

Registries Stakeholder Group Statement



Public Comment: **Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2**

Date statement submitted: **22 January 2021**

Reference url: <https://www.icann.org/public-comments/policy-recommendations-epdp-phase-2-2020-12-03-en> .

Background¹

- this Public Comment proceeding is seeking input on a set of final recommendations that relate to topics from the EPDP's Phase 1 (which have also been referred to as "priority 2 topics");
- the recommendations related to the System for Standardized Access/Disclosure ("SSAD") which were also adopted by the GNSO Council as part of the EPDP Phase 2 Final Report are **NOT** included in this Public Comment proceeding and will be part of a future Public Comment proceeding.

RySG comment on the EPDP Phase 2 Addendum to the Initial Report (5 May 2020):

https://84e2b371-5c03-4c5c-8c68-63869282fa23.filesusr.com/ugd/ec8e4c_1c4d4d792fbb4310ac0e9e3ecce5d3f7.pdf .

Registries Stakeholder Group comment

The Registries Stakeholder Group (RySG) welcomes the opportunity to provide feedback² on the Priority 2 Policy Recommendations for ICANN Board Consideration from EPDP Phase 2.

Recommendation #19.

Display of information of affiliated and/or accredited privacy / proxy providers

In the case of a domain name registration where an affiliated and/or accredited privacy/proxy service is used, e.g., where data associated with a natural person is masked, Registrar (and Registry, where applicable) MUST include the full RDDS data of the applicable privacy/proxy service in response to an RDDS query. The full privacy/proxy RDDS data may also include a pseudonymized email.

The RySG notes that this proposal to replace current EPDP phase 1 Recommendation #14 with Recommendation #19 text is a matter that more directly impacts our colleagues in the Registrars.

As was raised by our representatives to the EPDP team during consideration of the issue and reinforced by the legal guidance solicited and received by the EPDP Phase 2, the publication of a pseudonymized

¹ *Background: intended to give a brief context for the comment and to highlight what is most relevant for RO's in the subject document – it is not a summary of the subject document.*

² *Registries Stakeholder Group (RySG) Comment - In the interest of time, we did not conduct a vote on these comments. We did discuss them on our mailing list and during a biweekly conference call, and no member opposed their submission.*

email remains the publication of personal data as it is the publication of an email that refers to, and is capable of, identifying a specific data subject. The EPDP Phase 2 team received legal advice that supports such a statement, noting that while pseudonymization and anonymization are useful privacy enhancing measures, the publication of masked emails would not meet those standards because they are specifically intended to ensure contactability of individuals themselves. [Ruth Boardman (Bird & Bird LLP), ""Batch 2" of GDPR questions regarding a System for Standardized Access/Disclosure ("SSAD"), Privacy/Proxy and Pseudonymized Emails," dated 4 February 2020.].

Again, the RySG must caution against the creation of a recommendation that ignores the realities of the technology available. This recommendation has not been based on any assessment of the technical possibility or feasibility, of accurately identifying privacy/proxy registrations, and then successfully segregating en masse, the existence of a privacy/proxy registration which would be required for registrars or registries to meet the requirement to 'publish' this data created by this recommendation. Much as in the case of legal/natural identification, the RySG remains doubtful that the state of the art allows for the implementation of such a requirement. Noting that even if it did allow for it, the cost of implementation would likely be unreasonable and far outweigh the risks and benefits. It is the duty of the controller to ensure that there is not a single instance of inadvertent release of personal data. ICANN policy must not create a situation where contractual expectations are not based on realistic expectations, put parties at additional legal risk, or are impossible to implement.

The RySG will welcome any clarity on how this objective may be achieved, but until such a time, we do not support the inclusion of any mandatory publication. The decision to publish should remain optional for the relevant controller, as this allows the controller in each such situation to adequately assess the legal risks involved and allow them to proceed as they believe is subjectively, and based on the circumstances of the disclosure, to be in line with the expectations of the relevant legislation, which is applicable both to them as an entity, and to the data in question.

Finally, the changes to the Recommendation text expands the requirement from applying to "affiliated" privacy/proxy providers to all accredited privacy/proxy providers. This was to avoid scenarios where the registrar was out of compliance solely because they were unaware that the registration came from a privacy/proxy provider. This is in anticipation that the privacy/proxy IRT will complete its work resulting in accredited privacy/proxy providers that are known to registrars in theory making it possible for a registrar to (automatically) not redact such registration data. It should be noted that this is an assumption and is dependent on the final product from the privacy/proxy IRT.

