RySG
gTLD Registries
Stakeholder Group

Comments of the gTLD Registries Stakeholder Group (RySG) on the Revised Directive on Security of Network and Information Systems (NIS2)

The gTLD Registries Stakeholder Group (RySG) represents the interests of generic top-level domain (gTLD) registries. The RySG is an established stakeholder group within the Internet Corporation for Assigned Names and Numbers (ICANN) community and our membership comprises organizations that operate gTLDs under contract with ICANN.

We appreciate the opportunity to offer our input on the NIS2 proposal currently being considered by the European Parliament. While we respect and support the overall aim of the NIS2 directive to achieve a high common level of cybersecurity across the EU member states, we have specific concerns with the requirements proposed under Article 23 (and the related recitals) as they apply to gTLD Registry Operators. We ask that the Parliament review the following information and consider revising Article 23 and the related recitals to:

1. Reflect the different role that gTLD Registries play as compared to Registrars and other entities providing domain registration services;
2. Differentiate between requirements for gTLD Registries and the other parties;
3. Avoid imposing additional requirements on gTLD Registries, such as data verification, which are inappropriate to their role;
4. Avoid imposing additional requirements on Registrants (those persons or entities who wish to obtain and use a domain name), which may have a significant cooling effect on registrations, in effect raising the barrier to entry for many holding legitimate uses; and
5. Avoid overlap and conflicts with requirements that have already been established through ICANN's policy development process, which apply directly to all gTLD Registries, as well as existing EU legislation.

1. The Domain Name Registration Process in gTLDs

This section provides an overview of the process by which domain names are registered in generic top-level domains, or gTLDs, as well as the distinct roles that gTLD Registry Operators ("gTLD Registries") and ICANN-accredited Registrars ("Registrars") play in this system.

gTLD Registries are contracted with ICANN, who designates each gTLD Registry as the **Registry Operator** for the applicable gTLD(s), thereby authorizing the gTLD Registry Operator to maintain the authoritative records of domain names registered in their gTLD(s), and to perform other "Registry Services" for the gTLD(s), including the operation of the registry DNS servers. Registry Operators may provide all of the "Registry Services" themselves or may enter into contracts with **Registry Service Providers (RSPs)** to provide one or more of those services. RSPs do not have contracts with ICANN.

Domain names in gTLDs are registered via **Registrars**, who are accredited by ICANN and enter into separate contracts with gTLD Registries authorizing the Registrar to provide domain name registrations in the gTLD Registry's specific gTLD(s).

Although Registrars are the only entities authorized by ICANN and the gTLD Registries to register domain names in gTLDs, **Resellers**, which are organizations that are affiliated or under contract with Registrars, often sell domain name registrations to end-users that are then registered in the gTLDs by an authorized Registrar.

Due to their distinct roles in the process of registering a domain name, as described above, Registrars have a business relationship with the individuals or organizations that register domain names (known as Registrants), either directly or through their licensed resellers. By contrast, the vast majority of gTLD Registries, with few exceptions, have no relationship with Registrants and only conduct business with Registrars. **We urge the Parliament to consider adjusting Article 23 to reflect this difference in relationship with the domain name registrant, as well as to account for the ICANN policies that already apply to gTLD Registries (more detail to follow).** The requirements as currently written would appear to apply equally to all TLD registries, including gTLD Registries, as they do to Registrars; we believe a more nuanced and differentiated approach would align better with the realities of the domain name registration process in the gTLD space and achieve the stated goals of the NIS2 Directive.

There are approximately 1,200 gTLDs operated by nearly 500 gTLD Registry Operators under a variety of business models. These gTLDs generally fall into the following categories:

