Connecting European dots

CENTR Simplification Checklist

Introduction

The European Commission's simplification agenda aims to reduce administrative burden for EU businesses, with a special focus on SMEs. Namely, the European Commission's recent initiatives, such as the Digital Omnibus, amend the EU digital acquis to streamline compliance costs and clarify legislative interplays.

The simplification efforts could, however, benefit from additional targets that would alleviate the regulatory burden for European digital infrastructure actors without compromising cybersecurity, data or consumer protection. With these ambitions in mind, CENTR, the association of European country code top-level domain (ccTLD) registries, proposes a "simplification checklist", as practical guidance to EU policymakers. The simplification checklist highlights additional simplification targets, from cybersecurity to consumer protection, that could ease or avoid unnecessary compliance burden for European ccTLDs, without calls for deregulation. With simplified rules and saved resources, the checklist would strengthen the European digital space and bolster its competitiveness.

European ccTLDs play a critical role in the internet ecosystem by maintaining part of the Domain Name System (DNS) infrastructure, necessary for most digital services offered to individuals and businesses alike. The DNS is a well-established network protocol at the heart of the internet infrastructure. It maps user-friendly domain names to numeric Internet Protocol (IP) addresses and is used by any service running on the internet, whether visible to end-users (e.g., website, email) or entirely behind the scenes (e.g., instant messaging, Voice over IP, and infrastructure management). European ccTLDs operate globally critical internet infrastructure that directly benefits the European digital economy and have consistently demonstrated their commitment to ensuring a secure cyberspace and high levels of consumer and data protection within their technical remit.

Over the past years, legislative attention has increasingly involved European ccTLDs, often without appropriate consideration of their core technical mission. EU regulation increasingly relies on positioning ccTLDs as “general-purpose” enforcement actors, and instrumentalises their unique position within the internet infrastructure. Without proper consultation and involvement of the ccTLD community, such enforcement measures can have significant structural ramifications for the DNS infrastructure to the detriment of individuals, businesses and the broader internet ecosystem.

In addition, as a result of increased legislative attention, European ccTLDs fall under multiple, sometimes overlapping, legislative obligations and an increasingly complex compliance landscape. This applies similarly to both EU and non-EU ccTLDs. While individually the obligations imposed on ccTLDs in the respective legislative tools focus on acute issues, taken together, they create an unnecessary burden without certainty that they will improve cybersecurity or consumer protection online, as intended by the European Commission.

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 affect access to European domain space. Anything that disproportionately affects European identifiers could push EU citizens into less regulated and less secure environments, inadvertently weakening consumer and data protection available for European citizens and businesses.

EU policymakers must seize this simplification opportunity to benefit critical and essential internet infrastructure operators.

Simplification checklist

To guide EU policymakers in this endeavour, CENTR suggests the following simplification targets when revising the existing digital acquis, and considering any additional legislation:

☐ **Cybersecurity**	EU policymakers must ensure a single auditing framework, harmonised reporting timelines, and national single-entry points for essential digital infrastructure. Harmonisation should not shorten existing reporting deadlines.
☐ **Consumer protection**	EU policymakers must streamline powers available to consumer protection authorities across legislative areas and avoid overlapping legislation. Orders to delete domain names in the interest of greater consumer protection must remain the measure of last resort.
☐ **Data protection**	EU policymakers must maintain high data protection standards for all data subjects, regardless of technological developments, trends, and industries. EU ccTLDs should not be required to collect or retain more personal data than needed to provide technical services.
☐ **Access to business registers and eID**	EU policymakers must ensure free and open access to EU business registers' data and the EU Digital Wallet ecosystem for all parties with legitimate interest in order to facilitate compliance with EU legislation.
☐ **Role of a registry**	EU policymakers must safeguard ccTLDs' ability to perform their essential services for the digital society and avoid unnecessary and disproportionate interference with their technical function.
☐ **Better Regulation**	EU policymakers must ensure that any impact on or involvement of ccTLDs in regulatory discussions is accompanied by a proper impact assessment addressing the impact on the internet's essential infrastructure and any unintended consequences for users and the global DNS ecosystem. ccTLDs must be meaningfully consulted and involved in preparing impact assessments.

