Council of European National Top-Level Domain Registries

Brussels, Belgium
5 May 2021

CENTR comment on the Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 ('NIS2')

Summary of CENTR's key recommendations:

CENTR calls on co-legislators to clarify the provisions of Article 23 of the NIS2 proposal in order to align it with the existing EU data protection framework:

- Article 23 should include a clear purpose limitation to the data accuracy obligation, i.e. "**TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate domain name registration data, having regard to the purposes for which it is processed**". This way it is aligned with the respective data accuracy principle enshrined in Article 5 of the GDPR.
- Article 23(2) should be amended to include "relevant information to identify and contact the holders of the domain names and the **administrative** points of **contact** of domain names under the TLDs **that is strictly necessary and proportionate under the corresponding legal basis for such processing stipulated in Union or Member State law**".
- The vague notion of **"complete" should be omitted from Article 23,** as it is meaningless if detached from the limited purpose for which a TLD gathers data.
- For the sake of legal clarity, **Article 23(3) needs to be omitted and/or merged with Article 23(1).**
- **Legitimate access seekers under Article 23(5) need to be limited to competent national authorities,** as designated by Member States under their national cybersecurity strategies, including competent public authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, **provided that access to registration data is granted** under **the corresponding legal basis that satisfies the conditions of the Union data protection framework.**

Introduction

CENTR is the association of European country code top-level domain registries (hereinafter ccTLDs). All EU Member State and EEA country ccTLDs (such as .de, .no, and .pt) are members of CENTR.

CENTR members are at the core of the public internet, safeguarding the stability and security of the internet as we know it today. The majority of European ccTLDs 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 authorities and national governments).

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.

Furthermore, ccTLD registries maintain a domain name registration database. This database contains contact information of domain name holders, technical and administrative data necessary to provide DNS services. Only part of these registration databases is publicly accessible within the limitations of national and regional legislation. 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). These protocols allow a user to perform a search on a given domain (or IP address) and retrieve various information about its registration. For the entities providing services in the EU, access to domain name registration data is governed by the EU GDPR, as the registration database contains personal information.

ccTLD technical operations differ largely depending on the infrastructure and software they use. These differences reduce the risk that a single vulnerability would affect all ccTLD operators.

ccTLD registries are listed as "operators of essential services", as enshrined in Annex II of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive") and are considered to be "essential entities" according to the Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (the "NIS2 proposal").

As entities under the scope of the NIS2 proposal which will be directly impacted by the NIS2 framework, CENTR members would like to ask legislators to take into consideration and adequately assess the impact of the proposed legislation on ccTLD operators, who form the core of the public internet, together with other internet infrastructure actors.

CENTR members would like the co-legislators to address the following areas of concern in the NIS2 Proposal.

Domain name registration data

Article 23 of the NIS2 Proposal creates an obligation for TLD registries and the entities providing domain name registration services for the TLD (registrars) to "collect and maintain accurate and complete domain name registration data" (hereinafter the 'data accuracy obligation') and provide access to such data "upon lawful and duly justified requests of legitimate access seekers".

First, it is worth recalling that a domain name registration contains personal information and is, therefore, protected under the respective privacy and data protection framework in the EU[1]. Any interference with the individual's right to privacy and data protection needs to be subject to the appropriate balancing test, including against the principle of proportionality and necessity.

ccTLDs predominantly have a role of data controller or data processor when it comes to maintaining the registration database. The legal grounds for collecting registration data are in accordance with the GDPR and other national data protection legislation corresponding to EU law. One of the most common legal grounds for data processing among ccTLDs is for the "performance of a contract". The personal data processed by ccTLDs is strictly limited for the purposes identified in Article 6 of the GDPR.

[1] Charter of Fundamental Rights of the European Union; and Regulation (EU) 2016/679 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

The aforementioned data accuracy obligation, as enshrined in Article 23 of the NIS2 proposal, namely the obligation to "collect and maintain accurate and complete registration data" contains many unclear elements, and hence it is questionable if this obligation would serve the intended purpose of facilitating ”regulatory compliance for entities providing cross-border services".

