9 November 2023

Network and Information Systems Cooperation Group Work Stream for art.28 NIS2

RE: ICANN policies, procedures, and requirements relevant to art. 28 NIS2 Directive

Dear Network and Information Systems (NIS) Cooperation Group Work Stream for art.28 members,

In light of the NIS Cooperation Group's responsibilities to ensure cooperation and information exchange among Member States under NIS and the work of the dedicated working group with respect to the implementation of art. 28 of the NIS2 Directive, the Internet Corporation for Assigned Names and Numbers (ICANN) would like to share information about the role and work of the ICANN multistakeholder model and its policymaking, including existing policies, procedures, and requirements that are relevant to art. 28 "Database of domain name registration data" of the NIS2 Directive.

ICANN's mission is to help ensure a stable, secure, and unified global Internet. It does so by coordinating the operation of the Internet's unique identifier systems and especially the Domain Name System (DNS). ICANN follows a multistakeholder approach to policymaking in which individuals, non-commercial stakeholder groups, industry, civil society, the technical community, and governments play important roles. Collectively, they make up the ICANN community, which develops policies for the DNS through a consensus-driven, bottom-up process.

The consensus policies developed through the ICANN multistakeholder community are incorporated into agreements with generic top-level domain (gTLD) registries and ICANN-accredited registrars. ICANN enforces the obligations included in these agreements.

ICANN works closely with gTLD and country code top-level domain (ccTLD) operators to ensure the security and stability of the DNS. Although all TLDs are delegated through ICANN's Internet Assigned Numbers Authority (IANA), ccTLDs are independently managed according to the relevant oversight and governance mechanisms within their respective countries. The ccTLDs, therefore, develop and implement their own policies regarding domain name registration data and are not subject to the ICANN policies.

Involving all interested parties in the policy development process ensures that the ICANN multistakeholder model breeds optimal, inclusive solutions for the DNS, globally applied, which are essential for a stable DNS and a global Internet. In that respect, the ICANN multistakeholder model is paramount to the unified operation of the DNS and as such, is the appropriate place for the

development of policies related to it. Moreover, ICANN policies are not static. They are continually revisited by the ICANN community and evolve to adapt to the changing digital landscape.

It is in that spirit that the NIS2 Directive recognises that "*guidance and the standards developed by the multi-stakeholder governance structures at international level*" should be taken into account to the extent possible as policies and procedures to implement the domain name registration data requirements of NIS2 are considered.

Trust in ICANN's multistakeholder model has been reaffirmed multiple times by EU Member States, including most recently in the Council conclusions on EU Digital Diplomacy of 26 June 2023, referencing "*active support of the Internet Corporation for Assigned Names and Numbers (ICANN) on issues of strategic importance such as ensuring internet stability, security, and interoperability.*"

The multistakeholder model of Internet Governance is the foundation for a secure and interoperable Internet and it has allowed the Internet to flourish. It is recognised by the Tunis Agenda for the Information Society and the EU is a steadfast champion. ICANN's multistakeholder model is a key component of the multistakeholder approach to Internet Governance. As the EU's contribution to the Global Digital Compact (GDC) and accompanying statement notes, "*We strongly support the multistakeholder approach to internet governance, which ensures that all actors, including governments, the private sector, civil society, and technical communities, are involved in shaping the future of the internet. We believe the multistakeholder model is best able to allow for inclusive and consensus based decision making, whereby no actor is dominant or assumes all responsibility for the future development of the internet. A positive example of furthering the multistakeholder approach was the successful IANA stewardship transition to ICANN in 2016. All stakeholders, including governments, are welcome to participate in ICANN and can help increase the security and stability of the global domain name system DNS.*"

Requirements from national legislation that could create conflicts with the rules created within the ICANN ecosystem can pose significant challenges to the registries and registrars. This is particularly apparent in the case of varying interpretations and implementations of art. 28 that could potentially lead to a disparate landscape of national requirements, distinct from ICANN's policies. Such requirements can also pose challenges for the multistakeholder Internet governance model more generally.

We hope you will find the information regarding existing ICANN policies, procedures, and requirements that are relevant to art. 28 provided in the appendix is useful, as you consider matters related to the implementation of the said article of the NIS2 Directive.

