The ICANN GNSO "Business Constituency"

Comments of the ICANN Business Constituency on provisions of the draft NIS2 Directive related to domain name registration data

17 March 2021

This response is provided on behalf of ICANN's Business Constituency (BC), which is the voice of commercial Internet users within ICANN, and represents the interests of small, medium, large and multinational enterprises as users of the domain name system (DNS).

Thank you for the opportunity to provide detailed feedback on the draft Revised Directive on Security of Network and Information Systems (NIS2). We appreciate both the Commission addressing the DNS and domain name service providers in the NIS2 proposal, and its consideration of the role of the DNS in combating all types of illegal behavior online.

As the Commission is aware, over the past three years a multistakeholder policy development process within ICANN has endeavoured to develop new policies on the publication of, and access to, domain name registration data (commonly referred to as WHOIS data). The BC and other constituencies from ICANN's multistakeholder community, including the Governmental Advisory Committee (GAC), found the resulting policy recommendations to have failed the needs of cybersecurity, consumer protection, law enforcement, and intellectual property rights holders due to misapplication of certain important privacy protections created by the General Data Protection Regulation (GDPR).

The BC and other dissenting stakeholders all expressed, and still hold, strong support for privacy protections for personal data and are invested in the development of ICANN policies that strike a balance between the individual right to privacy and the safeguards for law enforcement and other legitimate interests. But we agree with the GAC, which withheld support for certain new policy recommendations precisely because they "do not strike the appropriate balance between protecting the rights of those providing data to registries and registrars and protecting the public from harms associated with bad actors seeking to exploit the domain name system."[1]

The provisions set out in Article 23 of the draft NIS2 Directive provide an important clarification on the critical value of WHOIS data, and when, how, and to what extent that data should be made available to third parties with a legitimate interest. It is supported by definitions in Article 4 and by recitals that explain the desired objectives of Article 23. In each section below, we convey our support for these provisions and suggest ways in which they can be strengthened and / or clarified to prevent unintended consequences and ensure that the NIS2 Directive will enable timely access to accurate and complete WHOIS data for legitimate purposes, thereby contributing to keeping users safe online.

[1] See page 122 at https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtldregistration-data-2-31jul20-en.pdf. Note that this document also contains similar concerns from four other parts of the ICANN multistakeholder community - the At-Large Advisory Committee, the Security and Stability Advisory Committee, the Business Constituency and the Intellectual Property Constituency.

Clarify the scope of DNS providers considered under Article 23

We support the aim of Article 23 to apply the obligations for processing and publication of WHOIS data not just to registrars, but also to registries, rightfully recognizing the critical part they can play in enabling access to WHOIS data. In the same spirit, the provision could be further clarified to include domain name resellers and privacy/proxy registration services.

A significant portion of registration data is not provided directly by registrants themselves, but rather by privacy and proxy service providers, which substitute their own data for that of the underlying registrant. These providers are sometimes a service provided by a registrar but may alternately be a third-party vendor. It is therefore important to provide further clarity regarding the scope of the DNS providers considered under the revised directive by including domain name resellers and privacy/proxy registration services in the scope of the Directive.

We request that Articles 23(1) and 23(3) (as well as Recitals 61 and 62) make explicit reference to resellers and privacy/proxy service providers as being among entities providing services related to domain name registration. We also request that three new paragraphs be added to Article 4 to provide separate definitions for resellers, privacy service providers, and proxy service providers. Article 2(2)(a)(iii) and point 8 of Annex 1 will also need to be modified to reflect this clarified scope of entities which are subject to Article 23. Separately, in order to ensure a baseline for uniformity and consistency, it is important to add definitions in Article 4 to describe both DNS abuse and the elements that comprise “complete domain name registration data”.

Allow for dedicated cloud service tenants as a place for collection and maintenance of domain name contact data

We support the text in Article 23(1) that seeks to ensure the secure management of domain name registration data. However, we feel it is unduly restrictive to allow for this to be done only via a “dedicated database facility”, which implies that controllers of the data must manage their own data centres.

We suggest that they should be given reasonable technical flexibility as to how they will securely manage the data. This could be achieved by additionally allowing for managing the data in a “dedicated cloud service tenant”. Management of the data via a commercial cloud service is an acceptable solution and one that is particularly suited to smaller controllers with less expertise in online security, high performance computing and modern data protection technologies.

