Expedited Policy Development Process (EPDP) on the
Temporary Specification for gTLD Registration Data – Phase 2
Input Template, 30 May 2019

To: ICANN Supporting Organizations / Advisory Committees / GNSO Stakeholder Groups / GNSO Constituencies

From: EPDP Team on the Temporary Specification for gTLD Registration Data – Phase 2

PLEASE SUBMIT YOUR RESPONSE AT THE LATEST BY 21 JUNE 2019 TO THE GNSO SECRETARIAT (gnso-secs@icann.org) which will forward your statement to the EPDP Team.

Following the completion of its work on phase 1 related topics, the EPDP Team has now commenced its work on phase 2. The scope of phase 2 includes:

1. Items identified in EPDP Team Charter:
   - System for Standardized Access to Non-Public Registration Data
   - Annex to the Temporary Specification (Important Issues for Further Community Action)
2. Items deferred from EPDP Team phase 1, either requiring further consideration or dependent on input from others

The following mind map provides further detail on these items: EPDP Team Phase 2 - upd 10 March 2019.pdf.

In order to tackle these items, the EPDP Team has agreed on the following approach - see Phase 2 Approach - updated 22 May 2019.pdf.

As required by the EPDP Manual, the EPDP Team is hereby reaching out to all ICANN Supporting Organizations, Advisory Committees and GNSO Stakeholder Groups and Constituencies to request your early input to help inform the EPDP Team's deliberations for phase 2. The EPDP Team would like to encourage you to focus your input on the questions outlined below as this will facilitate the EPDP Team's review of the input received. However, you should feel free to add any additional information you deem important to inform the EPDP Team's deliberations, even if this does not fit into questions listed below. Please try to avoid duplicating input that has already been conveyed through your representatives on the EPDP Team or provided through statements that were included as part of the Phase 1 Final Report.

For further information, please visit the EPDP Team Workspace (see https://community.icann.org/x/IYEpBQ). For the membership of the EPDP Team, please see https://community.icann.org/x/kBdIBg.

RESPONSES IN RED BELOW ARE FROM THE RRSG

Submitting Organization Information

a. Please identify your SO/AC/GNSO Stakeholder Group / GNSO Constituency:
Registrar Stakeholder Group (RrSG)

b. Please identify the member(s) of your SO/AC/GNSO Stakeholder Group / GNSO Constituency who is (are) participating in this EPDP Team:
RrSG EPDP Team: James Bladel, Matt Serlin, Volker Greimann (Alternates: Sarah Wyld, Owen Smigelski, Theo Geurts)

c. Please identify the members of your SO/AC/GNSO Stakeholder Group / GNSO Constituency who participated in developing the perspective(s) set forth below:
The RrSG EPDP Team, the RrSG ExCom and other RrSG Members

d. Please describe the process by which SO/AC/GNSO Stakeholder Group / GNSO Constituency used to arrive at the perspective(s) set forth below:
An initial response was drafted by the RrSG EPDP Team, followed by review and input from the RrSG ExCom and other RrSG Members

e. Please identify a primary point of contact with an email address in case any follow-up is needed:
Zoe Bonython - RrSG Secretariat (secretariat@icannregistrars.org)

Questions for specific input:

As the GNSO Council and the EPDP Team have identified as a priority the issues related to the System for Standardized Disclosure to Non-Public Registration Data, we would like to encourage you to provide your input to the following charter questions:

- (a) Purposes for Accessing Data – What are the unanswered policy questions that will guide implementation?
- (b) Credentialing – What are the unanswered policy questions that will guide implementation?
- (c) Terms of access and compliance with terms of use – What are the unanswered policy questions that will guide implementation?

In the annex, you will find the detailed charter questions and issues the EPDP Team is expected to address. If in addition to your input to the questions above you want to provide additional information, please feel free to do so focusing on input and information that has not been shared yet with the EPDP Team on previous occasions.

Annex A – Phase 2 Charter Questions and Issues

System for Standardized Access to Non-Public Registration Data

(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?
ADD: e.g. does a legal right or entitlement to request and receive disclosure exist for the third party under applicable law?

a3) What are the eligibility criteria for access to non-public Registration data?
ADD: What comparable processes exist for requesting disclosure in comparable situations?
For example, how would these parties obtain personal customer data from internet access providers, hosting providers, etc?

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 purposes?

a6) To what extent can we determine a set of data elements and potential scope (volume) for specific third parties and/or purposes?
ADD: How can legitimate interests/ third party purposes be matched against disclosure levels? What safeguards exist against misrepresentation of purposes?

a7) How can RDAP, that is technically capable, allow Registries/Registrars to accept accreditation tokens and purpose for the query? ADD: What purposes will accreditation ultimately serve? 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?
ADD: How would RDAP function in case a review process is needed for each request, e.g. as a process that is not instantaneous?