We trust that the EU Member States will consider the "*guidance and the standards developed by the multi-stakeholder governance structures at international level*" as they implement the NIS2 Directive and will implement it in a way that preserves and supports the multistakeholder policymaking model and avoids creating a patchwork of national requirements. Furthermore, we hope that the Member States will implement the NIS2 Directive in a way that recognises the uniqueness of ccTLDs to serve their local Internet community (as also highlighted in the Tunis agenda[1]) and the need to preserve that diversity in the interconnected digital ecosystem.

We appreciate your attention to these critical matters and welcome any inquiries or discussion to further clarify ICANN's stance and commitments in these matters.

Sincerely,

Sally Costerton
Interim President and CEO Internet Corporation for Assigned Names and Numbers (ICANN)

Cc: Governmental Advisory Committee (GAC)

[1] para 63. Countries should not be involved in decisions regarding another country's country-code Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanisms.

Appendix 1 - Domain Name Registration Data: ICANN Policies and Agreements and NIS2 Requirements

ICANN has various policies and agreements in place regarding domain name registration data. These encompass matters ranging from registration, maintenance of, and access to accurate and up-to-date information concerning Registered Names and name servers, to escrow and auditing. Some relevant ICANN policies and agreements are:

- Registrar Accreditation Agreement (RAA) (2013), including;
  - Data Retention Specification;
  - RDDS Accuracy Program Specification
- The Temporary Specification for gTLD Registration Data (Temporary Specification) (2018), which established temporary requirements to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR
- Interim Registration Data Policy for gTLDs (Interim Policy)(2019), which requires registries and registrars to continue to implement measures that are consistent with the Temporary Specification for gTLD Registration Data, until the Registration Data Policy (below) goes into effect.;
- Base Registry Agreement (2023)
- Registration Data Policy for gTLDs (upcoming) is set to replace the Temporary Specification upon its effective date. Although it largely reaffirms the requirements established by the Temporary Specifications, it nonetheless introduces significant changes and reductions in the amount of personal data collected, transferred, and published compared to the Temporary Specification, in line with the data minimization principle and data necessary to fulfill the purpose for which the data is collected. The policy is pending publication and will become effective 18 months after its publication.

ICANN Contractual Compliance ("Compliance") enforces the policies developed by the community and incorporated into ICANN's agreements with gTLD registries and registrars. Compliance ensures these obligations are implemented to preserve and enhance the security, stability, and resiliency of the DNS. Compliance undertakes enforcement actions resulting from complaints received from external users, proactive monitoring, and audit-related activities. Contracted parties that fail to cure breaches of their obligations are subject to remedies up to and including termination.

The NIS2 Directive establishes obligations about registration data collection, maintenance, and disclosure "for the purpose of contributing to the security, stability and resilience of the DNS," "which in turn contributes to a high common level of cybersecurity within the Union." It applies to both ccTLD and gTLD name registries and entities providing domain name registration services (registries and registrars) that are established in the EU or offer services in the EU.

Below, you will find a comprehensive overview of policies and agreements developed by ICANN's multistakeholder model, both implemented and in preparation. They are laid out by topic in reference to the NIS2 Directive Requirements.

1. Data collection and publication

According to NIS2 Art. 28(1), EU Member States' laws implementing NIS2 shall require registries and registrars to collect and maintain accurate and complete domain name registration data in a dedicated database in accordance with the GDPR.

ICANN agreements and policies, such as the Registrar Accreditation Agreement (RAA), already require gTLD registrars to collect a variety of data concerning domain name registrants. Indeed, Clause 3.4.1 of the RAA requires that "for each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain, in its own electronic database, as updated from time to time." Additionally, ICANN's Interim Registration Data Policy for gTLDs (Interim Policy), establishes temporary requirements to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR, primarily by limiting the publication of personal registration data.

Furthermore, ICANN org is in the process of implementing a new Registration Data Policy for gTLDs recommended by the ICANN community via the bottom-up, multistakeholder policy development process, as part of an effort to bring requirements concerning registrars' and registries' processing of registrants' contact data ("registration data") into compliance with data protection laws, including the GDPR. The Registration Data Policy reduced the amount of personal registration data that would be required to be collected and processed for each domain name registration through the introduction of a minimum data set that can be added to as needed based on appropriate legal basis and data processing arrangements.

a. Data fields collected

According to NIS2 Art. 28(2), data to be collected shall include: domain name, date of registration, registrant's name, contact email address and telephone number, the contact email address, and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.

