Comments on the Revised Directive on Security of Network and Information Systems (NIS2)

Registrar Stakeholder Group

The Association of the Registrar Stakeholder Group e.V. (RrSG) is an association with a registered office in Bonn, Germany. The RrSG represents ICANN-accredited[1] domain name registrars (Registrars) from all across the world.

Registrars play an integral part in the domain name system (DNS) to allow individuals and entities to register domain names and engage on the global Internet. The last year and a half has proven the importance of the Internet to connect communities, be a vehicle for commerce, and provide a simple but ever-important means of communication. Domain name registrars enable this engagement through the registration of domain names.

We are thankful for the opportunity to provide our input and comments on the NIS2 proposal as it is considered by the European Parliament. We are hopeful that these comments open a line of communication for understanding the interests of domain name registrars, our customers, our operations, and how certain approaches to regulations impact our business and the global citizens that we serve.

At the outset, the RrSG wishes to highlight that we support the intended purpose of further securing network and information systems and mitigating risks. We particularly appreciate the articulated commitment to implementing *appropriate* and *proportionate* measures. The RrSG offers the following comments in the hope that they assist the European Parliament in their final reviews of the NIS2, particularly Article 23.

At the highest level, we note that it is not clear if or how the contents of registrar databases (details of our customers) are a matter of securing networks and information systems and we therefore question the appropriateness of these proposed measures as they appear out of scope for the stated intention of NIS2.

Article 23 seems to relate more to cyber criminality than to network stability. Furthermore, such access is already properly defined in the more appropriate Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (e-evidence regulation). We appreciate that there may sometimes be overlap between cyber criminality and network stability, and would welcome clarification in NIS2 recognising both the distinction and overlap.

Further, it is unclear what is meant by “due diligence” for accurate and complete domain name registration data called for in Article 23. Currently, due diligence for the accurate and complete domain name registration data takes place at a number of points in the registration process:

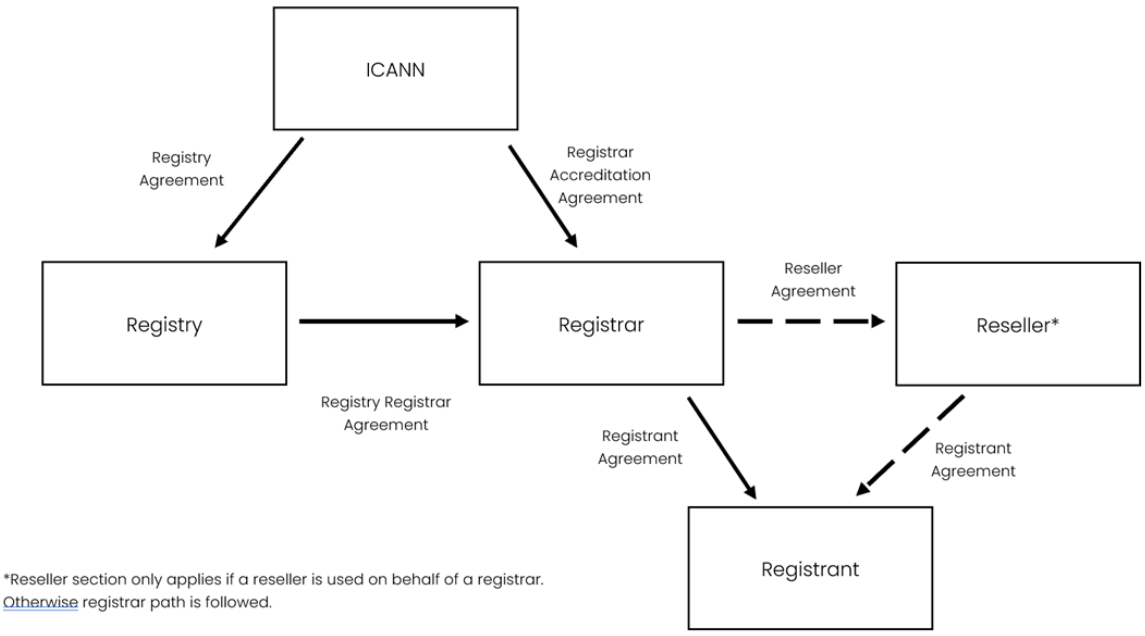
- Before a person can attempt to register a domain name;

[1] https://www.icann.org/get-started

- After registration but before the domain goes lives; and
- After a domain goes live.

