure actors, such as European country code top-level domain registries (ccTLDs).

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. It provides a navigation function to map user-friendly domain names to numeric Internet Protocol (IP) addresses and is equally used by any service running on the internet, either visible to the end-users (e.g., website, email) or entirely behind the scenes (e.g., instant messaging, Voice over IP, and infrastructure management).

### About CENTR

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. We currently count 51 full and 8 associate members – together, they are responsible for over 80% of all registered domain names worldwide. Our objectives are to promote and participate in the development of high standards and best practices among ccTLD registries.

European ccTLD registries and other technical internet infrastructure actors can provide a wealth of experience and knowledge for policymakers, stemming from decades of providing internet services for the public benefit.

More and more, however, these technical actors are taken for granted in EU legislation and digital policy, even when internet infrastructure is explicitly in focus. Some legislation (unintentionally) interferes with technical infrastructure actors' ability to perform their essential services for digital society. While the DNS and Internet Protocol are resilient, the next generation of EU policymakers must nevertheless take a holistic view of the internet across all its layers and contribute to the strengthening of the overall global digital ecosystem.

In EU digital policy, there is a pressing need for awareness of technical standards and protocols which form the backbone of the internet and on which the future must be built. Without this strong and resilient core that has allowed the internet to grow and become an essential part of society, the future of the internet is uncertain.

While imagining and building the future internet, and in the context of the new legislative term, EU policymakers must seize the chance to commit to maintaining the core elements of the free and open internet. This is what has allowed and will allow information society to develop and continue bringing the benefits of a connected world. To this end, CENTR offers the following set of principles to guide policymakers in the next EU legislative term.

## What is Web 4.0?

Web 4.0 is the expected next generation of the World Wide Web, based on the advanced use of artificial intelligence, the internet of things, virtual worlds, and extended reality capabilities. It is expected that user-experience within Web 4.0 will be more collaborative and interactive, while digital and physical environments will become more merged and intertwined.



# Interoperability

EU policymakers must formally recognise open standards developed in the international internet standard setting processes, and, where possible, promote their uptake via public procurement to support a free Next Generation Internet which is open for citizens and businesses alike.

The Next Generation Internet must continue to be based on open standards. The internet's success and scalability has only been possible due to open standards that are publicly available and are developed via transparent processes open to broad participation. They enable interoperability, compatibility between different services, and promote user choice.

To strengthen the support for open standards, governments must formally recognise open standards as a viable option in their jurisdictions when the development of new technology is discussed. All stakeholders, including the public sector, should participate in the development of open standards.

At EU and Member States level, public procurement should support and encourage solutions based on open standards. This allows for further competition on the market and ensures users' choice and the avoidance of vendor lock-in, all crucial for the development of the Next Generation Internet, including Web 4.0.

The Next Generation Internet and Web 4.0 stand on the shoulders of existing critical internet infrastructure, such as the Domain Name System, the Internet Protocol suite, and other standards and protocols developed and maintained within existing international standard-setting bodies based on the multistakeholder model. The Next Generation Internet and Web 4.0 must ensure its compatibility and interoperability with existing foundational pieces of essential internet infrastructure that have proven their ability to sustain a scalable internet through its many development stages. In order to maintain the internet's openness and ability to evolve further without excluding anyone, interoperability with existing internet infrastructure is a must.



# ● ● ● ● ● ● ● Competition


**EU policymakers should remain technologically neutral in legislation affecting the internet infrastructure, while creating a level playing field by insisting on the use of open standards.**

Decentralisation, understood as distributed operational responsibilities within a system, must be at the core of the Next Generation Internet and a future Web 4.0 and within such a decentralised system, a diversity of actors should be encouraged as a central feature.

Diverse, decentralised systems ensure that there is no single point of failure – actors compete for solutions and thereby strengthen the network's overall resilience. Knowledge and power are distributed, not concentrated, increasing consumer welfare and choice. Shared open standards underpinning decentralisation can facilitate interoperability and create room for innovation.

The change of ownership and, as a result, the changes in usability and content moderation policies in major social media platforms have demonstrated the limitations and risks of centralised models, where end-user experience and reliance on these platforms is not taken into consideration in business decisions. The emergence of federated social media platforms or the decentralised DNS and the diversity of European ccTLD registries could serve as design examples that should be promoted and taken as inspiration for the Next Generation Internet.