It is, therefore, in the interest of sustainable and future-proof legislation that Article 23 is clarified and provides the legal clarity needed for essential entities, regulators and third parties seeking access to personal information.

1.1 Importance of WHOIS for the security, stability and resilience of the DNS

Article 23(1) states that "For the purpose of contributing to the security, stability and resilience of the DNS, [...]TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate and complete domain name registration data[...]".

First of all, the justification for such a stringent and broad data accuracy requirement in the NIS2 proposal is that allegedly "maintaining accurate and complete databases of domain names and registration data (so called ‘WHOIS data)’[...] is essential to ensure the security, stability and resilience of the DNS" (Recital 59).

While maintaining a registration database is part of the responsibilities of ccTLD registries, the WHOIS protocol is not what makes the DNS function and/or resolves domain name queries in order for the internet to function. The aforementioned statement on the connection of accurate and complete registration data to the security, stability and resilience of the DNS is flawed and does not reflect the reality of cyberattacks targeting the DNS infrastructure: DDoS attacks, DNS poisoning, DNS hijacking etc.[2] None of the above-mentioned cyberattacks using the DNS infrastructure can be prevented or addressed by merely maintaining accurate and complete domain name registration data.

While accurate domain name registration data can contribute to the identification of perpetrators abusing the DNS infrastructure in cases such as malware distribution, phishing, botnets etc and to keep some of the rogue actors out, it is not the sole decisive and effective means to ensure a secure, resilient and stable DNS infrastructure.

It is, therefore, misleading to connect the data accuracy principle in Article 23 with the aforementioned purpose without any clear evidence for such a statement in the Impact Assessment conducted by the European Commission.

The Impact Assessment accompanying the NIS2 proposal does not mention the registration database at all, beyond describing what a TLD is in general terms. Legislation which in this case aims to increase the level of harmonisation of security and reporting requirements, and which may affect the protection of personal data, needs to be preceded by a clear impact assessment. This is missing in the NIS2 proposal.

Furthermore, there is no equivalent obligation, or even indication that the maintenance of a complete and accurate registration database should fall under the notion of "essential services" under the NIS Directive. Neither the results of the European Commission's report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services[3], nor the Summary Report on the open public consultation on the NIS

[2] CSC, “The DNS Ecosystem, Its Vulnerabilities, and Threat Mitigations”, CircleID, 24 September 2020, Available here: https://www.circleid.com/posts/20200924-the-dns-ecosystem-its-vulnerabilities-and-threat-mitigations/

[3] European Commission, Report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, 28 October 2019, Available here: https://ec.europa.eu/transparency/regdoc/rep/1/2019/EN/COM-2019-546-F1-EN-MAIN-PART-1.PDF

Directive from January 2021[4] have identified and accounted for the fact that inaccurate and incomplete registration data actually poses any significant cybersecurity risks to the operators of essential services, to the extent that this would merit its inclusion in the NIS2 proposal.

It is, therefore, unclear what data and evidence the European Commission based its conclusion[5] that the data accuracy obligation under Article 23 is essential to ensure the security, stability and resilience of the DNS on.

Consequently, Recital 59 should be rephrased to reflect that "maintaining accurate and complete databases of domain names and registration data (**part of which is the** so-called 'WHOIS data') and providing lawful access to such data **may contribute to increased cybersecurity when the DNS infrastructure is abused**, which in turn contributes to a higher common level of cybersecurity within the Union[...]".

1.2. "Relevant information"

Article 23(2) states that domain name registration data referred to in the NIS2 proposal shall "contain **relevant information to identify and contact the holders of the domain names** and **the points of contact administering the domain names under the TLDs**"[emphasis added].

While it is beneficial to the purposes of the Directive to ensure the variety of national differences and approaches exercised by TLD registries in this regard, it is still unclear what type of relevant information needs to be controlled by a TLD registry, considering this *is* personal information and is subject to the relevant data protection rules under EU primary law - the Charter of fundamental rights in the EU.

