

03 June 2024

Re: Dialogue with GNSO Council on EPDP Phase 1 Recommendation 18 (Urgent Requests)

Greg DiBiase, Chair
Generic Names Supporting Organization (GNSO) Council

Dear Greg and Members of the GNSO Council,

I am writing to provide information requested by the GNSO Council regarding the Board's concerns about the [Expedited Policy Development Process \(EPDP\) Phase 1 Recommendation 18](#). This recommendation, which was adopted by the Board on 15 May 2019, relates to urgent requests for unpublished registrant data in the context of situations that pose an imminent threat to life, serious bodily harm, infrastructure, or child exploitation.

At the Board's direction, ICANN org worked with a multistakeholder [Implementation Review Team](#) (IRT) to draft requirements for inclusion in the Registration Data Policy for gTLDs document (Registration Data Policy) based on the approved EPDP Phase 1 recommendations. The EPDP Phase 1 Final Report did not contain a specific rationale for Recommendation 18, and left the timeline for urgent requests for data disclosure to be worked out in implementation. In accordance with the [Consensus Policy Implementation Framework](#), ICANN org consulted with the IRT in finalizing the Registration Data Policy document for implementation, including the implementation of Recommendation 18.

During the implementation stage, the GAC [raised concerns](#) related to Recommendation 18 specific to the proposed timeline for responses to urgent requests in the Registration Data Policy. The Board subsequently reviewed the issue. After significant discussion, the Board concluded that it is necessary to revisit Policy Recommendation 18 concerning requests for registrant data made in the context of situations that pose an imminent threat to life, serious bodily harm, infrastructure, or child exploitation.

While we understand that direct communications channels between law enforcement and sponsoring registrars exist in many cases and are regularly used for the purpose of responding to true emergencies, the Board is also aware that such direct communications channels are not in place among all ICANN-accredited registrars and all emergency responders.

During its discussion, the Board identified the following issues and concerns:

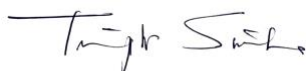
1. To the extent that law enforcement needs registration data to respond to situations that pose an imminent threat to life, serious bodily harm, infrastructure, or child exploitation, the proposed timeline - whether one, two, or three business days - does not appear to

be fit for purpose. To respond to truly imminent threats, a much shorter response timeline, i.e., minutes or hours rather than days, would seem to be more appropriate.

2. At the same time, applicable law, regulation, and reasonable registrar policies will often require registrars to authenticate self-identified emergency responders and confirm the purpose(s) for which registrant data is sought prior to disclosing personal data. Even where not required by law or regulation, authentication will often be appropriate under globally accepted principles of fair information processing to protect the rights and freedoms of data subjects.¹
3. Absent some authoritative, legally sufficient cross-border system for validating law enforcement/emergency responders, registrars will require time - almost certainly measured in business days rather than hours or minutes - to authenticate the source of urgent requests.
4. To the best of our knowledge, such an authoritative, legally sufficient cross-border system for authenticating emergency responders/law enforcement globally is not available to ICANN.
5. In addition to the fact that the creation, operation, and maintenance of a legally sufficient authentication system would consume significant human and financial resources, such a mechanism cannot be created, operated, and/or maintained without the material, ongoing assistance of law enforcement, first responders, and governments.

Under these circumstances, the Board has concluded that the proposed urgent response policy is not fit for purpose and must be revisited. The Board notes that neither the Bylaws nor existing procedures account for the situation in which we now find ourselves, i.e., where the Board concludes that a policy recommendation that it has previously approved should be revisited prior to implementation. We welcome the GNSO Council's input on next steps, and look forward to discussing this topic at the next opportunity.

Sincerely,



Tripti Sinha
Chair, ICANN Board of Directors.

¹ While authentication is likely in many cases to be a necessary prerequisite to personal data disclosure, it is unlikely to be sufficient to guarantee disclosure in many cases. Registrars may be precluded under applicable law and regulation from disclosing redacted personal information about a registrant to authenticated law enforcement in certain jurisdictions, without a valid local court order, etc. We note, as well, that these laws, regulations, and reasonable policies may appropriately prohibit release of registrant data, for example, to foreign law enforcement. Our understanding is that the approved recommendation is intended to establish an enforceable response time, but not to compel disclosure in violation of applicable law.