ICANN | RrSG
Registrar Stakeholder Group

RrSG Public comment: Timeline for Urgent Requests for Lawful Disclosure of Nonpublic Registration Data

15 December 2025

The Registrar Stakeholder Group ("RrSG") appreciates the opportunity to comment on the Timeline for Urgent Requests for Lawful Disclosure of Nonpublic Registration Data and thanks the EPDP Phase 1 Implementation Review Team (IRT) and the ICANN Implementation Project Team (IPT) for their work in drafting this update to the Registration Data Policy.

The RrSG has participated diligently in the policy development and implementation work relating to Urgent Requests for disclosure of gTLD registration data. **The required response timeframe has been a sticking point because policy must permit sufficient time to properly consider the request, make a sound legal decision, and remain compliant with relevant privacy laws, while also respecting the time-sensitive nature of the situation**.

RrSG response to the proposed Timeline

The policy may be complete but the conversation is not over. **Given the severe uncertainties around receipt of sufficient information, requests which do not match the definition of Urgent, and conflicting legal pressures, registrars need the support and collaboration of the Community—particularly law enforcement agencies represented at the GAC—to meet this timeline.**

Registrars will of course follow the policy when it is effective, and the RrSG appreciates the considerations that have gone into the proposed 24 hour response window. That said, **the critical concern that RrSG has with this Timeline is ensuring that registrars will have the ability and the appropriate legal cover to adequately respond to an Urgent Request**.

The dilemma in meeting this timeline is: will registrars have correct, sufficient information to lawfully and swiftly respond to an Urgent Request without running afoul of serious and competing legal pressures or violating privacy law, particularly when registrars have no guarantee that the information provided in the request will be complete or actionable or,

more importantly, that registrars as controllers can properly perform a balancing test under applicable privacy law.

The RrSG continues to have concerns with both the 24 hour response timeline and the extensions as described in the proposed Policy language which put registrars at unfair and unnecessary risk because:

- **Requests are often incomplete**, requiring additional information in order to make a decision; it is rare that this additional information is provided promptly by the requestor. **The RrSG looks forward to appropriate assurances that authenticated Urgent Requests will always supply enough information for a registrar to appropriately and lawfully take action on that Request within the 24 hour period.**

- **Requests marked as "Urgent" frequently do not meet the definition of Urgent;** similarly we see in the RDRS that requests marked as “expedited” do not meet requirements for that process[1]. **There must be consequences preventing requestors from falsifying the circumstances of the request in order to gain faster responses.**

- **Registrars must comply with the law.** Privacy regulations require registrars, as data controllers, to conduct balancing tests when processing personal data, creating a challenging situation where legal requirements can easily come into conflict with the current policy framework. Since governments rightfully expect registrar compliance with privacy laws, and ICANN policy cannot override these legal obligations, registrars will find themselves having to decline to action Urgent Requests when insufficient information is provided to conduct the required balancing test. **The RrSG looks forward to appropriate assurances that Registrars can perform the balancing test and also have sufficient legal cover to supply registrant data pursuant to an Urgent Request.**

- **Registrars have competing legal pressures to contend with.** The EU E-evidence Regulation will bring a legal framework for registration data disclosure requests into effect starting August 2026; cross-border disclosure requests from EU law enforcement (including those received by registrars outside the EU which offer

[1] **One registrar tracking RDRS requests notes that 6% of requests received through that platform were marked as “expedited” while only 0.5% truly met the definition**. Downgraded requests related to topics including UDRP filings (this was the majority of their “expedited” requests), registrants looking for their own domain data, copyright infringement claims, unsolicited purchase offers, technical support requests, and completing a take-home exam for a job as a security consultant.

services within the EU) will be handled under that framework, regardless of policies adopted within ICANN.

Registrars understand the importance of prompt response to Urgent Requests for registration data disclosure, as evidenced by ongoing participation in this policy implementation work, but **the policy must permit sufficient time to obtain the necessary information to properly consider the request and make a sound legal decision—which may include a request for due process—while also respecting the time-sensitive nature of the situation,** or it must be further refined to provide adequate legal cover for registrars to action an Urgent Request without risk that they will contravene the law.

Who can submit Urgent requests?

Only local law enforcement has both the visibility into situations that fall under the definition of Urgent as well as the legal authority to compel disclosure of Personal Data.

The RrSG trusts that ICANN and the GAC are aware of the global nature of registrar business, such that jurisdictional applicability will be a threshold question applied to every Urgent Request, determining whether a registrar can action an Urgent Request submission.

The RrSG looks forward to understanding how an authentication mechanism would take into account the jurisdictional primacy that underpins the certainty, enforceability, and predictability inherent in the contracts and geopolitical realities of our industry, and how the GAC proposes to protect each registrar's discretion in making legal determinations when faced with a request from foreign jurisdictions. When the authentication system becomes available for use it should ensure that registrars can indicate the jurisdictions considered local to them, so that requests can be filtered accordingly before submission.

The RrSG also appreciates that all involved in the policy-making process understand that **ICANN Policy cannot overextend jurisdictional discretion or supersede a registrar's obligation to comply with applicable national laws that govern the registrar** and—in the name of rule of law and in deference to the national sovereignty of all countries throughout the world—how carefully we must continue to guard from allowing Policy to do so.