EU policymakers should refrain from harmonising beyond the baseline of open standards: legislation should be technologically neutral to ensure it is future-proof and promotes competition.



# Access & Cybersecurity ● ● ● ● ● ● ●

## Access

**EU policymakers should remove and prevent any friction in future legislation that would hamper easy access to European digital identifiers, including domain names.**

Europe needs a regulatory environment that allows for competitive, reliable, and secure access to online identifiers such as domain names for both European citizens and businesses. Regulatory initiatives should not disproportionately impact the ease of access to these online identifiers. Anything that would disproportionately affect European identifiers would push EU citizens to less regulated and less secure environments. This consideration should be a standard part of any impact assessment.

More and more European citizens and businesses rely on US-owned social media platforms to establish their online identity. European ccTLDs are a preferable alternative as they give the user control over their identity and are subject to local policy with European values at the core. The EU should encourage sharing best practices across industries and with other regions.

## Cybersecurity

**EU policymakers should support collaboration in the area of cybersecurity, based on sharing existing good practices established across internet infrastructure.**

The EU should continue to support collaboration in the area of cybersecurity, working towards the objectives outlined in the Digital Decade Programme 2030. There is no cyber resilience without pulling together the know-how of all parties involved and fostering private-public endeavours where possible.

European ccTLDs have built up decades of experience in securely managing digital identifiers while safeguarding data protection principles (such as data minimisation) and insisting on respect for human rights (such as due process). European ccTLDs are available to share that experience.

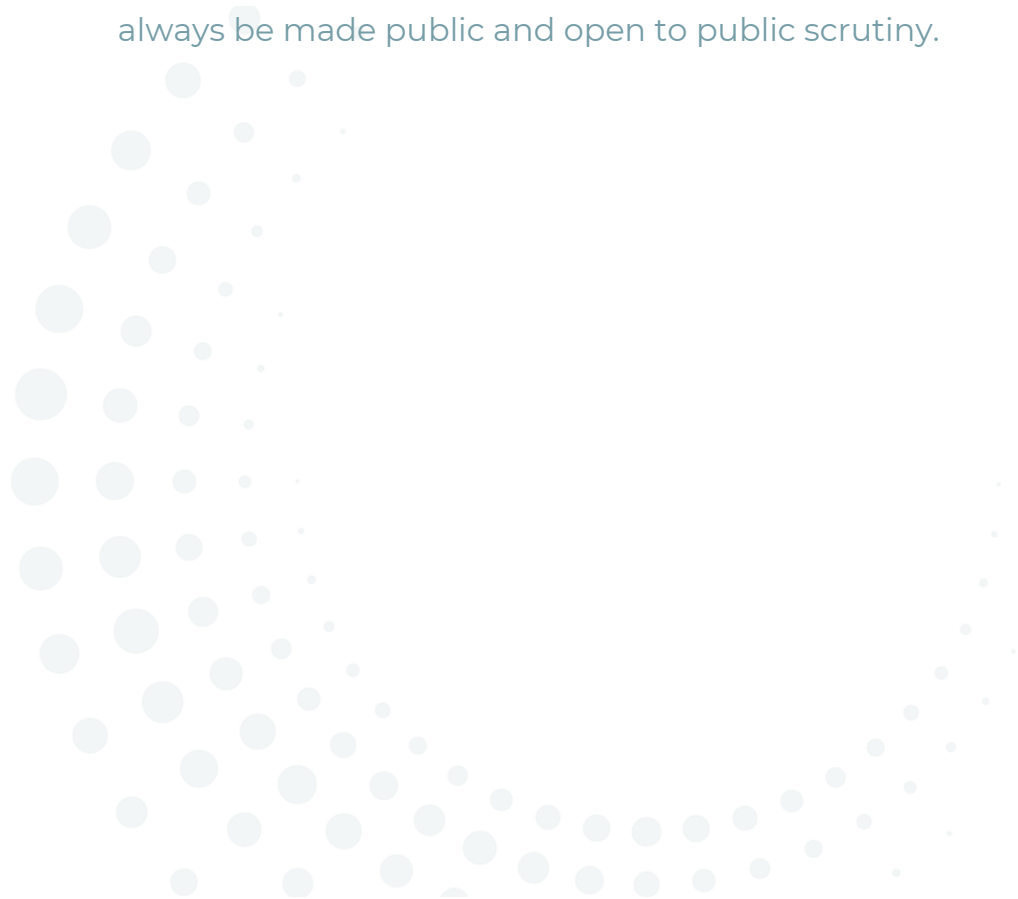
# Fundamental Rights

## Human Rights

When new legislation is discussed and considered, EU policymakers should make human rights impact assessments public without exception, to ensure transparency in the face of public scrutiny.