The RySG urges the Board to take this into account and instruct staff to report any incompatibility between this recommendation and the privacy/proxy recommendations back to the GNSO council.

Recommendation #20. City Field

The EPDP Team recommends that the EPDP Phase 1 recommendation #11 is updated to state that redaction MAY be applied to the city field in reference to the registrant's contact information, instead of MUST.

The RySG is supportive of this recommendation. Registries and registrars as controllers of the data are the appropriate parties to assess the legal risks of disclosure. Permitting rather than requiring publication strikes the appropriate balance to empower controllers to make those decisions based on their own relevant circumstances.

Recommendation #21. Data Retention

The EPDP Team confirms its recommendation from phase 1 that registrars MUST retain only those data elements deemed necessary for the purposes of the TDRP, for a period of fifteen months following the life of the registration plus three months to implement the deletion, i.e., 18 months. This retention is grounded on the stated policy stipulation within the TDRP that claims under the policy may only be raised for a period of 12 months after the alleged breach (FN: see TDRP section 2.2) of the Transfer Policy (FN: see Section 1.15 of TDRP). For clarity, this does not prevent Requestors, including ICANN Compliance, from requesting disclosure of these retained data elements for purposes other than TDRP, but disclosure of those will be subject to relevant data protection laws, e.g., does a lawful basis for disclosure exist. For the avoidance of doubt, this retention period does not restrict the ability of registries and registrars to retain data elements for longer periods.

As with Recommendation #19, The RySG notes that this proposal is to replace EPDP phase 1 Recommendation #15 text and is a matter that directly impacts our Registrar colleagues.

The RySG continues to caution that insofar as ICANN ‘obligations’ are concerned, only that data retained for a specific purpose (as enumerated by ICANN and as included in the final report) and as such, as is communicated to the relevant data subjects upon collection, shall be subject to any ICANN contractual compliance monitoring and/or enforcement.

The RySG agrees that data collected for a specific purpose may be processed further to another compatible purpose. However, processing data for another purpose is subject to the controller’s sole discretion, as is in line with data protection legislation as well as discussion and agreement within the EPDP Phase 2. Such processing shall be outside the influence or insistence of ICANN policy, and ICANN compliance cannot claim any authority over such processing (or the denial of any request for such processing) including purporting enforcement, be that via compliance notice, inquiry or similar effort.

However, we feel that this text provides clarification from the previous text by noting that TDRP is the only purpose for data retention.

Recommendation #22. Purpose 2

The EPDP Team recommends the following purpose be added to the EPDP Team Phase 1 purposes, which form the basis of the new ICANN policy:

- Contribute to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission.

The new Purpose 2 language in Recommendation 22 replaces the original Purpose 2 from EPDP Phase 1 Recommendation 1, which was not agreed to or adopted by the ICANN Board. While the language is amended, the RySG continues to have concerns, as noted in the EPDP Phase 1 Final Report, RySG Phase 1 Minority Statement.³

We do not feel that this purpose qualifies as a legal “Purpose” as defined in the GDPR. With direct reference to the ICO Guidance on Purpose Limitation: “This requirement aims to ensure that you are clear and open about your reasons for obtaining personal data, and that what you do with the data is in line with the reasonable expectations of the individuals concerned. Specifying your purposes from the outset helps you to be accountable for your processing, and helps you avoid ‘function creep’. It also

³ pg. 166, available at <https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf>.

helps individuals understand how you use their data, make decisions about whether they are happy to share their details, and assert their rights over data where appropriate. It is fundamental to “building public trust in how you use personal data”.⁴ It is not clear that by saying “contribute to the maintenance of the security, stability and resiliency of the Domain Name System in accordance with ICANN’s mission” that a data subject will understand how their data will be processed or why it is necessary. In addition, we note that requests for disclosure may be made with or without this, or other, specific Purpose. Finally, we do not believe the changes in the text of Purpose 2 resolve the EDPB’s previously stated concerns regarding conflating ICANN’s purposes with those of third parties.⁵ The RySG notes that this Purpose remains an ICANN purpose, as was requested and supported by the Board, and not a Registry or Registrar Purpose.

However, noting the above, the Board’s support for this amended Purpose 2 language⁶, and the narrow scope and spirit in which we believe it’s intended the RySG has agreed not to object to this purpose.

⁴ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/> .

⁵ Letter from Jelinek to Marby, 5th July, 2018, <https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf> .

⁶ letter from Martin Botterman to Keith Drazek, dated 11 March 2020, <https://www.icann.org/en/system/files/correspondence/botterman-to-drazek-11mar20-en.pdf> .