Cybersecurity

EU policymakers must ensure a single auditing framework, harmonised reporting timelines, and national single-entry points for essential digital infrastructure. Harmonisation should not shorten existing reporting deadlines.

Supervisory frameworks

The NIS 2 Directive is the primary cybersecurity legislation relevant for the security and stability of ccTLD technical operations. Under the ex-ante supervisory regime of the NIS 2 Directive, competent authorities can subject essential entities, such as ccTLDs, to regular audits, ad hoc audits following a significant incident, as well as additional security scans.

In the context of cybersecurity oversight frameworks applicable to digital infrastructure, several EU regulations prescribe rules that are not always aligned. As a result, an essential entity may be subject to overlapping supervisory frameworks that seek to establish compliance with the same or similar obligations. For example, the Digital Operational Resilience Act (DORA) and the European Digital Identity (EUDI) Regulation may subject European ccTLDs to overlapping supervisory activities.

To simplify and promote the uptake of new business opportunities across sectors, the cybersecurity oversight framework should be service-based, rather than operator-specific. Where services overlap or are covered by existing EU or national audits, operators should be able to demonstrate conformity with additional requirements by recognising existing audit results as valid. The Critical Entities Resilience (CER) Directive sets a positive precedent by recognising that the NIS 2 Directive already imposes extensive cybersecurity requirements on a wide range of entities. As a result, ccTLDs are exempt from the CER Directive's incident reporting and audit provisions. The European Commission should adopt a similar approach in any EU legislation containing cybersecurity elements, and clearly exempt ccTLDs from overlapping cybersecurity supervisory frameworks under DORA and the EUDI Regulation.

Reporting obligations

ccTLDs are subject to different EU regulations on reporting cybersecurity incidents and data breaches. However, reports must be submitted through separate tools and follow different timelines, with no account for potential overlap. Double reporting adds an extra burden for operators and creates informational silos for competent authorities. A single secure reporting interface at the national level would simplify reporting procedures, as information would need to be submitted once. The European Commission should work with Member States to facilitate the development of a single, secure reporting interface at the national level, tailored to each Member State, and support cross-authority cooperation and information exchange.

Aligning reporting timelines could reduce the reporting burden for non-profit organisations and SMEs, while increasing legal clarity for essential digital infrastructure. Reporting timelines across different legislation should be reviewed and aligned as much as possible. Where existing reporting timelines differ, alignment should be achieved by extending the shorter deadlines, ensuring operators retain sufficient and reasonable time to comply with their reporting obligations.

Consumer protection

EU policymakers must streamline powers available to consumer protection authorities across legislative areas. Orders to delete domain names in the interest of greater consumer protection must remain the measure of last resort.

The Consumer Protection Cooperation (CPC) Regulation is horizontal EU legislation that harmonises enforcement coordination between EU authorities across multiple consumer protection areas. It includes a list of powers available to consumer protection authorities to protect collective interests of consumers and, where appropriate, to order ccTLDs and registrars to delete domain names of infringing businesses, as a measure of last resort.

Recent EU financial regulation (e.g., MiCA, FiDA and PSR Regulation) includes a standard domain-deletion clause reserved for supervisory authorities in the financial sector to deal with non-compliant financial services, justified as protecting consumers. However, in the financial area, the power to delete domain names creates unnecessary duplication and legal uncertainty for supervisory authorities, affected businesses and ccTLDs.

EU policymakers must ensure that the CPC Regulation remains the primary legal framework for cross-border consumer protection enforcement across legislative areas, including financial regulation. Before granting additional consumer protection powers, such as a power to order deletion of domain names, to authorities outside the CPC competence, the European Commission must conduct a thorough impact assessment. This should include the impact on ccTLD operations in both the EU and globally.

