

Registration Data Request Service (RDRS) Policy Alignment Analysis

NCSG Comments

December 15th, 2025 *(deadline)*

About NCSG

NCSG represents the interests of non-commercial domain name registrants and end-users in formulating the Domain Name System policy within the Generic Names Supporting Organisation (GNSO). We are proud to have individual and organizational members in over 160 countries, and as a network of academics, Internet end-users, and civil society actors, etc, we represent a broad cross-section of the global Internet community. Since our predecessor's inception in 1999, we have facilitated global academic and civil society engagement in support of ICANN's mission, stimulating an informed citizenry and building their understanding of relevant DNS policy issues.

About this Public Comment Proceeding (Background)

<https://www.icann.org/en/public-comment/proceeding/registration-data-request-service-rdrs-policy-alignment-analysis-30-10-2025>

ICANN org launched RDRS on 28 November 2023 with the intention of operating the service for up to two years. This was a result of the ICANN Board's direction to ICANN to analyze usage of and demand for a system that handles requests for gTLD nonpublic registration data. The purpose of the RDRS is 1) to collect system usage data to inform the future discussion between the GNSO Council and the ICANN Board on the policy recommendations outlined in the EPDP Phase 2 Final Report , and 2) to provide a cost-effective system that will simplify the process for submitting and receiving requests for gTLD nonpublic registration data for both the requestors and registrars.

The ICANN Board and community began to discuss next steps regarding the future of the RDRS during ICANN81, including the future of the GNSO consensus policy recommendations concerning an SSAD, the impact of the PPSAI IRT policy work on disclosure of underlying privacy/proxy registration data, and the two tracks of work of

the Registration Data Policy IRT on a response time for urgent requests and law enforcement authentication. The GNSO Council during its meeting on 13 November 2024 also discussed whether it would be appropriate for the Council, following receipt of the GNSO Standing Committee's findings and recommendations, to reconsider the approved 18 policy recommendations from the EPDP Phase 2 Final Report, which recommended the development and implementation of an SSAD. The Council concluded that either revising or otherwise revisiting the approved SSAD recommendations would be the best next step.

I. Submission

The NCSG thanks ICANN staff for completing the policy alignment analysis for the RDRS, and recognizes the need to identify and align existing policies with the aim of developing a long-term solution for requesting access to generic top-level domain (gTLD) nonpublic registration data and address policy gaps.

Overarching Feedback

While the NCSG is supportive of this ambition and of the continuation of the pilot program, we do not support making such a system mandatory for registrars. Additionally, the alignment analysis lacks any mention of human rights impact assessments or requirements to protect and uphold the right to privacy or data protection rights. The NCSG calls for ICANN to reiterate its human rights commitment per section 1.2(b)(viii) of ICANN's [bylaws](#) through integrating due process and human rights protection mechanisms for registrants as an integral step in utilising the RDRS.

Why the RDRS Matters for Human Rights

In a human rights impact assessment ([HRIA](#)) [for the RDRS](#), the NCSG identified the following risks associated with the system:

- I. Involves facilitating disclosure of personal and sensitive data, impacting privacy ,freedom of expression,and access.
- II. Decisions about access to private data can affect security of journalists, activists and end-users in general.

When applied to real-world scenarios, decisions about access to private data can impact the safety and security of end-users, journalists, activists, and human rights defenders—all communities who are of the utmost priority to the NCSG and the ICANN community more broadly. The NCSG is supportive of developing a standard request process, particularly as it provides further transparency around data disclosure requests. However, the development of such a system must integrate accountability mechanisms—such as for authenticating requesters and evaluating the necessity of such requests—which the RDRS currently lacks.

The RDRS must address oversight, potential misuse, public reporting, and redress. The community impact of such systems on domain name registrants and Internet end users' privacy and security, the primary subjects of the data at issue, must appear in any impact assessment.

The NCSG's [public comment](#) on the RDRS made this clear: "Where international LEAs are involved, the mechanisms used for verification, eligibility, and request handling must be transparently disclosed." Any evaluation of "community impact" should therefore explicitly include the effects on registrants and end users, whose rights and interests are directly influenced by such decisions. The NCSG calls for any authentication mechanism to be accompanied by safeguards, transparency, accountability, and meaningful consideration of registrant and end-user rights, in order to avoid misuse. ICANN must also explicitly recognise that registrants and end-users are central stakeholders affected by these decisions, and to reflect this in its assessment of community impact. NCSG is ready to support the ICANN community to develop a standardized, transparent, rights-respecting and accountable framework for the RDRS.