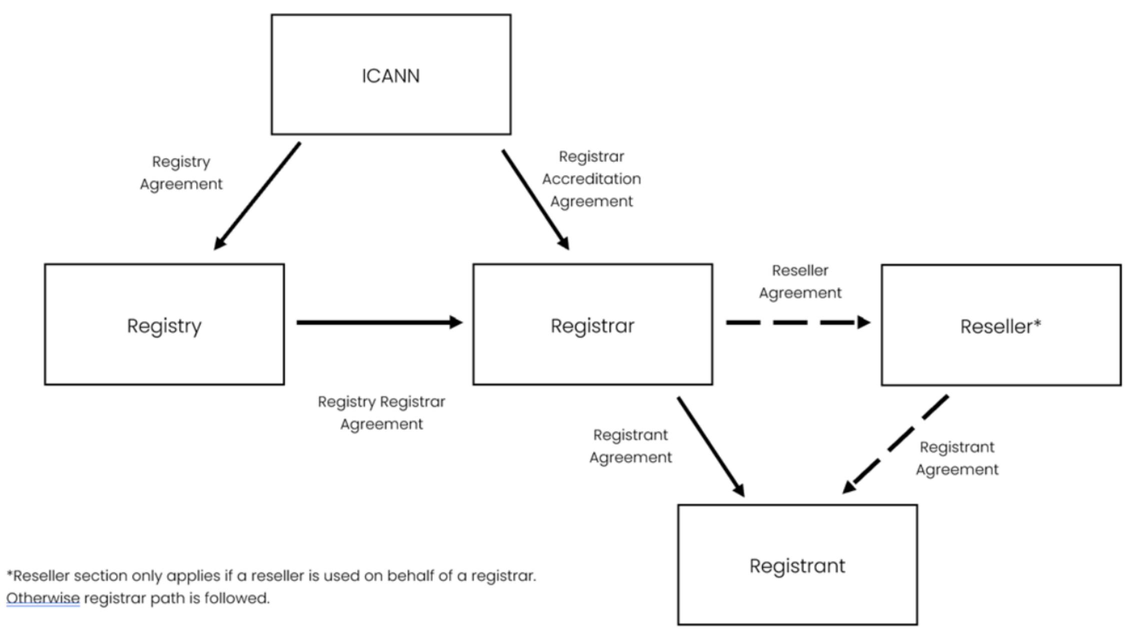
- **Open gTLDs**: These gTLDs have no eligibility requirements or restrictions and are available to all domain name Registrants via Registrars (or resellers).
- **Restricted or Validated gTLDs**: These gTLDs have registrant eligibility requirements set out in their contracts and/or registry policies. There are a variety of processes used by different restricted gTLD Registries to determine registrant eligibility. Some Registries require Registrants to establish that they meet criteria before being able to register a domain name in their space. Other Registries review eligibility requirements after a domain has been registered but before it is activated. Still others review eligibility after a domain has been registered and is live and suspend the domain if criteria are not met. The Registry may conduct verifications itself or rely on the Registrar or another third-party company to perform verification of the Registrants of domain names.
- **Brand gTLDs**: These gTLDs exactly match a qualifying registered trademark and, under the terms of their contract with ICANN, restrict registrations to the corresponding brand owner itself and its group companies and trademark licensees. Brand gTLDs, also

known as dotBrands, are not publicly available for registration and these Registry Operators do not sell or allocate domain names to unconnected third parties outside of this limited corporate or contractual nexus. As such, whilst the Brand gTLD may serve to deliver important internal infrastructure for a brand owner, the operation of a Brand gTLD is not the provision of critical third-party infrastructure of the type NIS2 intends to protect

While we agree that a secure, stable and resilient DNS plays a key role in the overall integrity of the Internet, we also wish to point out that not all gTLDs qualify as critical infrastructure. **To ensure measures do not go beyond what is necessary to meet the specific objectives and avoid any disproportionate effects, we ask the policymakers to consider restricting the scope of the NIS2 Directive, as it relates to providers of DNS services, only to those that serve to provide essential services to key sectors.**

2. Contractual Framework between gTLD Registries, Registrars and ICANN

Regardless of business model or structure, all gTLD Registries and ICANN-accredited Registrars operate within a series of agreements. The Registry Agreement (RA), between a Registry Operator and ICANN; the Registrar Accreditation Agreement (RAA), between a Registrar and ICANN; and the Registry-Registrar Agreement (RAA), between the gTLD Registry and the Registrar. Each of these agreements sets out the roles and responsibilities of each party in maintaining certain technical and policy standards to ensure the continued stable, secure, interoperable functioning of the DNS.



The **gTLD Registry Agreement (RA)** sets out the responsibilities and requirements for each gTLD Registry Operator and defines the relationship between the gTLD Registry and ICANN. Specifically, it sets out registration data and registry performance specifications[1] as well as data processing, publication, and redaction requirements[2]. These specifications and requirements collectively define what constitutes the "complete" set of domain name registration data that the gTLD Registry must maintain in order to support the secure and stable functioning of the Domain Name System.