Additionally, powers to delete domain names available to authorities refer to a very specific technical action that allows for instant re-registration of a domain name. This is why the CPC Regulation gives the authority the power to delete and then register the domain name to prevent the same or other malicious actors from re-registering it. However, registries and registrars also have other technical actions to disrupt and mitigate abusive activity, such as suspension, blocking, or transfer. When enforcement powers at the domain-name level carry over to other legislation, early consultation with ccTLDs can avoid unnecessary mishaps and respect ccTLD technical capabilities.

In any case, deleting or suspending a domain name is a drastic measure. It can be equally painful for both the affected business and its customers. If a domain name is deleted, all associated services become unavailable, whether a platform, online bank application, website, or communication services connected to it, including emails and live chats. Deleting or suspending a domain name does not remove unwanted content from the internet, as it can be moved and duplicated in other TLDs or digital services. Due to the risk of collateral damage to digital infrastructure and consumer rights, any enforcement action involving domain takedowns must undergo a proportionality assessment. Domain takedowns should be considered a measure of last resort, in line with the proportionality principle already codified in the CPC Regulation. Considering domain takedowns as a measure of last resort does not preclude registries from pursuing voluntary cooperation mechanisms with public competent authorities.

Data protection

EU policymakers must maintain high data protection standards for all data subjects, regardless of technological developments, trends, and industries. EU ccTLDs should not be required to collect or retain more personal data than needed to provide technical services.

ccTLDs maintain a domain name registration database containing the technical and administrative data needed to provide DNS services. To assist end-users in navigating the internet, ccTLDs handle DNS queries that help deliver the correct IP address of an online resource to the user. Although the DNS infrastructure managed by ccTLDs is essential for resolving these requests, ccTLD registries cannot typically identify the individual users behind the DNS queries. The NIS 2 Directive requires ccTLDs and entities providing domain registration services to collect more personal information than a technical service requires, and to verify the identity and contact details of domain name holders. Different data retention regimes apply to European ccTLDs for business and law enforcement purposes.

Lowering data protection standards, by revising fundamental definitions and codifying certain circumstantial case law, as proposed in the Digital Omnibus proposal, will create more legal uncertainty. The current European data protection tradition, as enshrined in the GDPR, offers enough flexibility for good-faith actors and supports the development of privacy-enhancing technologies and standards, including in the DNS space (e.g., RFC 9076: DNS Privacy Considerations).

Instead, national data protection authorities and the European Data Protection Board (EDPB) should provide more meaningful guidance on interpreting key requirements, taking into account existing case law and changing industry and judicial practices. Guidance from national data protection authorities and the EDPB should include practical examples relevant for SMEs and technical operators across the internet infrastructure stack. It should also provide more direction on the identifiability of individuals, including the technical and legal means reasonably likely to be used to identify a natural person.

As the EU is discussing the need for an EU-wide data retention regime, lengthy data retention periods for all data categories cannot be justified for ccTLDs.

Retaining large amounts of data not required to deliver a technical service increases privacy and data protection risks for data subjects. Extensive and indiscriminate data retention for law enforcement purposes adds costs for the infrastructure, IT equipment, and human resources needed to ensure secure data storage and timely responses to law enforcement data access requests. As most European ccTLDs are non-profit organisations and SMEs, it is reasonable to minimise the additional costs associated with data retention for operators of essential technical infrastructure. Any data retention regimes for law enforcement purposes require additional effort from service providers, including ccTLDs, and must be proportionate to their technical role, size and business model.

Before introducing any fundamental changes to data protection standards, such as redefining personal data or mandating an EU-wide data retention regime, the European Commission must conduct a thorough and transparent impact assessment in line with Better Regulation rules.

Access to business data and electronic identification

EU policymakers must ensure free and open access to EU business registers' data and the EU Digital Wallet ecosystem to facilitate compliance with EU legislation.

