August 2025 • *Brussels, Belgium*

CENTR Board statement on data retention for law enforcement purposes

Summary of CENTR key points

- In the context of the data retention debate, country code top-level domain (ccTLD) registries primarily collect a subcategory of subscriber data in order to identify specific domain holders. Any Domain Name System (DNS) 'traffic data' that is visible to ccTLD registries is insufficient to identify individual users.
- Before mandating any data retention regime applicable to EU ccTLDs, the European Commission must conduct a proper impact assessment of the feasibility and utility of retaining domain registration data for law enforcement purposes.
- Lengthy and indiscriminate data retention for law enforcement purposes leads to additional costs, including infrastructure, IT equipment and human resources necessary for ensuring a secure data storage and timely handling of law enforcement requests.
- In order to minimise the costs associated with any mandatory data retention incurred by EU ccTLDs, it would be advisable to establish a mandatory cost reimbursement mechanism across the EU.
- Voluntary cooperation mechanisms between service providers and law enforcement authorities, including with regard to sharing threat intelligence and non-personal data, should be actively promoted across the EU.

Introduction

CENTR is the association of European country code top-level domain registries (ccTLDs). All EU Member States and EEA country ccTLDs (such as .de for Germany and .no for Norway) are members of CENTR.

CENTR members are at the core of the public internet, safeguarding its stability and security. 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., end-users, CSIRTs, law enforcement and other competent authorities).

Domain names are the foundational pieces of internet infrastructure necessary for many online services (e.g., website, application, platform) to be accessible online. 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 considered the "phone book of the internet". It provides a navigation function to map user-friendly domain names to numeric IP addresses – whereas ccTLDs only hold information enabling users to navigate the internet without storing, transmitting or enhancing any content online.

ccTLD registries maintain a domain name registration database that contains technical and administrative data necessary to provide DNS services, as well as identity and contact information of domain name holders. Registration data can be queried by the general public using different protocols – as the web, WHOIS and RDAP – each offering their own unique controls to comply with the EU General Data Protection Regulation (GDPR)[1] and national data protection legislation.

As the technical operators of essential digital infrastructure[2] European ccTLDs invest significant effort in keeping their TLD zones safe and secure. As a result, European ccTLDs are consistently recognised as operators of TLD zones with the least amount of abuse.[3]

In the context of the ongoing call for evidence on the impact assessment on retention of data by service providers for criminal proceedings, CENTR members wish to highlight the following.

Registries and data retention

Data retention, in the context of law enforcement discussions, relates to the practice of time-limited storage of non-content data by service providers to ensure its availability for the prevention, detection and prosecution of criminal offences.[4] Among others, non-content data refers to: 1) 'subscriber data', such as information on the identity of the user of a service; and 2) 'traffic data', such as location data of the device used, date, time and duration of the communication and sender/receiver information. Both categories constitute personal data, and traffic data specifically may draw certain sensitive conclusions about individuals.

As ccTLD registries are not electronic communication service providers, the data category definitions found in EU legislation do not apply directly to the internet infrastructure operators. However, the e-Evidence Regulation on cross-border access includes ccTLD registries in its scope, since data held by domain registries can be particularly relevant for identifying the "actors behind malicious or compromised websites".[5]

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ('GDPR').
[2] TLD registries are considered "essential entities" according to the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union ('NIS 2 Directive').
[3] European Commission, "Study on Domain Name System (DNS) abuse", (2022).
[4] European Commission, Roadmap for lawful and effective access to data for law enforcement, (2025).
[5] Recital 28 of the Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings ('e-Evidence Regulation').

In the context of the data retention debate, ccTLD registries primarily collect a subcategory of subscriber data in order to fulfil their technical function and legal obligations. The limited 'traffic data' that is visible to ccTLD registries is insufficient to identify individual users.

TRAFFIC DATA

Article 3(11) of the e-Evidence Regulation defines 'traffic data' as "data generated or processed by an information system of the service provider", such as the source and destination of a communication, the location of the device, date, time, duration, and other electronic communications metadata concerning user access session to a service.