The **Registrar Accreditation Agreement (RAA**) defines the requirements each Registrar must implement to become an ICANN-Accredited Registrar. Each ICANN-Accredited Registrar must adhere to the standards in the RAA to register, transfer, and maintain domain names in gTLDs in a stable, interoperable manner. Similar to the RA, the RAA contains specifications and requirements that define what "complete" set of domain name registration data that the Registrar must collect and maintain in order to support the secure and stable functioning of the Domain Name System. The RAA also includes requirements for Registrars to routinely validate the data they collect to ensure accuracy.

The **Registry-Registrar Agreement (RRA**) exists between a gTLD Registry and an ICANN-Accredited Registrar and defines the technical and data processing responsibilities of each party.

3. The Role of ICANN Consensus Policy

The agreements that exist between ICANN and gTLD Registries and Registrars are unique in that they require gTLD Registries and Registrars to automatically incorporate and comply with Consensus Policies[3] developed by ICANN's multistakeholder community through a defined policy development process (PDP). These obligations are in addition to the terms of their contractual agreements with ICANN (the RA and RAA, described above).

All of this exists within the multistakeholder model of Internet governance that ICANN supports by coordinating the secure, stable, operations of the DNS. The multistakeholder model reflects the structure of the Internet – it is open, distributed, and bottom-up in its processes. The ICANN multistakeholder model allows the ICANN community to address issues like privacy and security in a flexible manner that incorporates input from across the community (technical, governments, end-users, contracted parties, etc.) to craft policy that is tailored to the needs of the global DNS. The benefit of global policy making is that it enables a single interoperable DNS and mitigates the risk of a fragmented internet.

[1] See Base gTLD Agreement Specification 10, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf
[2] Base gTLD Agreement Section 2.5, Specification 4, Temporary Specification for gTLD Data
[3] https://www.icann.org/resources/pages/registrars/consensus-policies-en

The terms and requirements of NIS2 as drafted, particularly Article 23, align significantly with existing ICANN Consensus Policies as well as the requirements of the RA and RAA. In fact, much of what is required by NIS2 is work gTLD Registries already carry out. **We urge the Parliament to recognize the policies and requirements that gTLD Registries must already comply with under their ICANN Registry Agreements and avoid creating overlapping and potentially conflicting requirements within the NIS2 Directive.**

It is important to note that in the context of the RA, RAA, and RRA, “accuracy” is the party’s assurance that data processed between Registrant and Registrar, Registrar and Registry, and Registry/Registrar and ICANN is accurate relative to what that party received from the previous party in the contractual chain, going back to what was provided originally by the Registrant, and maintained without change unless and until the Registrant make any change to their domain name account information. Thus, data received by any party from another party is only as “accurate” as the data which the first party received.

Further, “verification” is the assurance that the data Registrars and gTLD Registries receive and escrow (for redundancy) is complete. Verification can occur at a number of points in the registration process: before a registrant can register a name, after a name has been registered but before it has gone live, or after a name has been registered and after it has gone live. In the current ecosystem, registries, or third-party vendors of registries, conduct verifications before a registrant can register a name. Registrars then rely on the verification process of the Registry. Where the verification occurs after registration, the Registry relies on the verification efforts of the Registrar as they do not have control over the Registrar systems enabling the registration.

4. ICANN Policy Regarding the Processing of Personal Domain Name Registration Data

Historically, both gTLD Registries and Registrars have been required, through their contractual agreements with ICANN, to maintain certain data regarding the registration of the domain names under their respective management. This registration data (also sometimes referred to as “WHOIS data”) consists of technical details about the domain name, as well as data about the domain name Registrant that can serve as a means of discerning and contacting the administrator of a particular domain. Traditionally, this data was made publicly available to internet users.

The contact information of domain name registrants consists largely of personal data. As the Domain Name System has grown over time, enormous quantities of personal data have been collected, maintained, and made publicly available in accordance with ICANN requirements. The introduction of the GDPR forced the ICANN multistakeholder community to reconsider this existing practice of making such large quantities of personal data public.

The Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data is the community-driven policy development process that was tasked with confirming an ICANN crafted ‘emergency/temporary policy’ which was put in place to enable the contracted parties to come into GDPR compliance[4]. A key task of the EPDP team was to establish, formally, the purposes for the processing of registration data, and enumerate why such processing of data was necessary for the proper functioning of the Domain Name System. In total, seven "ICANN Purposes" were identified[5]. Included in these seven, naturally, was the purpose to register a domain. The team also reiterated the original purpose for registration data (i.e., to enable communication with the registrant), and then additional and practical purposes such as processing necessary to protect the security, stability and resiliency of the DNS, including monitoring for and escalating abuse reports, processing data in support of dispute resolution services, and others.