The amount and specifics of collected and publicly available registration data depends on the national jurisdiction and, where applicable on national legislation.[6]

It is a disproportionate burden on ccTLD registries to impose a broad obligation to collect and process ***all*** possible information that is relevant to identify and contact holders of domain names. In essence, relevant information in the context of registration data collected by a ccTLD is the minimal data needed to operate the registry's function. For increased legal clarity and so as not to disrupt the provision of essential services, which is the maintenance of the DNS that is essential for the provision of all other digital services in the internal market, this obligation should be reserved for the information that is strictly necessary, and in accordance with EU data protection safeguards such as lawfulness, purpose limitation, data minimisation, storage limitation, integrity and confidentiality (as enshrined in Article 5 of the GDPR).

Furthermore, the NIS2 proposal completely disregards the fact that the vast majority of European ccTLDs already collect and process registration data in accordance with their national legal frameworks. It is, therefore, surprising at least to see such a broad and vague definition of the data accuracy principle that completely disregards what is effectively already being done at national level across the Union.

[4] European Commission, Summary Report on the open public consultation on the Directive on security of network and information systems (NIS Directive), 27 January 2021. Available here: https://ec.europa.eu/digital-single-market/en/news/summary-report-open-public-consultation-directive-security-network-and-information-systems-nis

[5] The communication from the European Commission on the EU Security Union Strategy only mentions that "Access to Internet domain name registration information ('WHOIS data') is important for criminal investigations, cybersecurity and consumer protection", and does not provide any details as to how the respective data accuracy obligation is relevant in this regard.

[6] For more details on different approaches across European ccTLDs, see here: https://stats.centr.org/pub_whois

Therefore, CENTR members ask the co-legislators to clarify and limit the vague notion of "relevant information to identify and contact" to what is strictly necessary for TLD registries to perform their primary duty of providing a stable, secure and resilient service.

It is also unclear what type of information is meant by the requirement to collect “the points of contact administering the domain names under the TLDs” in Article 23(2). Domain name registration data collected by registries usually contains details of an administrative and / or a technical contact, needed to reach the individual maintaining a domain name in case there are any technical issues with the domain name. It should be clearly stated in Article 23(2) that these points of contact are limited to the administrative and technical contacts.

For this purposes, Article 23(2) should be amended to include "relevant information to identify and contact the holders of the domain names and the **administrative** points of **contact** of domain names under the TLDs **that is strictly necessary and proportionate under the corresponding legal basis for such processing as stipulated in the Union or Member State law**".

1.3 "Complete and accurate"

Article 23(3) states that Member States shall ensure that "the TLD registries and the entities providing domain name registration services for the TLD shall have policies and procedures in place to ensure that the databases include accurate and complete information".

First of all, for the sake of consistency with the rest of the article and the intended purpose to govern domain name registration data, it should be clarified whether the data accuracy obligation in Article 23(3) actually concerns registration databases. It is, otherwise, unclear ***which*** databases Article 23(3) refers to, and how it is different from the obligation in Article 23(1). It is also unclear what the purpose of including Article 23(3) in the legislation concerning cybersecurity is.

For the sake of legal clarity, **Article 23(3) needs to be omitted and/or merged with Article 23(1).**

The use of the vague notions "complete and accurate" throughout Article 23 should also be further specified, following the data protection safeguards under the GDPR.

At the very least, Article 23 should be amended to include a clear purpose limitation to the data accuracy obligation, i.e. "**TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate domain name registration data, having regard to the purposes for which it is processed**". This way it is aligned with the respective data accuracy principle enshrined in Article 5 of the GDPR.

As with the notion "complete", there is no indication on what could constitute a "complete" database for the purposes of the NIS2 proposal, or for which purposes or cybersecurity needs such an arbitrary obligation is being introduced on technical operators providing an essential service to society. Therefore, **the vague notion of "complete" should be omitted from Article 23,** as there is no added value in including such a notion in the legislative text.

1.4. "Legitimate access seekers"

Article 23(5) states that "Member States shall ensure that the TLD registries and the entities providing domain name registration services for the TLD provide access to specific domain name registration data **upon lawful and duly justified requests of legitimate access seekers,** in compliance with Union data protection law"[emphasis added].