The EU Digital Services Act recognises the role of ccTLDs as a "technical auxiliary function" in the functioning of the internet.[6] To help end-users navigate the internet, ccTLD registries handle DNS queries that deliver the correct IP address of an online resource to the user. Although the DNS infrastructure managed by ccTLD registries is essential for resolving these requests, **ccTLD registries cannot identify the individual users behind the DNS queries**.

The DNS is set up as a hierarchical system. DNS resolution is a process of querying the DNS to convert a human-readable domain name into a machine-readable IP address. The resolution process starts at the top of the DNS hierarchy, at the root zone, and works its way through the TLD nameserver to the specific DNS server hosting the domain name in question.

TLD nameserver does not collect data that could be tied to a concrete device from which the query was initiated (e.g., IP address). The TLD nameserver only sees the request as coming from the DNS resolver that plays an intermediary role in resolving individual DNS queries. In addition, the DNS resolver typically caches the DNS records of the queries previously requested by other users relying on the same resolver. This means that not every DNS query even reaches the TLD registry nameserver, further diminishing the potential identifiability of the origin of the DNS queries.

Therefore, the relevance of retaining limited 'traffic data' visible to ccTLD registries for law enforcement purposes is marginal, as it cannot lead to a meaningful attribution in criminal investigations, nor identify "actors behind malicious or compromised websites".

SUBSCRIBER DATA

Article 3(9) of the e-Evidence Regulation defines subscriber data as "any data held by a service provider relating to the subscription to its services". The data covers the identity of the subscriber (i.e., name, contact details) and technical data related to interfaces used by or provided to the subscriber or customer at the moment of initial registration.

[6] Recital 28 of the Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services ('Digital Services Act').

As a part of the domain name registration process, ccTLD registries collect personal and non-personal data. Although no personal data is technically required for a domain to be accessible online, ccTLD registries collect the personal data of domain holders to fulfil legal obligations under European and national legislation.

The main EU legislation relevant to the collection of domain registration data is the NIS 2 Directive. Article 28 of the NIS 2 Directive obliges TLD name registries and entities providing domain name registration services (e.g., registrars) to collect and maintain accurate and complete domain name registration data, including the domain name, registration date, registrant name, email address, and telephone number.

The majority of European ccTLDs do not offer direct registration services to domain holders. Instead, domain names are purchased through registrars. After a purchase, the registrar is required to transfer certain domain registration data to the relevant registry. Consequently, for most ccTLDs, domain holders do not interact with the registries to acquire a domain name. Registries do not collect any additional data that could identify the domain holder at the time of registration, such as the IP address of their device, web browser information or session length. Therefore, **ccTLD registries collect limited data that can fall under the subcategory of subscriber data.**

CURRENT DATA RETENTION PRACTICES

Current registration data retention practices across European ccTLDs vary between Member States. The most common reasons for limiting data retention periods for EU ccTLDs are data minimisation and purpose limitation with regard to the personal data of domain holders. Certain Member States impose specific obligations on their national ccTLD to retain historical domain registration data for archiving and research purposes, while still applying the principles of data minimisation and purpose limitation. Different data retention regimes also apply to EU ccTLDs for business and law enforcement purposes. The context and legislative framework applicable to each EU ccTLD reflects the complexity and divergence of the data retention landscape in the EU.

Some minimum harmonisation efforts could help align law enforcement expectations and diverging data retention regimes applicable to EU ccTLDs. Lengthy data retention periods for all data categories cannot be justified for any service provider, including EU ccTLDs. Furthermore, extensive and indiscriminate data retention for law enforcement purposes leads to additional costs relating to the infrastructure, IT equipment and human resources necessary for ensuring a secure data storage and timely handling of responses to law enforcement data access requests.

As the majority of EU 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. Consequently, any consideration of a potential data regime applicable to TLD registries should be limited to the mandatory registration dataset under Article 28(2) of the NIS 2 Directive.

Before mandating a specific data retention regime applicable to EU ccTLDs, the European Commission must conduct a proper impact assessment of the feasibility and usefulness of retaining the mandatory registration dataset for law enforcement purposes for each data category.