Having established these purposes, the EPDP team then defined what specific elements of registrant data were considered to be reasonably necessary to achieve the purposes as defined[6]. Noting as stated above that the business relationship and attendant contract ordinarily exists between a Registrar and a Registrant (whereas the gTLD Registry generally maintains no direct contact with the Registrant), the policy considered both the aggregate minimum set of personal data that a Registrar must collect from a Registrant, and separately, the aggregate minimum set of data the Registry must collect from the Registrar, in order to fulfill the identified purposes.

Registrars must collect or generate technical information about the domain name, as well as collect from the Registrant the following personal data:

1) Registrant Name
2) Registrant Organization (may contain PII)
3) Address (street, city, state, province, postal code, country)
4) Phone number
5) Email address

Some of the registration data collected or generated by the Registrar, specifically the technical details of the domain name, must be transferred to the gTLD Registry. Additional data elements may be optionally transferred to the gTLD Registry based on the gTLD Registry's unique terms, conditions, and policies (in other words, policies that are not applicable to all gTLD Registries designated by ICANN and are not necessary to fulfill the ICANN Purposes). The data elements that are optional for transfer include all of the contact data for the Registrant, such as name, address, phone number and email. While Registrars must collect and maintain those data elements in their own databases, it is not necessary for Registrars to then transfer all of those data elements on to the gTLD Registry in order to fulfill any of the identified ICANN Purposes.

---

[4] Temporary Specification for gTLD Registration Data (available at: https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#temp-spec)

[5] Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process, EPDP Team Recommendation 1, (available at : https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf)

[6] ibid., EPDP Team Recommendation 5.

As mentioned previously, we request that the Parliament recognize this distinction between gTLD Registries and Registrars and update the requirements under Article 23 accordingly to account for the parties' different responsibilities in collecting and maintaining registration data.

We also request that the Parliament considers avoiding overly prescriptive requirements to achieve the goals of NIS2. We would submit that the use of principle-based expectations, e.g., registration data must ensure contactability of the relevant registrant (as opposed to defining specific data elements), remains sufficient to achieve the purpose and desired outcome. We submit that such maintains the balance of ensuring accessibility of domain names for legitimate use and free expression, without unnecessarily raising the barrier to entry by imposing specific requirements on Registrants that may not be universally held (e.g., phone number or even a long-term physical address).

A. Publication

Having formally established both the ICANN Purposes themselves and the necessity grounding each Purpose, as well as the aggregate minimum set of data necessary to be collected, maintained and transferred to achieve those Purposes, the EPDP Team turned to a number of ancillary matters relating to the processing and use of that data, including the question of what data should continue to be made publicly available. Members of the ICANN community and others have historically used registration data for a variety of purposes, including investigating criminal activities, supporting cybersecurity, enforcing intellectual property rights, and others.

While the public availability of registration data has historically provided a benefit for some users, it has also been subject to criticism. For example, the then "Article 29 Working Party" ("WP29") were very critical of the widespread publication of this data. They were clear, on numerous occasions, that any publication of registration data relating to a natural person must be necessary to achieve the legitimate, specified and explicit purposes which are to be determined clearly by ICANN[7]. To address this ongoing issue, the EPDP team recommended that personal data that was subject to the GDPR, must be redacted from open publication[8].

It is worth noting that the EPDP team also recommended that as soon as commercially feasible, Registrars must provide an opportunity for their Registrants to consent to the publication of their data.[9]

B. Access

A common theme in the respective expectations of the European Data Protection Board (EDPB), the European Commission, Law Enforcement Agencies, the ICANN community and the gTLD Registries and Registrars themselves, is an acknowledgement that registration data

[7] Article 29 Working Party, Letter to Mr. Goran Marby of 11 April 2018, page 4. https://ec.europa.eu/newsroom/article29/redirection/document/51020
[8] supra fn 2, EPDP Team Recommendation 10.
[9] supra fn 2, EPDP Team Recommendation 6.

should be made available to those entities who can establish a 'legitimate interest' in the use of the data. To be clear, gTLD Registries and Registrars are very supportive of such an expectation. However, it must be clearly understood that such third-party purposes are very much separate to the purposes as set by ICANN policy and must not be conflated with distinct purposes of the gTLD Registries and Registrars required for the stable operation of the Domain Name System.