Art. 3.4.1 of the RAA specifies that for each registered name sponsored by the registrar within a gTLD, the registrar shall collect and securely maintain, in its own electronic database:

(a) The data specified in the Data Retention Specification to the RAA including, of relevance to NIS2 implementation, the following data:

i. The first and last name or full legal name of the registrant;
ii. The first and last name or, in the event the registrant is a legal person, the title of the registrant's administrative contact, technical contact, and billing contact;
iii. The postal address of the registrant, administrative contact, technical contact, and billing contact;
iv. Telephone contact for registrant, administrative contact, technical contact, and billing contact.

(b) The name, postal address, email address, and voice telephone number provided by the customer of any privacy service or any proxy registration service, in each case, offered or made available by the registrar or its affiliates in connection with each registration.

The new Registration Data Policy is expected to be finalized in 2023 (with an effective date to be determined). This new policy will reduce the amount of "Registration Data" that registrars must collect from registrants. Under the new Policy, the registrars will be required to collect:

(a) Domain name
(b) Registrant name
(c) Registrant postal address (including country)
(d) Registrant email
(e) Registrant telephone number

The new Registration Data Policy will permit, but not require, registrars to collect the following additional data elements:

(a) Registrant telephone number extension
(b) Registrant fax number
(c) Technical contact
(d) Technical contact telephone number
(e) Technical contact email address

The new policy also permits registrars to collect additional data elements as required by the registry-registrar agreements, the registry operator's registration policy, and for the registrars' own business purposes (which may include data the registrar must collect if required by applicable law).

b. Data publication and personal data protection (including distinction of natural vs legal person)

According to NIS2 Art. 28(4), EU Member States' laws implementing NIS2 shall require registries and registrars to make publicly available, without undue delay after the registration of a domain name, the domain name registration data that are not personal data.

Furthermore, NIS2 recital (112) states that "For legal persons, the TLD name registries and the entities providing domain name registration services should make publicly available at least the name of the registrant and the contact telephone number. The contact email address should also be published, provided that it does not contain any personal data, such as in the case of email aliases or functional accounts."

Consistent with ICANN's stated objective to comply with the GDPR, while maintaining the existing WHOIS system to the greatest extent possible, the Temporary Specification (applicable through the Interim Policy) maintains robust collection of registration data (including registrant, administrative, and technical contact information), but restricts publication of personal data.

Specifically, the Temporary Specification (Appendix A) requires that contracted parties whose processing of registration data is within the scope of the GDPR must redact much of the registration data set out above from public access. In addition, all other contracted parties may redact this data from public access where they have a commercially reasonable purpose to do so, or where it is not technically feasible to limit application of the redaction requirements to registration data processing that is within the scope of the GDPR. The specific fields that may (or MUST, depending on the circumstances) be redacted, unless the registrant or relevant contact has provided consent, are:

(a) Registry Registrant ID
(b) Registrant Name
(c) Registrant Street
(d) Registrant City
(e) Registrant Postal Code
(f) Registrant Phone
(g) Registrant Phone Ext
(h) Registrant Fax
(i) Registrant Fax Ext
(j) Registry Admin/Tech/Other ID
(k) Admin/Tech/Other Name
(l) Admin/Tech/Other Organization
(m) Admin/Tech/Other Street
(n) Admin/Tech/Other City
(o) Admin/Tech/Other Phone
(p) Admin/Tech/Other Phone Ext
(q) Admin/Tech/Other Fax
(r) Admin/Tech/Other Fax Ext

In responses to WHOIS queries, in the value of the “email” field of every contact (registrant, admin, technical), the registrar must provide an email address or web form to facilitate email communication with the relevant contact, but must not identify the contact email address or the contact itself.

These WHOIS redaction requirements do not distinguish between the registration data of legal and natural persons. The ICANN community has developed guidelines for how to facilitate making the distinction for those registries and registrars who choose to, but in light of the potential risks involved in making this distinction, it is not, as a matter of ICANN policy, a requirement.