Recital 60 gives an indication of the purpose and a potential group of intended "legitimate access seekers" to ensure access to personal information collected and processed by domain name registries. Namely, the "availability and timely accessibility of these data to public authorities, including competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs, (CSIRTs, and as regards the data of their

clients to providers of electronic communications networks and services and providers of cybersecurity technologies and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents"[sic].

The majority of ccTLDs provide some form of access to non-public registration data containing personal information, primarily for law enforcement purposes and to the parties identified in a court order.

For the sake of clarity for essential entities, such as ccTLDs, there is a need to clearly limit the scope of potential "legitimate access seekers", as Article 23(5) constitutes an interference with the fundamental right to the protection of personal data guaranteed under the EU Charter of Fundamental Rights.

Furthermore, both the European Data Protection Board[7] and the European Data Protection Supervisor[8] have recalled in this regard that conditions under which entities providing domain name services, including TLDs, must grant access to registration data must be provided by law, so as to ensure that the processing relies on a clear legal basis. Furthermore, according to the European Court of Justice (CJEU) the legal basis which permits such interference must itself **define the scope of the limitation** on the exercise of the right concerned, and **impose minimum safeguards** for the data subjects concerned to be effectively protected against the risk of abuse.

It is worth recalling that Article 23 of the GDPR lays down the conditions for Union or Member State law to make derogations from certain provisions in the GDPR, including the data protection principles in Article 5 and the corresponding data subject's rights. However, these restrictions must respect the essence of fundamental rights and freedoms and **be a necessary and proportionate measure in a democratic society**.

Article 23(2) of the GDPR clearly stipulates that the essential elements of such a legislative measure restricting the rights of the data subject must contain specific provisions at least, where relevant on: 1) the purposes of the processing or categories of processing; 2) the categories of personal data; 3) the scope of the restrictions introduced; 4) the safeguards to prevent abuse or unlawful access or transfer; 5) the specification of the controller or categories of controllers; 6) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; 7) the risks to the rights and freedoms of data subjects; and 8) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

There is no evidence, beyond two sentences in the Explanatory memorandum accompanying the NIS2 proposal[9], that any of the essential elements of Article 23 of the GDPR were properly assessed when introducing the obligation on data controllers to provide access to personal information to third parties that clearly constitutes an interference with data subjects' rights.

Consequently, Article 23 of the NIS2 proposal should be aligned with the GDPR and clearly state which categories or which purpose access to personal information should be granted for; and the scope of legitimate access seekers, taking into account the purpose of the NIS2 and the intended aim to increase the resilience and security of network

[7] In the context of cross-border access requests to domain name registration data, the European Data Protection Board's Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) , adopted on 2 February 2021. Available here: https://rm.coe.int/edpb-statement022021onbudapestconventionnewprovisions/1680a1617f

[8] European Data Protection Supervisor, Opinion 5/2021on the Cybersecurity Strategy and theNIS 2.0 Directive, 11 March 2021. Available here: https://edps.europa.eu/system/files/2021-03/21-03-11_edps_nis2-opinion_en.pdf

[9] Section "Fundamental rights" in the Explanatory memorandum: "The EU is committed to ensuring high standards of protection of fundamental rights. All voluntary information sharing arrangements between entities that this Directive promotes would be conducted in trusted environments in full respect of Union data protection rules, notably Regulation (EU) 2016/679 of the European Parliament and of the Council."

and information systems**. For these purposes, the pool of legitimate access seekers shall be limited to: competent national authorities, as designated by Member States under their national cybersecurity strategies, including competent public authorities under Union or national law for the prevention, investigation or prosecution of criminal offences** - as these entities have the necessary mandate to respond to cyberthreats affecting users of network and information systems. However, such access shall only be granted under **the corresponding legal basis that satisfies the conditions of Union data protection framework.**

Additionally, it should be clarified that similar data protection safeguards, such as a clear legal basis, need to govern any access procedures including the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data, as envisaged in Recital 62. Every disclosure of personal information needs to be assessed in accordance with the GDPR and corresponding national legal frameworks.