The WP29/EDPB have continued to encourage ICANN to facilitate the personal data processed in the context of WHOIS, so that it may be made available to third parties who have a legitimate interest in having access to the data. Notwithstanding that position, they also expect appropriate safeguards are in place to ensure that the disclosure is proportionate and limited to that which is necessary and that other requirements of the GDPR are met, including the provision of clear information to data subjects[10]. The gTLD Registries and Registrars continue to be legally responsible for ensuring that personal data processed in the context of WHOIS would only be disclosed to third parties with a legitimate interest or other lawful basis under the GDPR. Although EPDP Phase I recommendations included a mandatory expectation of review and response of such requests[11], the EPDP team were again convened (Phase II[12]), this time, being tasked with investigating the possibility of a centralized system for requesting disclosure of such data in a timely fashion, but with importing appropriate safeguards, including measures to ensure a sufficient degree of compliance assurance.

In short, ICANN policy not only makes the consideration of third-party requests mandatory, ICANN continues to work on a centralized system, including requester accreditation to further streamline the process. All this is necessitated by the fact that the GDPR does not appear compatible with unlimited publication of non-public registrant data, as we have been reminded by the WP29, and the EDPB in turn, on a number of occasions.

C. Accuracy

At the most basic level, the level of requirement for accuracy in a registration of a domain name, must be linked fundamentally to two important aspects:

1) The purpose of the processing; and
2) The instructions of the data subject

1) The purpose of the processing

[10] supra fn 5.; EDPB letter to Goran Marby, 5 July, 2018. Para 6, (available at: https://edpb.europa.eu/sites/default/files/files/news/icann_letter_en.pdf)
[11] supra fn 2, EPDP Team Recommendation 18
[12] Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process, (available at: https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf)

As explained above, at its most distilled, the purpose for the collection of registration data, is to ensure contactability of the Registrant[13]. All additional purposes, ultimately relate to that fundamental requirement of contact with a Registrant, be that in the case of alleged abusive activity, stability issues, issues relating to the technical resolution of the domain, etc.

ICANN policy requires that Registrant contact details provided at registration are accurate and reliable, such that a Registrant is contactable throughout the life of a registration[14]. This is achieved by requiring the Registrant to positively respond to a communication issued by the Registrar, via the contact details provided. Where such a contact is not positively confirmed, the domain is suspended, or depending on the policy of that Registrar, may even be deleted/cancelled (i.e., the domain will no longer resolve to any content, effectively removing a Registrant's ability to use the domain). Registrars must also issue a reminder as to such a requirement on an annual basis[15]. If at any time during the life of the registration, reasonable doubt is cast over the validity of the contact data, then the Registrar must re-confirm the contactability again.

Simply, when contact fails, a domain is suspended or deleted. Any requirement of the processing of additional personal data to achieve this purpose would be likely to fail the test of both necessity and proportionality, and would be of a much larger risk to all contracted parties and represent an unjustifiable impact to the Registrant.

2) Instructions of the Data Subject

All registration data are collected by the Registrar (at times via reseller relationships). These data elements are collected from Registrants who enter into individual agreements with that Registrar. Where the Registrant passes the contact test outlined above, that Registrar has no reason to believe, except where presented with objective evidence to the contrary, that the information, provided by the data subject themself, is not accurate. The existing system of ensuring contactability has proven effective in achieving the purpose (ability to contact the Registrant via the data provided) while limiting the amount of additional personal data process and the invasiveness of that processing.

We ask that the Parliament bear all this in mind when considering any requirements for registration data verification or validation under NIS2. We also would like to point out that the Registrar is the most appropriate party to perform such accuracy verifications, as evidenced by the ICANN requirements outlined above, and that it would be duplicative and disproportionate to apply such requirements to gTLD Registries as well.

D. Conflation of Purposes vis á vis Accuracy

As stated previously, numerous third parties have developed important uses for registration data, including criminal investigations and supporting cybersecurity. Because these use cases

---

[13] This is also consistent with the expectations of NISII (Art 23,2)

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

[15] WHOIS Data Reminder Policy (WDRP)https://whois.icann.org/en/whois-data-reminder-policy-wdrp

are not the same as the initial purpose for which Registrars collect the registration data (i.e., ensuring that the Registrant can be contacted), those third parties have inherently different expectations around the “accuracy” of that data and the level to which it has been verified. However, the EDPB made it abundantly clear that ICANN should not conflate its purposes for processing data (and by extension the purposes of Registries and Registrars) with the interests of such third parties.

As it is currently established, the verification of data for the purposes of the registration of a domain and ensuring the contactability of a registrant are considered to be reasonable, proportional and sufficient.