Registrars employ various tools to ensure accuracy and completeness at each point.

As the European Parliament may already be aware, Registrars are already required to perform due diligence checks via multiple contractual structures with the ICANN community. With reference to the diagram below, all generic top-level domain (gTLD) registry operators are required to enter into a Registry Agreement (RA) with ICANN. ICANN has a standard base RA[2] that is used by most registry operators (although Registry Operators are permitted to negotiate modified versions of the RA with ICANN). All gTLD Registrars are required to enter into a Registrar Accreditation Agreement (RAA)[3] with ICANN (which is not subject to negotiation by registrars). All Registry Operators are obligated by the RA to enter into a Registry-Registrar Agreement (RRA) with Registrars, and the RA specifies a number of requirements that must be included in every RRA. Although RRAs vary by registry operator, a representative sample RRA is the RRA for the .com TLD.[4] The RAA and RRA both require Registrars to enter into a registration agreement with domain name registrants. Some Registrars additionally utilize the services of Resellers to provide registration services, and the RAA requires that Registrars enter into a written contract with Resellers, and the Registrar is responsible for the compliance of the Reseller.



[2] https://www.icann.org/en/registry-agreements/base-agreement
[3] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en
[4] https://itp.cdn.icann.org/en/files/registry-agreements/com/com-appx-08a-pdf-27mar20-en.pdf

The RAA requires Registrars to collect and maintain registrant contact information; the WHOIS Accuracy Program Specification (WAPS)[5] requires verification; and the Temporary Specification for gTLD registration data covers disclosure requirements[6]. Further, the RAA, RA, and RRA dictate how and what data is collected and transmitted between Registrars and Registries. Additionally, each registration agreement must include provisions prohibiting registrants from "distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name."[7] Failure by a Registrar to abide by the terms of its RAA and/or RRA results in termination of these (and, thus, its ability to register generic top-level domain names). (See **Relevant RAA sections and ICANN Compliance Activities** at the end of this document for a more detailed description of the RAA requirements.)

This leads to our next concern — whether parties in the contractual structure will be able to rely on the due diligence of another party in the chain. As currently written, Article 23 implies that each party in a contractual chain (see graphic above) will be required to conduct due diligence on the accuracy and completeness of domain name registration data. This is contrary to data minimisation principles. In order to serve the purpose of due diligence, the RrSG suggests that only one party in the contractual chain—the registrar itself—be required to conduct due diligence on domain name registration data while others in the chain are permitted to rely on that due diligence. This avoids multiple parties collecting the same personal data for the same purpose whilst also ensuring that each domain name registration is subject to due diligence.

Further, we would like to point out that under Recital 59 of NIS2, the concept of "verifying" database information has been added. The RrSG is particularly concerned with this addition because if the expectation is for registrars to require "proof" that *all* information is correct (such as provision of identification prior to allowing the registration of a domain name), this could have a chilling effect on the ability of everyday citizens to engage online. Recital 59 appears to assume that all domain name registrations are made by legal persons or by persons with the intent to commit fraud or other abusive behaviors. However, the great majority of domain name registrations are made by law-abiding individuals looking to engage in and be on the Internet. Requiring them to "prove" the information they provide—and for registrars to "verify" it—in order to register a domain creates additional steps in the process that could ultimately cause marginalized groups to forgo registering a domain name. This is especially true if an individual is not able to provide the requisite means to prove the veracity of the information[8] or if the

---

[5] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy
[6] https://www.icann.org/resources/pages/gtld-registration-data-specs-en
[7] https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html#_DV_M466
[8] The draft regulation doesn't stipulate how information is to be "verified," so much of the impact will be dependent on how companies choose to comply and/or based on what is ultimately required vis-a-vis regulation.

individual believes the collection of their personal data goes beyond the purpose of a registrar's processing activity and is in violation of Union data protection law. Further, registrars may not always be able to verify non-EU registrant information. We would welcome clarification on whether non-EU registrants are within scope of NIS2 and what the standards of verification would be for non-EU registrants.