Addressing the use of privacy or proxy registration services to conceal the entity using the domain name

Article 23(2) importantly requires that domain name registration data contains information that makes it possible to identify and contact the holders of domain names. We propose to strengthen this provision by addressing privacy and proxy registrations, which are used to conceal from public view the data of the person or organisation using the domain name. Registrars and service providers should be pre-empted from using privacy and proxy registration shields for the purpose of circumventing the intent of this Directive. We therefore propose the addition of text to Article 23(2) to require TLD registries and registrars to provide access to the true underlying domain name registration data upon lawful and duly justified requests of legitimate access seekers, in compliance with Union data protection law.

This issue should also be clarified by adding text to Article 23(3). As highlighted by Commission officials during a February 2021 briefing call with ICANN stakeholders[2], it would provide an obligation of the service provider (not solely the registrant) to ensure that registration data is accurate. The wording in Article 23(3) requiring providers to have "procedures in place to ensure that the databases include accurate and complete information" provides helpful clarification about this obligation. In addition, the requirements for accuracy in Article 23(3) will help address a policy area that has proved extremely challenging for ICANN to resolve: the distinction between natural and legal persons when processing contact data.

To strengthen the requirement and reduce the possibility that registries and registrars will use privacy and proxy services to conceal true registrant information and circumvent the intention of this Article, the text of Article 23(3) should be expanded to specify that the "accurate and complete information" must pertain specifically to the domain name registrant or the customer of the privacy/proxy service.

We also recommend that Article 23(1) be clarified to require service providers to periodically verify the accuracy of their data, and that Article 23(3) include an obligation for service providers to refuse or terminate services upon discovering that a registrant has provided inaccurate data and the registrant does not remedy the inaccuracy in a reasonable amount of time.

Ensure timely access to WHOIS data

Many of the legitimate purposes for accessing WHOIS data, such as for law enforcement or cybersecurity, are extremely time-critical and rely on swift access to data to respond to fast-moving situations and mitigate, as quickly as possible, harm being caused by cyberattacks or criminal or terrorist activities. Registrars and registries often "rate-limit" (control the rate of) queries for such data, impeding critical investigations. Article 23 has the important intention of calling for publication (paragraph 4) and provision (paragraph 5) of data without undue delay. However, the wording should be strengthened to specify that the data should be published and provided within 24 hours, and without delay or impediment, and that a response to a lawful and justified request for data should not simply be a "reply" (which might be understood simply as acknowledgement of the request) but entail a provision of the requested data.

Recognise that legitimate access to domain name registration data serves the public interest

The ICANN Business Constituency has frequently noted the difficulty of creating effective Internet Governance policies given a lack of explicit acknowledgement of the legitimate interest of third parties in requesting and further processing these domain name registration data records. Indeed, the Commission's July 2020 Communication on the EU Security Union Strategy[3] stated that access to WHOIS data "is important for criminal investigations, cybersecurity and consumer protection. However, access to this information is becoming more difficult." References to "lawful and duly justified requests of legitimate access seekers" in Article 23(5) go a long way to addressing this gap.

However, it is important for Article 23 to explicitly state that access to domain name registration data serves the public interest and contributes to the security and stability of the Internet. This would be in line with existing EU regulation; for example, the .eu registry is required to "organise, administer and manage the .eu TLD in the

[2] https://features.icann.org/event/icann-organization/icann-stakeholder-assembly-briefing-european-commission-recent-eu

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&rid=9

general public interest and ensure in all aspects of the administration and management of the .eu TLD"[4], including for "high quality, transparency, security, stability, predictability, reliability, accessibility, efficiency, non-discrimination, fair conditions of competition and consumer protection". This fact is evidenced by certain Member States' more practical policies with regard to registration data access (e.g., Denmark), where the Danish Domain Names Act requires that data be accessed for legitimate purposes without violation of GDPR provisions[5]. We therefore propose a new Article 23(6) which would state that "Domain name registration data serves the public interest; accordingly, Member States shall ensure that a natural person registrant's name, verified email address, and postal address, as appropriate to establish jurisdiction, are disclosed when requested for legitimate purposes."

This document was approved in accord with the Charter of the ICANN Business Constituency[6].

[4] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58847
[5] See explanation of Section 18 in correspondence between Denmark and ICANN: https://www.icann.org/en/system/files/correspondence/vignal-schjoth-to-plexida-28may20-en.pdf
[6] https://www.bizconst.org/charter