The new Registration Data Policy will require registries and registrars to publish the following data elements in response to RDDS/WHOIS queries (items marked with an asterisk* are required to be published only if the contracted party collects, transfers, or generates the data element):

(a) Domain name
(b) Registrar URL
(c) Creation date
(d) Registry expiration date
(e) Registrar registration expiration date
(f) Registrar
(g) Registrar IANA ID
(h) Registrar abuse contact email
(i) Registrar abuse contact phone
(j) Domain status(es)
(k) Last update of RDDS
(l) Registrar WHOIS Server*
(m) Updated date*
(n) Name Server*
(o) DNSSEC elements*
(p) Registry domain ID*
(q) Registry registrant ID*
(r) Registrant organization*
(s) Registrant postal code*
(t) Registrant state/province*
(u) Registrant country*
(v) Registry tech ID*
(w) Tech name*
(x) Tech phone*
(y) Tech email*

The Registration Data Policy will require the registrars and registries to redact the data fields immediately below from public RDDS/WHOIS access if this is required to comply with applicable laws. Contracted parties may in other circumstances elect to redact these data elements even if applicable law does not require redaction. In determining whether or not to redact these data elements, the contracted parties may, but are not required to, consider whether the registration data pertains to a legal person and the geographic location of the registrant or relevant contact.

(a) Registry domain ID
(b) Registry registrant ID
(c) Registrant name
(d) Registrant street
(e) Registrant postal code
(f) Registrant phone
(g) Registrant phone ext
(h) Registrant fax
(i) Registrant fax ext
(j) Registrant email
(k) Registry tech ID
(l) Tech name
(m) Tech phone
(n) Tech email

As under the Temporary Specification/Interim Policy, the registrar must publish an email address or a link to a web form to facilitate email communication with the relevant contact when the email address is redacted from public RDDS/WHOIS.

The Registration Data Policy will require registrars to give the registrant the opportunity to consent to the publication of their registration data in the public WHOIS/RDDS.

2. <u>Data access</u>

According to Art. 28(5) of the NIS2 Directive, “Member States shall require the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with Union data protection law. Member States shall require the TLD name registries and the entities providing domain name registration services to reply without undue delay and in any event within 72 hours of receipt of any requests for access. Member States shall require policies and procedures with regard to the disclosure of such data to be made publicly available.”

Rectial 112 further adds that “Those policies and procedures should take into account, to the extent possible, any guidance and the standards developed by the multi-stakeholder governance structures at international level. The access procedure could include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonized practices across the internal market, the Commission can, without prejudice to the competences of the European Data Protection Board, provide guidelines with regard to such procedures, which take into account, to the extent possible, the standards developed by the multi-stakeholder governance structures at international level. Member States should ensure that all types of access to personal and non-personal domain name registration data are free of charge.”

ICANN’s contractual requirements and community-developed policies already establish principles and conditions regarding access to domain name registration data collected by registrars from registrants. This includes the specific access needed by data escrow agents, as outlined in the RAA Section 3.6, where registrars must transfer domain name registration data to "a reputable data escrow agent." Additionally, for thick registries, registrars are obligated to transfer registration data to registries with "thick" entries. Thick registries are registries who maintain the registrant’s contact information and designated administrative and technical contact information, in addition to the sponsoring registrar and registration status information supplied by a thin registry, while thin registries only include technical data sufficient to identify the sponsoring registrar, status of the registration, and creation and expiration dates for each registration in its WHOIS data store.

ICANN may also require registries and registrars to transfer data for compliance enforcement and audits, but this is specific to compliance inquiries related to identified domain names, not bulk transfers. Furthermore, WHOIS data access requirements mandate that registrars and registries provide public access to a subset of the collected registration data in their Registration Data Directory Services (RDDS), often referred to as "WHOIS."

a. Third-Party Access to Redacted Registration Data (including legal basis)

According to NIS2 art. 28(5), registries and registrars shall provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with EU data protection law, without undue delay and in any event within 72 hours of receipt of any requests for access.

In accordance with the currently applicable Interim Policy (and Temporary Specification, Appendix A, Section 4), when Registration Data is redacted from public RDDS/WHOIS, contracted parties are required to grant reasonable access to personal data within the registration data to third parties, based on legitimate interests pursued by the third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the registered name holder or data subject, as outlined in Art. 6(1)(f) of the GDPR.

The new Registration Data Policy will update the Temporary Specification's requirements concerning registrars' responses to requests from third parties for access to redacted registration data. The new policy will require the contracted parties to each publish their process for responding to requests for lawful disclosure to redacted registration data. This must set out the contracted party's criteria for the contents of requests for registration data access, and the anticipated timeline for responses.

b. Portal for requesting nonpublic gTLD registration data

According to NIS2 Recital 112, the access procedure (to registration data) could include the use of an interface, portal, or other technical tool to provide an efficient system for requesting and accessing registration data.