Returning to the concept of "proportionality," the RrSG applauds Europe's commitment to "not go beyond what is necessary to meet the specific objectives satisfactorily." The RrSG is concerned that introducing verification measures is not proportionate to the purpose of ensuring that registrants are contactable throughout the life of a registration.[9] Registrants are currently required to give registrars accurate and reliable contact details, and to correct and update them promptly if there are any changes during the term of the registration period. Contactability is verified by the registrars when the registrant positively responds to a communication issued by the registrar at time of domain registration and, if contact is not positively verified, the domain may be suspended or cancelled. As set out more fully at the end of this document, section 3.7.7 of the RAA includes this verification requirement that is narrowly tailored to the purpose of contactability. Registrars are concerned that further collection and processing of personal data (i.e., IDs, passport, photos) is not necessary nor proportionate to achieve contact verification for domain name registration.

We are confident that it is not the intention of the NIS2 drafters, but the requirement of identity verification raises concerns about inhibiting freedom of expression online for European and global citizens. Validation and verification of registration data does not prevent cybercrime in combination with domain names. Rather, the validation and verification in one space only encourages cybercriminals to use other spaces with lower barriers to entry. More authoritative regimes that have taken similar measures in terms of verification and validation, have not stopped cybercrime. In fact the presence of this validation and verification data in breached datasets has provided cybercriminals with the means to weaponize that data for their criminal activities and *bypass* automated validation and verification. Additionally, the requirements of NIS2 could complicate registrars that operate within and outside the EU. EU-based registrars will be required to implement potentially costly processes to comply, whereas registrars outside of the EU (such as the US and Russia) may not be required to implement these processes. This will give non-EU registrars a competitive advantage and potentially increase business for non-EU based companies.

The RAA and other cross-community policy development efforts are the results of the multistakeholder approach to governing the DNS through the ICANN Community and the global stakeholders it represents. Europe has been integral in supporting the multistakeholder model of Internet governance as the best mechanism for maintaining an open, resilient, and secure Internet; recognizing, among other things, that it is informed by a broad foundation of interested parties – including businesses, technical experts, civil society, and governments – arriving at consensus through a bottom-up process regarding policies affecting the underlying functioning of the Internet domain system. We have an overarching concern that Article 23 could be viewed

[9] https://www.icann.org/resources/pages/whois-data-accuracy-2017-06-20-en

as contrary to the multistakeholder model and its principles. Specifically, the RrSG is concerned that European regulation of the processing of registration data will put into question the role of ICANN, the multistakeholder approach to Internet governance. This in turn could encourage other regions and nations seeking to apply their own legal requirements which, collectively, could lead to a fragmented approach to the DNS. From an operational perspective, we are concerned that these laws and regulations will likely run counter to and conflict with one another—as, indeed, they do now—introducing further complexity to the management of the DNS that will ultimately be at the detriment of European and global citizens as companies are forced to comply with myriad regulations.

In conclusion, the RrSG would like to thank the European Parliament again for the opportunity to engage on these issues as NIS2 continues to be developed and considered. We hope these comments prove useful and welcome forthcoming opportunities to discuss these concepts further.

Sincerely,

Ashley Heineman
Chair, RrSG

Relevant RAA sections and ICANN Compliance Activities

Article 23 requires the "entities providing domain name registration services" to:

- collect and maintain accurate and complete domain name registration data in a dedicated database facility with due diligence subject to Union data protection law as regards data which are personal data.
- ensure that the databases of domain name registration data 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.
- have policies and procedures in place to ensure that the databases include accurate and complete information and that such policies and procedures are made publicly available.
- publish, without undue delay after the registration of a domain name, domain registration data which are not personal data.
- 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; reply without undue delay to all requests for access; make policies and procedures to disclose such data publicly available.