The free and open internet fosters the protection of human rights. While states, and by extension the EU, bear the ultimate responsibility for compliance with human rights laws, a shared responsibility applies to a broad spectrum of both public and private actors when it comes to ensuring the protection of those rights in the online space. The multistakeholder model offers solutions for mutual accountability, and decision-making must be guided by the tenets of the rule of law, due process, and transparency of decision-making.

The EU's approach to the Next Generation Internet and Web 4.0 should ensure that policy initiatives which impact human rights online are considered through a multistakeholder lens, to assess technical feasibility of proposed measures and legislative interventions. Furthermore, human rights impact assessments should always be made public and open to public scrutiny.





# Fundamental Rights


## Privacy and Data Protection

**EU policymakers must uphold and adhere to high data protection standards.**

New legislation must not weaken existing data protection principles under the relevant Union-level acquis, or conflict with it. Strong data protection safeguards are strictly necessary in a democratic society.

Consistent enforcement of existing data protection standards should be strengthened, and privacy-enhancing approaches should be encouraged, beginning in the product design stage. Critiques stating that privacy-enhancing and data protection requirements hamper innovation and societally beneficial progress should be met with the already existing legal grounds in the Union's data protection law, e.g., informed consent to data processing or warrants for law enforcement agencies.

Technological infringement on data protection and privacy should not be treated as silver bullets for solving societal problems and pretences of public safety. The security of EU citizens and their ability to control their own personal data should always be prioritised over the interests of the commercial players in a data-driven economy.



# Online Content ● ● ● ● ● ● ●

European legislators must respect the principles of due process and proportionality in any future legislation that deals with removal or blocking of online content.

European legislators should abstain from legislative interventions without a comprehensive and publicly available evidential basis.

Online content related problems need to be addressed at the level where they can be dealt with most effectively while respecting fundamental rights. Illegal content is made available, published, and hosted on the internet with the involvement of several parties (e.g., content publisher, website owner, domain name holder) and service providers (e.g., hosting provider, internet service provider, domain name registry), while making it inaccessible online can be performed with different levels of interference and risks for collateral damage to end-users. This requires a collaborative cross-industry approach. Because of the potential impact on human rights of content removal at the infrastructure level (such as domain name suspension), each intervention must be respectful of due process, transparency and involve a competent public authority. European legislators must respect and adhere to those principles in any future legislation.

Respect for due process and involvement of public competent authorities when removal of online content is sought, as well as recognition of different levels of intervention at infrastructure level (such as deletion of domain names as a measure of last resort), has resulted in Europe consistently leading the charts of low DNS abuse, and effective consumer protection.

European internet infrastructure has proven to be reliable and secure. European ccTLDs have been extremely successful in serving their communities compared to other regions. Some legislation directly or indirectly refers to intervention at internet infrastructure level as a solution to a range of societal problems. Side effects of such legislation could have structural ramifications for the infrastructure's stability. In order to charter possible side effects, it is essential that legislative impact assessments address this area specifically. Studies that accompany impact assessments of proposed legislation targeting removal or blocking of online content should be public without exception.



# Governance

The EU must ensure continuous support for the evolving multistakeholder model by actively participating in and insisting on its relevance for the Next Generation Internet.