Any potential data retention regime applicable to TLD registries should also be limited in maximum length, determined by the utility of domain registration data for law enforcement investigations after the expiration of a domain name registration. In principle, the retention of basic subscriber data for law enforcement purposes could be aligned across digital sectors for increased legal clarity, based on the average mandatory retention period currently applicable in EU Member States.[7] However, the maximum length must be determined by a proper impact assessment that takes into consideration the needs of law enforcement authorities, the technical and operational feasibility of a service provider, and the level of interference with fundamental rights of individuals.

In addition, to minimise the costs associated with any mandatory data retention for EU ccTLDs, it is advisable to **establish a mandatory cost reimbursement mechanism for service providers across the EU**, taking into account existing experiences from EU Member States.[8] The main cost factor in this case is increased human resources, including for providing appropriate training and handling of responses to data access requests.

As confirmed by the CJEU on numerous occasions, data protection standards in the EU require privacy safeguards that minimise interference with individuals' fundamental rights, including protection from unauthorised access and further misuse. Consequently, data retention regimes for law enforcement purposes require additional efforts from service providers and must be proportionate to the providers' size and business models. Cost reimbursement mechanisms should be made available to SMEs and non-profits.

Cooperation with law enforcement authorities

EU ccTLDs consider the trust and safety of their TLD zones as a key service for their local internet communities. Voluntary cooperation mechanisms between ccTLD registries and law enforcement authorities, including for increased information sharing, can serve as valuable examples of effective private-public partnerships. Such **voluntary cooperation mechanisms with law enforcement authorities, including on threat intelligence, should be actively promoted across the EU.**

Personal data is not the only information that can be valuable for law enforcement investigations in cyberspace. As such, its importance should not be overestimated, especially at the expense of privacy and data protection safeguards. DNS query data, which are visible to ccTLDs (e.g., query logs and spikes in visits to certain domain names), can contribute to identifying suspicious behaviour and track abuse patterns, without identifying specific users or retaining large amounts of personal data. This information on abuse patterns may be shared with law enforcement authorities on a voluntary basis and does not include any personal data.

[7] For example, the mandatory data retention period for law enforcement purposes is 12 months, which corresponds to the average age of the most frequently requested data by law enforcement authorities (i.e., up to one year) according to the European Commission "Study on the retention of electronic communications non-content data for law enforcement purposes" (2020).

[8] For example, under Finland's Act on Electronic Communications Services, a telecommunications operator is entitled for compensation from the state funds for the direct costs of investment and maintenance of systems and equipment used solely to assist public authorities. In the Czech Republic under the Electronic Communications Act, legal entities providing a publicly available communications network are entitled for reimbursement for incurred costs for the storage of traffic and location data.

Therefore, it is advisable to take a holistic approach in the discussions on data sharing with law enforcement authorities that does not overly rely on personal data retention and access. **Certain data is already shared with law enforcement authorities, without the need for legislative intervention.**

Some notable cooperation examples from CENTR members include:

- .cz is developing an Advanced DNS Analytics and Measurements (ADAM) project that analyses the DNS requests directed at .cz. The project helps to better understand the usage of .cz domains and helps with the analysis of security incidents and attacks. .cz also established a Memorandum of Understanding with the Czech Trade Inspection on the exchange of data on potentially fraudulent e-shops detected by ADAM.

- .eu provides regular assistance to law enforcement and other relevant authorities supporting them in the fight against illegal activities involving .eu domain names. This encompasses cooperation with the Belgian Federal Ministry of Economic Affairs, the Belgian Customs (Cybersquad) and the Belgian Public Prosecutor's Office, as well as engaging in regular dialogue with the Computer Emergency Response Team for the EU (CERT-EU), and cooperating with Europol by exchanging statistical data and trends, running joint projects aimed at combatting cybercrime.

- .pt together with Portuguese Public Security Police (PSP) established a cooperation protocol for the development of national cybersecurity and cybercrime prevention capabilities. The cooperation includes strategic development of capacities in the fight against cybercrime, training and upskilling of PSP's employees, and the creation of specific tools to support investigation and joint operations.