ICANN is currently working on developing the Registration Data Request Service (RDRS), a free and global proof of concept service that will handle requests for access to nonpublic registration data related to generic top-level domains (gTLD). It will connect requestors seeking disclosure of nonpublic registration data with the relevant ICANN-accredited registrars for gTLD domain names who are participating in the service. The service will streamline and standardize the process for submitting and receiving requests through a single platform.

The service may evolve into a permanent tool that will continue to connect data requestors and data holders by gathering usage and demand data. The ICANN Board has requested up to two years of operational data to determine next steps.

The RDRS will not guarantee access to the registration data, as that remains a decision of the data controller, in this case the registrar, and all communication and data disclosure between the registrars and requestors will take place outside of the system.

The RDRS is expected to launch in November 2023. Any updates to the timeline will be made public.

Legal basis for processing of registration data

The legal basis for processing registration data, including disclosure of data, is defined under GDPR 6(1)f. In this context, data controllers such as registries and registrars, evaluate the legitimate interest of the requestors against the privacy rights of registrants.

According to NIS2 Recital 109, "maintaining accurate and complete databases of domain name registration data (WHOIS data) and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity across the Union. For that specific purpose, TLD name registries and entities providing

domain name registration services should be required to process certain data necessary to achieve that purpose. Such processing should constitute a legal obligation within the meaning of Article 6(1), point (c), of Regulation (EU) 2016/679. That obligation is without prejudice to the possibility to collect domain name registration data for other purposes, for example on the basis of contractual arrangements or legal requirements established in other EU Union or national law."

It would be a welcome development to have the option of relying on 6(1)c of the GDPR as a legal basis for processing registration data, including disclosure of this data, as long as data controllers are permitted to do so. The NIS2 Directive acknowledges the use of GDPR 6(1)c for the specific purpose of "ensuring the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity across the Union" and for "legitimate access seekers" who "are to be understood as any natural or legal person making a request pursuant to Union or national law" (Recital 121). They can include authorities that are "competent under this Directive and those that are competent under Union or national law for the prevention, investigation, detection or prosecution of criminal offenses, and CERTs or CSIRTs." (Recital 110).

3. Data duplication (Thick vs. Thin WHOIS)

According to NIS2 Directive Recital 109, "TLD name registries and entities providing domain name registration services should be required to process certain data [*registration data*] necessary to achieve that purpose. Such processing should constitute a legal obligation within the meaning of Art. 6(1), point (c), of Regulation (EU) 2016/679. [...] That obligation aims to achieve a complete and accurate set of registration data and should not result in collecting the same data multiple times. The TLD name registries and the entities providing domain name registration services should cooperate with each other in order to avoid the duplication of that task."

NIS2 Art. 28(6) and Recital 109 further add that the obligation to process certain necessary (while complete and accurate) domain name registration data "should not result in collecting the same data multiple times."

As noted above, thick registries are registries that maintain the registrant's contact information and designated administrative and technical contact information, in addition to the sponsoring registrar and registration status information supplied by a thin registry. A thick registry requires the registrar to transfer the names, phone numbers, email addresses and mailing addresses of the registrant, technical contact and administrative contact for each domain name registration. Thin registries only maintain technical data sufficient to identify the sponsoring registrar, status of the registration, and creation and expiration dates for each registration in its WHOIS data store.

The ICANN multistakeholder community adopted on 7 February 2014 a policy that would require all registries to be "thick" (see Thick WHOIS Transition Policy). However, the ICANN Board determined in its Resolution, dated 7 November 2019, to defer contractual compliance enforcement of this policy pending further work, including work in furtherance of implementing the new Registration Data Policy.

Under the draft Registration Data Policy, the decision regarding whether a registry will receive the "thick" data or not will depend on the registry and registrar determining the legal basis for the transfer (including that a legitimate purpose exists for the transfer which is not outweighed by the registrant's interests under applicable data protection law) and entering into a data protection agreement that covers the data, where such an agreement is required by law. ICANN would enforce a transfer requirement only if the relevant contracted parties agree that a legal basis exists for the transfer and that a data protection agreement is in place.

