From the EPDP Team Charter in relation to System for Standardized Access to Non-Public Registration Data

From the EPDP Team Charter in relation to the Temporary Specification Annex

Issues deferred from the EPDP Team Final Report for Phase I

Phase II: 1) System for Standardized Access to Non-Public Registration Data, 2) Annex - Important Issues for Community Consideration and 3) Issues deferred from EPDP Phase I

System for Standardized Access to Non-Public Registration Data (note, questions are copied from EPDP Team Charter)

1 Pursuant to Section 4.4, continuing community work to develop an accreditation and access model that complies with GDPR, while recognizing the need to obtain additional guidance from Article 29 Working Party/European Data Protection Board.

? Is this topic captured by the overarching topic of the System for Standardized Access to Non-Public Registration Data?

4 Consistent process for continued access to Registration Data, including non-public data, for users with a legitimate purpose, until the time when a final accreditation and access mechanism is fully operational, on a mandatory basis for all contracted parties.

? Is this topic addressed through the implementation of recommendation #18 of the Final Report of phase 1?

a) Purposes for Accessing Data - what are the unanswered policy questions that will guide implementation?

- a1) Under applicable law, what are legitimate purposes for third parties to access registration data?
- a2) What legal bases exist to support this access?
- a3) What are the eligibility criteria for access to non-public Registration data?
  - 3 Developing methods to provide potential URS and UDRP complainants with sufficient access to Registration Data to support good-faith filings of complaints.
    - The EPDP Team requests that when the EPDP Team commences its deliberations on a standardized access framework, a representative of the RPMs PDP WG shall provide an update on the current status of deliberations so that the EPDP Team may determine if/how the WG's recommendations may affect consideration of the URS and UDRP in the context of the standardized access framework deliberations.
- a4) Do those parties/groups consist of different types of third-party requestors?
- a5) What data elements should each user/party have access to based on their purpose?
- a6) To what extent can we determine a set of data elements and potential scope (volume) for specific third parties and/or purposes?
- a7) How can RDAP, that is technically capable, allow Registries/Registrars to accept accreditation tokens and purpose for the query? Once accreditation models are developed by the appropriate accreditors and approved by the relevant legal authorities, how can we ensure that RDAP is technically capable and is ready to accept, log and respond to the accredited requestor's token?
- Note that Purpose 2 is a placeholder pending further work on the issue of access in Phase 2 of this EPDP and is expected to be revisited once this Phase 2 work has been completed.

b) Credentialing - What are the unanswered policy questions that will guide implementation?

- b1) How will credentials be granted and managed?
- b2) Who is responsible for providing credentials?
- b3) How will these credentials be integrated into registrars'/registries' technical systems?

c) Terms of access and compliance with terms of use - What are the unanswered policy questions that will guide implementation?

- c1) What rules/policies will govern users' access to the data?
  - 6 Limitations in terms of query volume envisaged under an accreditation program balanced against realistic investigatory cross-referencing needs.
- c2) What rules/policies will govern users' use of the data once accessed?
- c3) Who will be responsible for establishing and enforcing these rules/policies?
- c4) What, if any, sanctions or penalties will a user face for abusing the data, including future restrictions on access or compensation to data subjects whose data has been abused in addition to any sanctions already provided in applicable law?
- c5) What kinds of insights will Contracted Parties have into what data is accessed and how it is used?
- c6) What rights do data subjects have in ascertaining when and how their data is accessed and used?
- c7) How can a third party access model accommodate differing requirements for data subject notification of data disclosure?
  - 7 Confidentiality of queries for Registration Data by law enforcement authorities.

EPDP Team Recommendation #3.
In accordance with the EPDP Team Charter and in line with Purpose #2, the EPDP Team undertakes to make a recommendation pertaining to a standardised model for lawful disclosure of non-public Registration Data (referred to in the Charter as 'Standardised Access') now that the gating questions in the charter have been answered. This will include addressing questions such as:
• Whether such a system should be adopted
• What are the legitimate purposes for third parties to access registration data?
• What are the eligibility criteria for access to non-public Registration data?
• Do those parties/groups consist of different types of third-party requestors?
• What data elements should each user/party have access to?