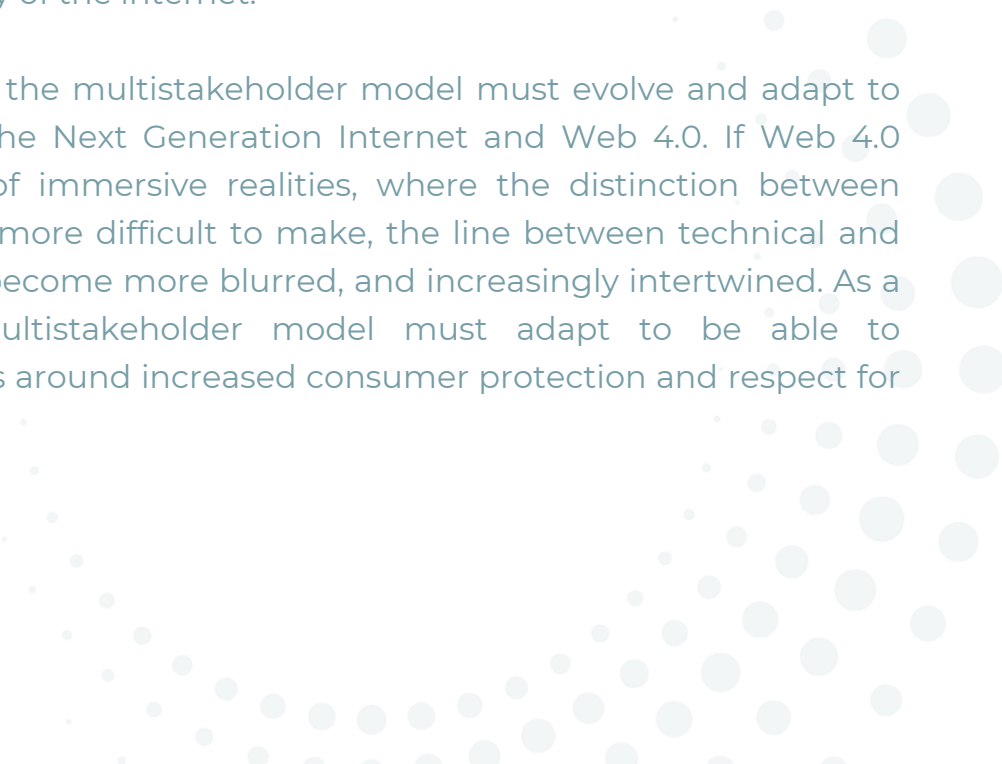
There is no future of the open and free internet without all stakeholders' continuous support for the internet's multistakeholder model.

The multistakeholder model is fit for purpose to maintain the foundational pieces of the internet to continue delivering stable, resilient, and secure internet infrastructure, including for its future development. However, the model relies on continuous support of all stakeholders, with allocating enough resources for its continuous evolution to respond to new challenges.

These resources include allocating experts, ensuring wide participation of stakeholders with different backgrounds, and taking a collective responsibility for its effectiveness as a result. The success of the multistakeholder model relies solely on its support from all stakeholders, including governments.

Duplicating internet governance efforts, either via national or regional legislation or through other multilateral fora risks creating technical fragmentation and weakening the universality of the internet.

Just as the internet itself, the multistakeholder model must evolve and adapt to meet the challenges of the Next Generation Internet and Web 4.0. If Web 4.0 assumes characteristics of immersive realities, where the distinction between online and offline will be more difficult to make, the line between technical and non-technical issues will become more blurred, and increasingly intertwined. As a result, the internet's multistakeholder model must adapt to be able to accommodate discussions around increased consumer protection and respect for fundamental rights.



# More about CENTR

## Objectives

*To promote and participate in the development of high standards and best practices among ccTLD registries.*

## Mission

*CENTR is the association that brings together the community of mainly European country code top level domain operators (ccTLDs). CENTR strives to facilitate collaboration, to promote its members' interests, and to be the centre of intelligence in order to assure world-class ccTLDs, resulting in a better internet for all.*

## Vision

*CENTR is to be recognised as an outstanding association, providing essential services for its community: enabling collaboration and the trusted exchange of information, acting as the voice of European ccTLDs, and shaping the DNS ecosystem in a sustainable, safe and secure manner to maintain an open, reliable and inclusive internet infrastructure.*

Our members are responsible for over **80% of all registered domain names** worldwide

### 51 Full members

.ac .ad .af .am .at .ba .be  
.bg .bv .ca .ch .cy .cz .de .dk .ee  
.es .eu .fi .fo .fr .ge .gg .gi .gr .hr  
.hu .ie .il .im .io .is .it .je .lt .li .lu .lv  
.pm .me .mk .mt .nl .no .pl .ps  
.pt .ro .rs .se .sh .si .sj .sk .tr .ua  
.uk .va

### 8 Associate members

.au .biz .cat .cc .com .jp .net  
.nz .org .tv .us .saarland



[www.centr.org](http://www.centr.org)



CENTR



@CENTRnews