4. Data accuracy and verification procedures

According to Art. 28(3) of the NIS2 Directive, "Member States shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the databases referred to in paragraph 1 include accurate and complete information. Member States shall require such policies and procedures to be made publicly available."

The term "accuracy" is not defined in the NIS2 Directive nor are the "verification procedures" mentioned in Art. 28(3).

Recital 111 sets out comparatively specific and dynamic requirements regarding verification obligations. Verification processes of TLD registries and the entities providing domain name registration services "should reflect the current best practices used within the industry and, to the extent possible, the progress being made in the field of electronic identification." This recital also provides general examples of verification processes, which "may include both ex ante controls, performed at the time of the registration, and ex post controls, performed after the registration." In particular, TLD registries and the entities providing domain name registration services are required to verify at least one means of contact of the registrant.

The RAA RDDS Accuracy Program Specification requires that registrars validate, inter alia, that email addresses (Section 1(b)), telephone numbers (Section 1(c)), and postal addresses (Section 1(d)) are in the proper format. The Specification also requires registrars to verify that either the registrant's email address (Section 1(f)(i)) or telephone number (Section 1(f)Iii) are operable. Additionally, the RAA requires that upon being notified of an inaccuracy in contact information associated with a domain name, registrars take reasonable steps to investigate and, where applicable, correct the inaccuracy.

Compliance undertakes enforcement of these requirements through actions resulting from complaints received from external users, proactive monitoring, and audit-related activities.

Upon receiving a complaint alleging a registration data inaccuracy, Compliance confirms that:

- The complaint is within ICANN's contractual scope (e.g., it refers to a matter addressed by an ICANN policy or agreement and to a party over which ICANN org has enforcement authority).
- The complainant provides evidence of the claimed inaccuracy (e.g., a bounce-back or returned "undeliverable" email or post) or the inaccuracy is evident in the RDDS/WHOIS (e.g., the telephone number listed is "123").

Once a complaint is confirmed, Compliance initiates an investigation into the registrar's compliance with the contractual requirements explained above, including the obligation to take reasonable steps to investigate the claimed inaccuracy.

The "reasonability" of the steps will depend on the type of inaccuracy reported. For example, a report of a nonfunctional email address may only require the registrar to perform email verification to ensure the email is functioning. However, if the complaint is about identity (e.g., the registrant is not who they say they are), Compliance may ask the registrar to provide further information concerning its findings and the results of its investigation specific to the facts of the complaint.

Compliance will typically close an inaccuracy case when the registrar demonstrates compliance with the investigation and validation or verification requirements, which may include the suspension or cancellation of the domain name registration. The registrar's failure to demonstrate compliance results in escalation through the Contractual Compliance process, which may include the issuance of a public breach notice and that may also result in the suspension or termination of the registrar's RAA.[2]

Compliance enforcement of these contractual requirements also includes regular registrar audits, which collect information to (1) determine whether registrars are complying with registration data validation and verification requirements, and (2) address identified instances of non-compliance with the RDDS Accuracy Program Specification requirements to validate and verify contact information, and to take action in the event that a registrar fails to remediate an identified deficiency. Specifically, Compliance confirms that the registrar performed verification of the required registration data, and is maintaining records required to demonstrate the actions taken and results obtained, for a sample of 15 randomly selected domain names by the auditor. For each of the sampled domain names, Compliance validates

[2] Prior to the Temporary Specification and impacts of GDPR, which resulted in the obfuscation of much of the publicly available gTLD WHOIS contact data, ICANN used to conduct proactive checks through the "WHOIS Accuracy Reporting System" (ARS). The ARS aimed to identify potentially inaccurate contact data in public databases. Compliance received referral cases from the ARS and initiated investigations with gTLD Registrars in the manner described above. ARS was placed and remains on pause to consider the impact of data protection laws and community efforts concerning accuracy.

that the required verification email was sent within 15 days of the registration, transfer, or change in Registered Name Holder (RNH) information and shows a confirmed verification by the RNH within 15 days of receiving the verification email from the registrar.

The audit team also inquires registrars about their processes for registration data validation during initial registration, inbound transfer, or any change of registrant's information. The audit team reviews the responses and determines if validation techniques are adequate and compliant with the RAA, particularly the application of RAA-specific standards and templates regarding the address and phone number.

The ICANN community is currently considering whether additional policy development work concerning registration data accuracy should be explored.

