Registration Data Request Service Standing Cmte. Report for GNSO Council Review

NCSG Comments

September 29, 2025

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

https://www.icann.org/en/public-comment/proceeding/registration-data-request-service-standing-cmte-report-for-gnso-council-review-19-08-2025

Our Comment

Dear GNSO Council,

NCSG submits the attached human rights–oriented input in response to the RDRS Standing Committee Final Report dated 19 August 2025. This submission addresses each of the seven

recommendations with a view toward preserving users' human rights, especially privacy, ensuring transparency and accountability, and preventing unintended harms that may arise from automation, overreach, or insufficient oversight.

We appreciate the Council's continued engagement with the broader community and remain available to support further work toward rights-respecting evolution of the RDRS framework.

Recommendation 1: Continuity of the RDRS

We support the continued operation of the RDRS beyond the pilot phase, but this extension must be conditioned on meaningful improvements to transparency and accountability. Disaggregated transparency reporting that was introduced should be continued, identifying the volume of requests by requester type, geographic origin, registrar involvement, and disclosure outcomes.

Recommendation 2: Authentication of Law Enforcement and Other Requestors

The process for authenticating law enforcement and other requestors must be clearly documented, publicly accessible, and subject to independent oversight. As much as possible, the mechanism and software should be open source. Where international LEAs are involved, the mechanisms used for verification, eligibility, and request handling must be transparently disclosed. Authentication should not mean automatic disclosure of private and sensitive registrant data, nor urgent processing of requests without rights balancing consideration.

Recommendation 3(a): User Experience (UX) Improvements

Improved UX supports both the registrar and the rights of the registrant. A well-designed interface helps requestors provide complete, precise information and supports registrars in documenting decision-making that is evidence-based,proportional, and rights-respecting. (e.g. a proof of beta tester or end user experience by advancing the system to avoid some bias).

Recommendation 3(b): API Development

While the RDRS remains a triage mechanism, API development introduces automation risks. The API's scope must be clearly limited to intake and structured submission — not disclosure or status resolution. Built-in safeguards must include rate limits, request pattern analysis, and audit trails.The API Development section may contain a guideline to assure a process for habilitation of integrators labelized. API should conform to international standards.

Recommendation 3(c): ccTLD Participation

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 users.

Recommendation 4: Future Policy Areas – Privacy/Proxy and RDAP

Privacy/proxy registrations are essential for many users facing threats to their safety or anonymity. Any policy development must include heightened thresholds for disclosure. RDAP integration of RDRS links should not suggest that data is easily accessible. The disclosure request and framework that PPSAI is trying to implement should not conflict with other

disclosure frameworks. NCSG has already made a comment on the principles that should be upheld. Please refer to this document.

Recommendation 5: Evaluation of SSAD Recommendations

Modifications to SSAD recommendations must not weaken human rights safeguards. Oversight mechanisms in a multistakeholder manner such as transparency reporting and committee monitoring should be expanded.

It is unclear whether review and refinement of metrics used in data collection and reporting will continue. Institutionalising a process of regular metrics review will ensure the data collected to remain insightful, and aligned with policy and rights-based concerns. For example, categorization of requestors could be periodically reviewed to ensure that the wide range of requestors is captured. At the same time, any refinement must be implemented with caution to preserve comparability with previous data.

Recommendation 6: Role of the Standing Committee

The Standing Committee must continue to play an oversight role that includes system-level transparency, rights-based risk monitoring, and inclusion of civil society, privacy experts, and smaller registrar voices.

Other feedback

Incomplete/More Information is Required : The pilot data shows "Request is incomplete/more information is required" was a common reason for denial, accounting for 639 denials since launch. This might be a systemic issue with the request process,We suggests registrars should be required to provide more detailed, standardized reasons for denials to improve transparency and assist requestors in submitting valid requests. This is not simply a matter of a denial, but a breakdown in the process that negatively affects legitimate non-commercial requests.

Data Publicly Available: The report indicates that 303 requests were closed with the outcome "Data Publicly Available". This outcome means the requested data was already public, but the registrar did not approve or deny the request. This highlights a lack of clarity in registrar responses and can cause confusion for requesters, leading to an unnecessary submission. We urge for more clear, standardized registrar responses to improve user experience and reduce confusion.

Further comments:

Multilingual Access (p. 11):

We strongly support expanding language support in RDRS. Multilingual accessibility is not just about convenience for requestors — it is vital to ensure that registrars can fully understand the evidence and legal justification of a request. Without this, it is impossible to evaluate necessity, proportionality, or fundamental rights impacts. Multilingualism is foundational to procedural fairness.

Authentication:

While the Standing Committee recognizes the cost savings of avoiding full accreditation and supports a Minimum Viable Product approach, it does not sufficiently address the implications of pivoting to authentication. Specifically, any kind of authentication should clarify:

- **Who qualifies for authentication** and under what criteria,
- **How authentication will be conducted** and by whom (e.g., identity providers),
- **Protocols for use and revocation** post-authentication.

These gaps create ambiguity about the accountability, proportionality, and oversight of the system. Without a transparent, documented, and rights-respecting authentication framework, the RDRS risks replicating the very complexity and opacity it seeks to avoid. We recommend that any alternative to accreditation—especially an authentication-based model—include clear standards and documentation as a matter of policy and operational integrity.

Lessons Learned: Urgent requests

We urge the SC and Council to ensure that any implementation of SLAs, particularly for "urgent requests", respects the registrar's obligation to conduct a fundamental rights balancing test prior to disclosure. SLAs should not result in pressure to disclose without adequate assessment, especially in sensitive cases.

A constructive approach would include:

- Differentiated SLAs for low-risk vs. high-risk disclosures,
- A requirement for registrars to document when rights balancing causes delay,
- An "Urgent Track" process with checkpoint-based transparency, rather than hard deadlines,
- Human rights risk flags embedded in the request system.

These adjustments would help reconcile the tension between timeliness and legal obligations, ensuring that urgent requests are handled promptly but lawfully.

Authorized disclosures:

The obligation to conduct a fundamental rights balancing test in disclosure decisions should not be contingent on whether the GDPR applies.

Instead, fundamental rights, including privacy, freedom of expression, and due process, must be considered in all cases where personal data is at stake, regardless of jurisdiction or whether a specific data protection law mandates it. The response should be documented and if it is too risky to provide a “fundamental rights” reason to the requestor, the reason can be reported in aggregated responses on transparency reports.

Our final thoughts: Registrar Role in Rights Assessment

Throughout our comments, we underscore that registrars must not simply render requests. They should conduct a documented evaluation of the fundamental rights at stake — including privacy, freedom of expression, and due process, and provide a clear rationale for any decision to disclose the information. This is not only a best practice; it is necessary to ensure registrant rights are not subordinated to expediency or automation.

In closing, NCSG reiterates its unwavering commitment to privacy, accountability, and the protection of fundamental human rights. These are not optional add-ons, they must be the foundation of any system that mediates access (in any shape or form) to personal data. We call on the GNSO Council, the RDRS Standing Committee, and participating registrars to embed these principles with clarity, enforceability, and visibility in every procedural step.