NCSG Feedback per Policy Issues

3.1 SSAD Policy Recommendations

Under this section, the alignment paper observes that the GNSO Council may focus its recommendations "...less on prescriptive functionality and more on ensuring that contracted parties can accurately identify law enforcement requestors and the jurisdictions they represent." It is unclear what "prescriptive functionality" means. It would be helpful to have a more detailed description to ensure clarity for future work.

Additionally, despite the NCSG's many contributions on the topic—including most recently in a letter to the ICANN board dated 1 October 2025 "**Re-the October 2025 Resolution Concerning Law-Enforcement Authentication and Registrant Rights**"—there is no recognition in the document that any authentication or accreditation mechanism **must be accompanied by safeguards, transparency, and accountability**.

3.2 Disclosure of Privacy/Proxy Customer Data

In terms of the path forward outlined here, the NCSG agrees that any policy development process regarding whether PPSAIs be required to use the RDRS would not affect the determination of which data is disclosed in a given case. However, the NCSG requests the additional requirement be noted here that recipients of such requests—whether a registrar, registry operator, privacy or proxy service provider—**must conduct a fundamental rights balancing assessment when considering such requests**, in addition to any obligations under applicable laws and policies. They must also provide a clear rationale for any decision to disclose the information.

4. Possible Next Steps

The NCSG strongly urges the ICANN Board and GNSO Council to disregard the recommendation for "Mandatory Registrar Participation in RDRS." While the NCSG is supportive of the RDRS pilot continuing, it should do so on a **voluntary basis** for registrars. Having such a system is not only beneficial for registrars to facilitate in navigating requests for such data, but also for registrants if these systems integrate transparency requirements (such

as disclosing to registrants who has requested their data) and accountability mechanisms (to ensure requests are vetted to prevent registrant data from being shared with anyone who asks for it). This balance was discussed extensively in the ICANN84 [session](#) “GNSO: DNS Security Without Sacrificing Rights-HRIA on RDRS.”

Should the RDRS become mandatory, there is the additional risk that registrars may be pressured into disclosing data automatically (or more rapidly than otherwise) instead of conducting authentication procedures and/or impact assessments of individual requests. As many registrars themselves noted in the ICANN84 [GNSO session](#) on HRIAs for RDRS , requiring this places registrars in a tricky position as different jurisdictions have differing data protection requirements, and this is particularly complicated for registrars operating in the European Union. Hence there is a need to discuss, in a broader format, these aspects of data disclosure triage and how a rights-balancing test can be applied across different jurisdictions. Additionally, voluntary ccTLD participation must respect local jurisdiction, community governance, and diverse privacy frameworks. If ccTLDs choose to participate, their involvement — and any variation in policies — must be clearly disclosed to end-users.

ICANN needs to consult the community regarding whether the system as it stands now is fit for purposes (for example, does it collect the requisite information for a registrar to make an informed decision?) **before making it mandatory.**

Conclusion

There is a need for a broader community discussion on privacy and human rights-related issues with respect to the policies and services that ICANN is developing—both including and beyond the RDRS.

The NCSG expresses its sincere gratitude for the chance to provide feedback and guidance on important ICANN policy matters as such. We therefore extend our thanks to the ICANN Staff for their diligent consideration of our remarks and look forward to our concerns being addressed.

Relevant Resources

- NCSG Comments “Registration Data Request Service Standing Cmte. Report for GNSO Council Review” ([September 29, 2025](#))
- GNSO Privacy & Proxy Service Accreditation Issues WG Initial Report ([7 July 2015](#))

II. Summary of Submission

The NCSG supports the continued operation of the RDRS beyond the pilot phase, but this extension must be conditioned on meaningful improvements to transparency and accountability. The process for authenticating law enforcement and other requestors must also be clearly documented, publicly accessible, and subject to independent oversight.

Additionally, and to reiterate prior NCSG [comments](#), registrars must not simply passively render requests, but rather actively conduct documented evaluations of the fundamental rights at stake, such as by conducting a community impact assessment. Privacy, freedom of expression and process are integral to ensuring the safety and security of end-users and the stability of the DNS

Finally, RDRDS should not be made mandatory for registrars.

III. Summary of Attachment (optional)

[To summarize the PDF file that will be submitted, if any description different than the Summary of Submission is needed - if there are appendices, for example]