Appendix 2 - Comparative table of NIS2 provisions and relevant ICANN Policies and Agreements

	References in the NIS2 Directive	Relevant ICANN policies and agreements
Data collection	- NIS2 Art. 28(1) requires registries and registrars to collect and maintain accurate and complete domain name registration data in a dedicated database. - NIS2 Art 28(2) states that data to be collected shall include: domain name, date of registration, registrant's name, contact email address and telephone number, the contact email address and telephone number of the point of contact administering the domain name in the event that they are different from those of the registrant.	- Clause 3.4.1 of the Registrar Accreditation Agreement (RAA) "For each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain, in its own electronic database, as updated from time to time." - Data Retention Specification to the RAA - Registration Data Policy (upcoming) requires registries and registrars to publish the following data elements in response to RDDS/WHOIS queries (items marked with an asterisk* are required to be published only if the contracted party collects, transfers, or generates the data element): (a) Domain name (b) Registrar URL (c) Creation date (d) Registry expiration date (e) Registrar registration expiration date (f) Registrar (g) Registrar IANA ID (h) Registrar abuse contact email (i) Registrar abuse contact phone (j) Domain status(es) (k) Last update of RDDS (l) Registrar WHOIS Server* (m) Updated date* (n) Name Server* (o) DNSSEC elements* (p) Registry domain ID*

		(q) Registry registrant ID* (r) Registrant organization* (s) Registrant postal code* (t) Registrant state/province* (u) Registrant country* (v) Registry tech ID* (w) Tech name* (x) Tech phone* (y) Tech email*
Data publication and personal data protection (including distinction of natural vs legal person)	- NIS2 Art. 28(4), EU Member States' laws implementing NIS2 shall require registries and registrars to make publicly available, without undue delay after the registration of a domain name, the domain name registration data which are not personal data. - NIS2 recital (112) states that "For legal persons, the TLD name registries and the entities providing domain name registration services should make publicly available at least the name of the registrant and the contact telephone number. The contact email address should also be published, provided that it does not contain any personal data, such as in the case of email aliases or functional accounts.	- Interim Registration Data Policy for gTLDs (Interim Policy), which requires registries and registrars to continue to implement measures that are consistent with the Temporary Specification for gTLD Registration Data *For context:* - Temporary Specification for gTLD Registration Data establishes temporary requirements to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR. - Temporary Specification (at Appendix A) requires that contracted parties whose processing of registration data is within the scope of the GDPR must redact much of the registration data set out above from public access. - Registration Data Policy (upcoming) will require the registrars and registries to redact the data fields immediately below from public RDDS/WHOIS access if this is required to comply with applicable laws.

Data access	- NIS2 Art. 28(5): "Member States shall require the TLD name registries and the entities providing domain name registration services to provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with Union data protection law. Member States shall require the TLD name registries and the entities providing domain name registration services to reply without undue delay and in any event within 72 hours of receipt of any requests for access. Member States shall require policies and procedures with regard to the disclosure of such data to be made publicly available." - NIS2 Rectial 112: "Those policies and procedures should take into account, to the extent possible, any guidance and the standards developed by the multi-stakeholder governance structures at international level. The access procedure could include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission can, without prejudice to the competences of the European Data Protection Board, provide guidelines with regard to such procedures, which take into account, to the extent possible, the standards developed by the multi-stakeholder governance structures at international level. Member States should ensure that all types of access to personal and non-personal domain name registration data are free of	- Registrar Accreditation Agreement (RAA) Section 3.6: Specific access needed by data escrow agents, as outlined in the RAA. - ICANN's Temporary Specification for gTLD Registration Data sets out requirements that enable ICANN, gTLD registry operators, and registrars to maintain compliance with existing ICANN contractual requirements and community-developed policies in the context of GDPR.