In this context, the EPDP team will consider amongst other issues, disclosure in the course of intellectual property infringement and DNS abuse cases.There is a need to confirm that disclosure for legitimate purposes is not incompatible with the purposes for which such data has been collected.

Annex: Important Issues for Further Community Action

Feasibility of unique contacts to have uniform anonymized email address:
2 Addressing the feasibility of requiring unique contacts to have a uniform anonymized email address across domain name registrations at a given Registrar, while ensuring security/stability and meeting the requirements of Section 2.5.1 of Appendix A.

Legal vs Natural
5 Distinguishing between legal and natural persons to allow for public access to the Registration Data of legal persons, which are not in the remit of the GDPR.

EPDP Team Recommendation #17.
1) The EPDP Team recommends that Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so.
2) The EPDP Team recommends that as soon as possible ICANN Org undertakes a study, for which the terms of reference are developed in consultation with the community, that considers:
• The feasibility and costs including both implementation and potential liability costs of differentiating between legal and natural persons;
• Examples of industries or other organizations that have successfully differentiated between legal and natural persons;
• Privacy risks to registered name holders of differentiating between legal and natural persons; and
• Other potential risks (if any) to registrars and registries of not differentiating.
3) The EPDP Team will determine and resolve the Legal vs. Natural issue in Phase 2.

Issues Deferred from EPDP Phase I

Additional purpose for ICANN's OCTO
EPDP Team Recommendation #2.
The EPDP Team commits to considering in Phase 2 of its work whether additional purposes should be considered to facilitate ICANN's Office of the Chief Technology Officer (OCTO) to carry out its mission (see https://www.icann.org/octo). This consideration should be informed by legal guidance on if/how provisions in the GDPR concerning research apply to ICANN Org and the expression for the need of such pseudonymized data by ICANN.

Dependent on legal guidance and expression of need by ICANN

Display of information of affiliated vs. accredited privacy / proxy providers
EPDP Team Recommendation #14.
In the case of a domain name registration where an "affiliated" privacy/proxy service used (e.g. where data associated with a natural person is masked), Registrar (and Registry where applicable) MUST include in the public RDDS and return in response to any query full non-personal RDDS data of the privacy/proxy service, which MAY also include the existing privacy/proxy pseudonymized email.

Note, PPSAI is an approved policy that is currently going through implementation. It will be important to understand the interplay between the display of information of affiliated vs. accredited privacy / proxy providers. Based on feedback received on this topic from the PPSAI IRT, the EPDP Team may consider this further in phase 2.

Dependent on feedback received from PPSAI

Data Retention
EPDP Team Recommendation #15.
1. In order to inform its Phase 2 deliberations, the EPDP team recommends that ICANN Org, as a matter of urgency, undertakes a review of all of its active processes and procedures so as to identify and document the instances in which personal data is requested from a registrar beyond the period of the 'life of the registration'. Retention periods for specific data elements should then be identified, documented, and relied upon to establish the required relevant and specific minimum data retention expectations for registrars. The EPDP Team recommends community members be invited to contribute to this data gathering exercise by providing input on other legitimate purposes for which different retention periods may be applicable.
2. In the interim, the EPDP team has recognized that the Transfer Dispute Resolution Policy ("TDRP") has been identified as having the longest justified retention period of one year and has therefore recommended registrars be required to 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[34]. 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). This retention period does not restrict the ability of registries and registrars to retain data elements provided in Recommendations 4 -7 for other purposes specified in Recommendation 1 for shorter periods. (Footnote: In Phase 2, the EPDP Team will work on identifying different retention periods for any other purposes, including the purposes identified in this Report.) (....)

Dependent on ICANN Org undertaking a review of all its active processes and procedures so as to identify and document the instances in which personal data is requested beyond the 'life of registration'.

City Redaction Field
EPDP Team Recommendation #11.
The EPDP Team recommends that redaction must be applied as follows to this data element:
City - Redacted
The EPDP Team expects to receive further legal advice on this topic which it will analyze in phase 2 of its work to determine whether or not this recommendation should be modified.

Dependent on further legal advice

Review legal guidance provided in phase 1

- Territorial Scope
- Legal Basis (6.1b)
- Technical Contact
- Whois Accuracy