The NIS 2 Directive requires TLD registries and registrars to collect and verify domain holder identity and contact information. To fulfil this obligation, European ccTLDs and registrars rely on several verification methods, including information available in national business registers.

However, access to legal entities' data in these national registers is often hidden behind paywalls and lacks easily available automated access. There is no justification for keeping information on EU legal entities behind unnecessary access restrictions, especially for entities with a legitimate interest in this information to fulfil their obligations under EU cybersecurity legislation.

EU policymakers should ensure open, free-of-charge, and automated access, including via an application programming interface (API), to information in EU business registers to facilitate seamless verification of identity and the legitimacy of businesses seeking to establish their online presence.

The EU Digital Identity Wallet (EUDIW) ecosystem could significantly support compliance with the domain holder identity verification obligation. In principle, natural and legal persons established in the EU will be able to use EUDIW to prove their identity, including for domain name registration purposes. During the domain name registration process, European ccTLDs rely on registrars as client-facing entities that facilitate domain purchases. Registrars typically offer multiple TLDs for sale and can be global companies, without EU establishment or presence. Under the current EUDIW framework, non-EU-established registrars are excluded from the opportunity to rely on the EUDIW ecosystem. This would put an unnecessary obstacle in the domain name verification process.

To rely on the EUDIW ecosystem for domain name holder verifications, ccTLD registries and registrars must register with the Member States' authorities at their place of establishment through a "cost-effective" process. While this process is yet to be implemented, any potential fees should be waived for European ccTLDs and other entities providing domain name registration services to facilitate compliance with the domain name verification obligations.

EU policymakers should ensure that the EUDIW ecosystem is free of charge and open to all ccTLDs and entities providing domain name registration services to facilitate their compliance with the NIS 2 Directive.

The role of a registry

EU policymakers should avoid turning the internet's infrastructure essential entities, such as ccTLDs, into general-purpose enforcement actors. EU policymakers must safeguard ccTLDs' ability to perform their essential services for the digital society and avoid unnecessary and disproportionate interference with their technical function.

EU regulatory trends show a proliferation of legislation, from agricultural policy to the financial sector, that directly references or attempts to interfere with the technical function of ccTLDs. Often, these interventions happen in trilogues and lack public evidence or debate on the need to include ccTLDs in the scope of regulatory interventions. Others fail to grasp the drastic nature of regulatory interventions involving domain takedowns of non-compliant businesses, or disregard existing rights-protection mechanisms already available to third parties (i.e., alternative dispute resolution procedures). Every EU regulatory area rediscovers the DNS and ccTLDs for their policy objectives, without understanding the underlying infrastructure, governance models, and industry needs. These discussions suffer from a lack of internal coordination and knowledge transfer within institutions. As a result, the regulation will fail to produce any tangible effect or meet its aims, whether that is strengthened consumer protection, intellectual property rights protection, or online safety.

ccTLDs are mostly non-profit organisations with public-interest missions. However, EU regulation often treats ccTLDs and their managed infrastructure as an "auxiliary" enforcement mechanism when other actors fail to act, and disregards their core mission: to keep the internet stable, secure, resilient, and available to all users at all times.

Some legislation refers to intervention at the internet infrastructure level as a solution to a range of societal problems. Such legislation could have structural ramifications for the infrastructure's stability while straining limited resources. To chart possible side effects, legislative impact assessments must address this area specifically.

Studies accompanying impact assessments of proposed legislation targeting the removal or blocking of domain names should be public and include broad consultation with European ccTLDs and the broader DNS ecosystem.

EU policymakers must ensure that any impact on or involvement of ccTLDs in regulatory discussions is accompanied by a proper impact assessment addressing the impact on the internet's essential infrastructure and any unintended consequences for users and the global DNS ecosystem. ccTLDs must be meaningfully consulted and involved in preparing impact assessments.

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.

CENTR has **51 Full members** and **10 Associate members**

Our members

Our members are responsible for **79% of all registered domain names** worldwide

www.centr.org CENTR secretariat@CENTR.org