	charge.”	
Third-Party Access to Redacted Registration Data (incl. legal basis)	- NIS2, Art. 28(5): Registries and registrars shall provide access to specific domain name registration data upon lawful and duly substantiated requests by legitimate access seekers, in accordance with EU data protection law, without undue delay and in any event within 72 hours of receipt of any requests for access. - NIS2, recital 110: Description of “legitimate access seekers”	- Temporary Specification, Appendix A, Section 4: When registration data is redacted from public RDDS/WHOIS, contracted parties are required to grant reasonable access to personal data within the registration data to third parties, based on legitimate interests pursued by the third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the Registered Name Holder or data subject, as outlined in Article 6(1)(f) of the GDPR. - The Registration Data Policy (upcoming) will update the Temporary Specification’s requirements concerning registrars’ responses to requests from third parties for access to redacted registration data. The new policy will require the contracted parties to publish and implement a process for responding to requests for lawful disclosure to redacted registration data. This must set out the contracted parties’ criteria for the contents of requests for registration data access, and the anticipated timeline for responses.
Portal or other technical tool	- NIS2 Recital 112: The access procedure (to registration data) could include the use of an interface, portal, or other technical tool to provide an efficient system for requesting and accessing registration data.	- Registration Data Request Service (RDRS): a free and global service that will handle requests for access to nonpublic registration data related to generic top-level domains (gTLD)s.
Legal basis for processing of registration data	- NIS2 Recital 109: “Maintaining accurate and complete databases of domain name registration data (WHOIS data) and providing lawful access to such data is essential to ensure the security, stability,	- RDDS Accuracy Program Specification

	and resilience of the DNS, which in turn contributes to a high common level of cybersecurity across the Union. For that specific purpose, TLD name registries and entities providing domain name registration services should be required to process certain data necessary to achieve that purpose. Such processing should constitute a legal obligation within the meaning of Article 6(1), point (c), of Regulation (EU) 2016/679. That obligation is without prejudice to the possibility to collect domain name registration data for other purposes, for example on the basis of contractual arrangements or legal requirements established in other Union or national law." - Recital 121: "The processing of personal data, to the extent necessary and proportionate for the purpose of ensuring security of network and information systems by essential and important entities, could be considered to be lawful on the basis that such processing complies with a legal obligation to which the controller is subject, in accordance with the requirements of Article 6(1), point (c), and Article 6(3) of Regulation (EU) 2016/679. Processing of personal data could also be necessary for legitimate interests pursued by essential and important entities, as well as providers of security technologies and services acting on behalf of those entities, pursuant to Article 6(1), point (f), of Regulation (EU) 2016/679, including where such processing is necessary for cybersecurity information-sharing arrangements or the voluntary notification	

	of relevant information in accordance with this Directive."	
Data duplication	- Rectital 109 NIS2: "TLD name registries and entities providing domain name registration services should be required to process certain data [*registration data*] necessary to achieve that purpose. Such processing should constitute a legal obligation within the meaning of Article 6(1), point (c), of Regulation (EU) 2016/679. [...] That obligation aims to achieve a complete and accurate set of registration data and should not result in collecting the same data multiple times. The TLD name registries and the entities providing domain name registration services should cooperate with each other in order to avoid the duplication of that task." - NIS2 Art. 28(6) and recital 109 further add that the obligation to process certain necessary (while complete and accurate) domain name registration data "should not result in collecting the same data multiple times." - Recital 14 NIS2: "Union data protection law and Union privacy law applies to any processing of personal data under this Directive. In particular, this Directive is without prejudice to Regulation (EU) 2016/679"	- Registration Data Policy: The decision regarding whether a registry will receive the "thick" data or not will depend on the registry and registrar determining the legal basis for the transfer (including that a legitimate purpose exists for the transfer that is not outweighed by the registrant's interests under applicable data protection law) and entering into a data protection agreement that covers the data, where such an agreement is required by law.
Data accuracy and verifications procedures	- Art. 28(3) NIS2: "Member States shall require the TLD name registries and the entities providing domain name registration services to have policies and procedures, including verification procedures, in place to ensure that the	- RAA's RDDS Accuracy Program Specification requires that registrars validate, inter alia, that email addresses (Section 1(b)), telephone numbers (Section 1(c)), and postal addresses (Section 1(d)) are in the proper format. The specification

	databases referred to in paragraph 1 include accurate and complete information. Member States shall require such policies and procedures to be made publicly available." - Recital 111 NIS2 "The TLD name registries and the entities providing domain name registration services should adopt and implement proportionate procedures to verify domain name registration data. Those procedures should reflect the best practices used within the industry and, to the extent possible, the progress made in the field of electronic identification. Examples of verification procedures may include ex ante controls carried out at the time of the registration and ex post controls carried out after the registration. The TLD name registries and the entities providing domain name registration services should, in particular, verify at least one means of contact of the registrant."	also requires registrars to verify that either the registrant's email address (Section 1(f)(i)) or telephone number (Section 1(f)Iii) are operable.