10 NOVEMBER 2023 • *Brussels, Belgium*

Recommendations to the national implementation of data accuracy provisions in Article 28 of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)

Introduction

This document provides a list of CENTR recommendations in the context of the implementation discussions on Article 28 of 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 ('NIS2 Directive').

CENTR is the association of European country code top-level domain registries (hereinafter 'ccTLDs'). The CENTR membership includes every ccTLD registry for EU and EEA member states (such as '.cz', '.no', and '.it').

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 (i.e., registrars, end-users, rightsholders but also in cooperation with CSIRTs and law enforcement authorities).

ccTLDs are responsible for operating and maintaining the technical Domain Name System (DNS) infrastructure for their top-level domain (TLD). 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 IP addresses.

ccTLD registries maintain a domain name registration database. This database contains various information of domain name holders (e.g., name and contact details), as well as technical and administrative data necessary to provide DNS services. Registration data can be queried by the general public using different protocols like the web, WHOIS and RDAP. For entities providing services in the EU, access to non-public domain name registration data containing personal data is governed by the General Data Protection Regulation (GDPR) and other national data protection legislation. ccTLD registries are considered to be "essential entities" according to the NIS2 Directive.

The goal of these recommendations is to provide insights into how the public policy objectives can be reached without disproportionate impact on the European registrants, TLD name registries and entities providing domain name registration services, such as registrars and resellers.

The recommendations should be read in the context of existing legal requirements, including those set by GDPR. Given the explicit references to the GDPR in the NIS2 Directive, and the fact that obligations related to

maintaining a database for domain name registration data implies the processing of personal data, Article 28 and the recommendations below must be read in light of the GDPR.

CENTR recognises that the NIS2 Directive sets minimum requirements for measures for a high common level of cybersecurity across the EU. Specific legal requirements in Member States per national and EU law might require different approaches for the implementation of Article 28.

It is impossible to identify one solution that would conform to all legal requirements across the EU, as inter alia evident from the variety of existing registration data accuracy practices across European ccTLDs. Article 28 is drafted in a technologically neutral manner, while recognising various technical means and processes that may be suitable for the purpose of ensuring accuracy and completeness of domain name registration data.

These recommendations should not be interpreted as requirements prescribed in the Directive. We recognise that specific requirements will be set by the transposition of the Directive in each Member State.

Considering the above, CENTR would like to provide the following high-level recommendations to the NIS Cooperation Group on the implementation of Article 28, taking into account the long-standing experience of European ccTLDs.

Recommendations

1. It is necessary for national implementation timelines of Article 28 to recognise the complexity of the DNS landscape, as well as the availability and accessibility of appropriate verification infrastructure in the Member States, in order to preserve stability of the current domain name registration systems serving registrants across borders. A gradual approach to implementation of Article 28 requirements is essential, allowing the TLD registries and entities providing registration services to adapt their technical set-up without impacting new registrations.

2. European ccTLDs are recognised to represent the lowest levels of DNS Abuse in the global industry. Any verification obligation should serve the purpose of contributing to the security, stability and resilience of the DNS, and be proportional to the size of the problem the requirement aims to address.

3. National implementations of Article 28 need to take into account the fundamental data protection principles, such as data minimisation and accuracy. Hence, requirements to collect and maintain domain name registration data should not go beyond what is necessary to achieve the purpose of Article 28. The data minimisation principle, for example, shall apply to the minimum datasets that TLD registries and entities providing domain name registration services are obliged to collect and publish under Article 28(2), and shall not include other data elements than those listed in the NIS2 Directive.

4. National implementations of Article 28 need to accommodate a hybrid model that allows for either the TLD registry or the entity providing registration services, or both operators to do the verification. In

some situations, this might result in the TLD registry and the entity providing registration services verifying different parts of the required dataset.

5. Entities providing domain name registration services need to abide by the verification requirements of the TLD they are registering for and strictly comply with to the extent of the national requirements under which this particular TLD operates.

6. The minimal EU-wide recommendation should be for verification measures to be flexible and risk-based depending on the national circumstances of the ccTLD. Both pre-delegation and post-delegation verification measures should be allowed, however pre-delegation verification may not always be required due to low risk. The risk could be assessed based on a range of factors (e.g., reputation of entity providing domain name registration service) which have been identified by the registry as indicators of increased risk of inaccurate or incomplete information to identify and contact the domain name holders. A risk-based approach should allow for a concrete assessment of whether and to what extent verification measures include both existing and new registrants.

7. In some Member States, electronic identification (eID) solutions might be the preferred solution to address the verification requirement. In such cases it is essential that TLD name registries and entities providing domain name registration services have access to national eID infrastructure and eIDAS nodes.

8. Currently, self-selection by the domain name holder of their legal status (individual vs. legal representative) during the domain name registration process is the only solution for many EU/EEA entities to make a distinction between legal entities and individuals. Self-selection by the registrant should be recognised as sufficient basis for the TLD name registries and entities providing domain name registration services to recognise in what capacity the domain name is registered by the domain name holder, and proceed with the publication of relevant registration data (such as name and contact information) within the limits of data protection requirements.

9. Verification of legal entities (and their rightful representatives for the purpose of domain name registration) is still problematic in the majority of Member States. In the event that TLD name registries and entities providing domain name registration services are required by their national legislation to strengthen verification of legal entities, they will need access to external authoritative sources (such as VIES and other national databases), whose reply could serve as an authoritative basis for validation. Where appropriate, such access should be regulated in the national legislation. This would limit the need to use external commercial verification services with potential GDPR issues.