As the European Parliament is already aware, Registrars are already required to do much of this: the Registrar Accreditation Agreement (RAA)[10] between ICANN and registrars requires registrars to collect and maintain registrant contact information; the WHOIS Accuracy Program Specification (WAPS)[11] requires verification; and the Temporary Specification for gTLD registration data covers disclosure requirements [12]. Failure to abide by any of these terms results in termination of the registrar's RAA (and, thus, its ability to register generic top-level domain names). Specific requirements include:

- Section 3.7.7.1: The registrant "shall provide to Registrar accurate and reliable contact details and correct and update them within seven (7) days of any change during the term of the Registered Name registration, including: the full name, postal address, e-mail address, voice telephone number, and fax number if available of the Registered Name Holder[13]; name of authorized person for contact purposes in the case of an [sic] Registered Name Holder that is an organization, association, or corporation."
- Section 3.7.7.2: A registrant's "willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration."

[10] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en
[11] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy
[12] https://www.icann.org/resources/pages/gtld-registration-data-specs-en
[13] Registered Name Holder is the registrant (holder) of the domain name.

- Section: 3.7.7.3: “Any Registered Name Holder that intends to license use of a domain name to a third party is nonetheless the Registered Name Holder of record and is responsible for providing its own full contact information and for providing and updating accurate technical and administrative contact information adequate to facilitate timely resolution of any problems that arise in connection with the Registered Name.”
- Section 3.7.8: “Registrar shall comply with the obligations specified in the Whois Accuracy Program Specification. … Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event the Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy.”
- *Inter alia* the WAPS requires:
    - The collection of certain contact information at domain name registration, and confirmation that it meets required formats
    - Confirmation that the registrant’s telephone number and/or email address are operational and contactable
    - When contact information is updated, that its format is confirmed and in certain scenarios confirm that the email address is operational and contactable
    - Take steps to correct contact data if the registrar has any information suggesting that the data is inaccurate, and if the data is not corrected by the registrant, the domain name must be suspended until corrected
- Whois Data Reminder Policy[14]: Requires all registrars to email domain name registrants annually to have them review and confirm that their contact information is accurate (and warn them about the consequences of inaccurate information).
- The Registrants' Benefits and Responsibilities[15] requires registrants to provide “accurate information for publication in directories such as WHOIS, and promptly update this to reflect any changes”, and registrants must respond to requests from registrars within 15 days to keep their domain active.

The ICANN organization has significant resources dedicated to ensuring that domain name contact information is accurate. Some of the initiatives include:

- ICANN Contractual Compliance: Approximately 20 full-time staff[16] providing 24x5 coverage for all registrar and registry compliance. This includes registration data inaccuracy complaints, and between 2016 and 2020, ICANN Contractual Compliance processed over 174,000 complaints.[17] While these numbers appear substantial, they represent a negligible amount of total gTLD domain names (there were 186.6 million gTLD domain names in 2016[18] and 207.4 million in 2020[19])- less than .02% of gTLD domain names annually were the subject of registration data inaccuracy complaints.

[14] https://www.icann.org/resources/pages/registrars/consensus-policies/wdrp-en
[15] https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#registrant
[16] https://www.icann.org/resources/pages/about-2014-10-10-en
[17] Annual data avaialble at https://features.icann.org/compliance/dashboard/report-list
[18] https://www.verisign.com/assets/domain-name-report-Q42016.pdf
[19] https://www.verisign.com/assets/domain-name-report-Q42020.pdf

- WHOIS Accuracy Reporting System (ARS) Project: This initiative sampled registration contact information for accuracy between 2015 and 2018. Inaccurate data was sent to registrars for correction, and systemic problems were the focus of outreach by ICANN to improve accuracy. The results of the final Whois ARS cycle (January 2018) were that:
    - 98% of records had at least one email or telephone number that were operable
    - 99% postal addresses, 60% of telephone numbers, and 92% of email addresses were operable[20]
- Whois Review Teams: ICANN's Bylaws require it to "use commercially reasonable efforts to enforce its policies relating to registration directory services and shall work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data."[21] ICANN conducted reviews in 2010 and 2016, resulting in recommendations for ICANN Board action.
- Accuracy Scoping Team: ICANN's Generic Names Supporting Organization (GNSO) Council, which is responsible for all ICANN policy initiatives, is currently forming an Accuracy Scoping Team. Although the full scope of the team, and any eventual results, are still under consideration by the GNSO Council, this is another commitment by the ICANN Community to ensure registration data is accurate.

[20] https://whois.icann.org/en/whois-ars-phase-2-reporting
[21] https://www.icann.org/resources/reviews/specific-reviews/whois