Conclusion

To reiterate the points indicated above, CENTR members would like to put forward the following recommendations in the ongoing legislative debate on the NIS2 proposal:

- CENTR recalls that a domain name registration contains personal information and is, therefore, protected under the respective privacy and data protection framework in the EU. Any interference with the individual's right to privacy and data protection needs to be subject to the appropriate balancing test, including against the principle of proportionality and necessity.
- CENTR highlights that, while maintaining a registration database is part of the responsibilities of ccTLD registries, the WHOIS protocol is not what constitutes the Domain Name System (DNS). The statement on the connection between accurate and complete registration data and the security, stability and resilience of the DNS in Article 23 of the NIS2 proposal is flawed and does not reflect the reality of cyberthreats targeting the DNS infrastructure.
- CENTR highlights that, while accurate domain name registration data can contribute to the identification of perpetrators abusing the DNS infrastructure to keep some of the rogue actors out, it is not the sole decisive and effective means for a secure, resilient and stable DNS.
- CENTR calls for the alignment of the intentions of the proposed directive and the expectations stemming from the increased data accuracy obligation in Article 23 by amending recital 59 to reflect that “maintaining accurate and complete databases of domain names and registration data (**part of which is the** so-called ‘WHOIS data’) and providing lawful access to such data **may contribute to increased cybersecurity when the DNS infrastructure is abused[...]”.**
- CENTR recalls that the vast majority of European ccTLDs already collect and process registration data in accordance with their national legal frameworks, including the relevant data protection rules. Similarly, the majority of ccTLDs already provide some form of access to non-public registration data, primarily for law enforcement purposes and to the parties identified in a court order.
- CENTR calls on co-legislators to clarify the provisions of Article 23 of the NIS2 proposal, so that it provides the legal clarity needed for essential entities, regulators and third parties seeking access to personal information.
- CENTR recommends that Article 23(2) should be amended to include "relevant information to identify and contact the holders of the domain names and the **administrative** points of **contact** of domain names under the TLDs **that is strictly necessary and proportionate under the corresponding legal basis for such processing stipulated in the Union or Member State law"** to align the data accuracy principle with the existing EU data protection framework.

- CENTR recommends aligning Article 23(1) with Article 23(3) for the sake of consistency with the rest of the article and the intended purpose to govern domain name registration data. For the sake of legal clarity, **Article 23(3) needs to be omitted and/or merged with Article 23(1).**
- CENTR recommends amending Article 23 to include a clear purpose limitation to the data accuracy obligation, i.e. "**TLD registries and the entities providing domain name registration services for the TLD shall collect and maintain accurate domain name registration data, having regard to the purposes for which it is processed**". This way it is aligned with the respective data accuracy principle enshrined in Article 5 of the GDPR.
- CENTR recommends omitting the vague notion of **"complete" from Article 23,** as it is meaningless if detached from the limited purpose for which a TLD gathers data and serves no evident purpose for increased cybersecurity resilience across the Union.
- CENTR recalls that conditions under which entities providing domain name registration services, including TLDs, must grant access to registration data must be provided by law, so as to ensure that the processing relies on a clear legal basis.
- CENTR recalls that the legal basis which permits the interference must itself **define the scope of the limitation** on the exercise of the right concerned, and **impose minimum safeguards** for the data subjects concerned to be effectively protected against the risk of abuse.
- CENTR calls on co-legislators to align Article 23 with the GDPR and clearly state which categories or which purpose access to registration data should be granted for.
- CENTR calls on co-legislators to clearly limit the pool **of legitimate access seekers under Article 23 to competent national authorities, as designated by Member States under their national cybersecurity strategies, including competent public authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, provided that access to registration data is granted** under **the corresponding legal basis that satisfies the conditions of Union data protection framework.**

About CENTR

CENTR is the association of European country code top-level domain (ccTLD) registries, such as .de for Germany or .si for Slovenia. CENTR currently counts 53 full and 9 associate members – together, they are responsible for over 80% of all registered domain names worldwide. The objectives of CENTR are to promote and participate in the development of high standards and best practices among ccTLD registries. Full membership is open to organisations, corporate bodies or individuals that operate a country code top level domain registry.