Considering due process

The RrSG is significantly concerned about the conflict created by an Urgent Requests process and basic due process obligations, a foundational pillar of the legal system.

While an LEA representative may be authenticated, that does not guarantee that requests will enable registrars to action them without running afoul of due process. The RrSG cannot overstate the sensitivity of this conflict, or the serious risks that could be created without careful, respectful, well-considerated policy in this area. **The RrSG requests that the GAC consult with their law enforcement agencies and national policymakers to explain further how this conflict can be resolved in a manner that both upholds the rule of law and respects the national legal frameworks of each member of the GAC.**

There remains the option for law enforcement to get a warrant (or subpoena) for the data, which would allow a swift response without requiring the registrar to obtain legal counsel in a very short time. **Alternatively, the requestor could expedite the process even further by determining that the situation is "exigent[2]" and require that the data be disclosed before they go through the process of getting a warrant.**

Under the EU E-Evidence Act there is the corollary "emergency case" option, which requires a response time of 8 hours from receipt of the order; the responding registrar is required to comply without review, but there is an ex-post review of the order by a competent authority and if a request is deemed unlawful at that point then the order is withdrawn immediately and any data obtained destroyed.

The RrSG suggests a similar mechanism where the urgent request can be reviewed ex post. This still has clear drawbacks—although if the request is deemed unlawful the data must be destroyed even still any effects of the disclosure cannot truly be undone—but it **provides a legal grounding for registrars, allows law enforcement to obtain data quickly, and guarantees that the rights of the registrant are given due consideration.**

[2] "Exigent circumstances, as defined in *United States v. McConney* are "circumstances that would cause a reasonable person to believe that entry (or other relevant prompt action) was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."" "exigent circumstances." *Legal Information Institute*, Cornell Law School, December 2022, https://www.law.cornell.edu/wex/exigent_circumstances.

ICANN | RrSG
Registrar Stakeholder Group

Responses to ICANN Org questions

Does the draft language proposed for inclusion in Sections 3.8, 3.9, 10.7, and Implementation Note K of the Registration Data Policy clearly describe the applicable requirements?

Yes, the draft language clearly describes the applicable requirements.

Does the proposed Urgent Request timeline align with the requirements in EPDP Phase 1 Rec 18, and the expectations provided by the Board, GAC and GNSO Council?

The RrSG notes that **faithful implementation of approved Policy Recommendations should be the priority over expectations held by any one group.**

EPDP Phase 1 Rec 18: The proposed Urgent Requests timeline does not align with the requirements in EPDP Phase 1 Rec 18. The Working Group recommended a response time in business days; despite RrSG attempts to faithfully implement this recommendation, the IRT has settled on a period of hours.

Board expectations: The proposed Urgent Requests timeline does seem to align with the Board's expectations. Notably, the timeline recognizes the application and utilization of authentication for LEA; and that only authenticated LEA requestors are the requestors under 10.7. However, what is still missing is the actual consensus policy, process, and system itself for authenticating LEA requestors. Thus, while the timeline in and of itself may meet Board expectations, there are still key components missing at this stage. **The Board's role here should be, as always, to ensure that the bottom-up multistakeholder policy development process is respected and adhered to.**

GAC Expectations: The proposed Urgent Requests timeline should meet the GAC's expectations, as it recognizes authentication of LEA requestors and shortened response times compared to standard requests. However it is the opinion of the RrSG that accommodating GAC expectations has resulted in unprecedented tinkering with policy development and implementation which should be guarded against in the future. Further, while it is understood that true Urgent Requests are few, the GAC has given little consideration to the operational realities of small registrars or the sufficient time necessary to evaluate requests.

GNSO Council Expectations: Based on the 29 August 2024 Council Chair communication to the Board**, the proposed Urgent Requests timeline does not meet Council expectations.** Specifically, the Council Chair flagged that there is no mechanism by which to revisit a policy recommendation that has been approved by the Board, but recognized the importance of the concerns. That being said, Council also recognized that there is not yet a process or system for authenticating LEA requestors. **Nowhere in that communication did Council request a 24 hour timeframe for response.**

The IRT has discussed the proposed Section 10.7 and some IRT members believe the authentication mechanism (when available) would require additional policy work, while others believe the authentication mechanism is part of the implementation of Rec 18 and would not require additional policy work. Do you believe this requires additional policy work?

The RrSG agrees that having an authentication mechanism can be a valuable part of the process as it would provide assurance that the requestor is who they claim to be and potentially save time in the registrar's review; that said, **any required use of an authentication system must be governed by an adopted Consensus Policy.**

This Policy would address important questions such as who is eligible to be authenticated, who operates and funds the system, where system data is hosted and who can access it, and what security measures are in place to prevent fraud and abuse.

We are pleased to see that the timeline recognizes the need for consensus policy supporting the authentication mechanism. While there is not yet any such policy; if the GNSO Council and ICANN Board determine that there should be policy work done on this topic the RrSG will of course participate in that effort.

Thank you,

Owen Smigelski

Registrar Stakeholder Group Chair