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

b1) How will credentials be granted and managed ADD: (including requestor demonstration of affiliation, and revocation or adjustment of credential)?
NOTE: An appointed organization shall have procedures, and these procedures will vary from sector to sector and country to country. It is perhaps out of scope for the EPDP team to address the specifics; international guidance should be sought from international accreditors with experience in similar processes. Validity of a demonstration of affiliation or status should be verified by a group with appropriate ability to do so. Once credentials are granted, they should be tracked and periodically audited for continued relevance. Credentials that are no longer required should be suspended so that access is appropriately limited.

b2) Who is responsible for providing ADD: and managing credentials?
NOTE: This may fall to ICANN, as an overseeing body already present in the industry. However, ICANN may not be able to appropriately discern if a requestor's affiliation or other group membership is valid and applicable to the situation at hand (e.g. ICANN may not have awareness about the inter-relationship between various law enforcement agencies in an unfamiliar jurisdiction). In that case, credential management may need to reside with industry bodies who coordinate with ICANN to be designated as the approved credentialing group for a given industry.

b3) How will these credentials be integrated into registrars'/registries' technical systems?
NOTE: This will depend on several other factors that have to be determined first. But from a high level the EPDP Team could come up with a setup where ICANN for example has a set of master credentials that connect to registries to registrars where the assumption is that the credentialing on a micro level prior is done through a system that connects to ICANN first or a web portal that connects to ICANN. If all flags are checked there it could technically in an easy manner pull the data from CP's.

ADD: b4) What process should be followed for a data controller to dispute a credential?
NOTE: The controller should contact the credentialing body and provide information as to why it disagrees with the issued credential. The credentialing body should have a designated point of contact and/or process for reviewing these disputes.

(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?
NOTE: Should be only applicable laws

c2) What rules/policies will govern users' use of the data once accessed?
NOTE: Should be dictated by applicable laws and best practices and be only for the original purpose.

c3) Who will be responsible for establishing and enforcing these rules/policies?
NOTE: The question is who or what can legally enforce the rules/policies globally and how would it work? Currently the only international legal body is the Hague International Court of Justice, which is not recognized by all countries in the world. Therefore, unless the SSAD is jointly operated by governments, enforcement could be a deal breaker/show stopper. If ICANN takes on any of this liability, what guarantees do CPs get?

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 ADD: and/or data processors whose data has been abused in addition to any sanctions already provided in applicable law? ADD: How can enforceability of sanctions and payment of compensation be ensured to avoid contracted parties being left with the responsibility?

c5) What kinds of insights will Contracted Parties have into what data is accessed and how it is used?
NOTE: CPH should discuss this within their respective SG's and supply the EPDP WG with a procedure and requirements. The data subject has a direct relationship with the CP, and so the CP needs visibility into all queries, with the ability to deny requests.

c6) What rights do data subjects have in ascertaining when and how their data is accessed and used?
NOTE: In general best practices should be used. Data protection law requirements and applicable law need to be complied with and could involve several different procedures. This question is very

complex as there might be scenarios where LEAs request data but the data subject cannot be informed as that could compromise the investigation. As always, the LEA must follow due process, and the data subject's rights must be protected.

c7) How can a third party access model accommodate differing requirements for data subject notification of data disclosure?
NOTE: As we have little to no experience with this, it is best that at first everything is manually evaluated. At a certain point automation can kick in. This approach, while possibly labor intensive at first, at least gets the project going as opposed to trying to automate and predict the unknowns, which usually stalls entire projects. Also new technology might emerge during the operational phase which cannot be predicted by the WG.

ADD: c8) What requirements, if any, should be implemented to processing of disclosed data by third parties (security, deletion timeframes, prohibitions on further transfers, etc)?

Annex: Important Issues for Further Community Action

The purpose of this Annex is to set forth implementation issues raised during the course of development of this Temporary Specification for which the ICANN Board encourages the community to continue discussing so that they may be resolved as quickly as possible after the effective date of the Temporary Specification. This Annex does not create new or modified requirements for Registrar or Registry Operator, nor is it intended to direct the scope of the Policy Development Process, which will be initiated as a result of the Board's adoption of this Temporary Specification.

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.

   NOTE: The WG should bring itself up to speed with the latest/final version of the Guidelines on Certification, following public consultation of Annex 2. Which is available at the EDPB website:
   https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

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.

3. Developing methods to provide potential URS and UDRP complainants with sufficient access to Registration Data to support good-faith filings of complaints.

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.

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.

6. Limitations in terms of query volume envisaged under an accreditation program balanced against realistic investigatory cross-referencing needs.

7. Confidentiality of queries for Registration Data by law enforcement authorities.

Phase 1 Recommendations

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.

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.

EPDP Team Recommendation #4.
The EPDP Team recommends that requirements related to the accuracy of registration data under the current ICANN contracts and consensus policies shall not be affected by this policy.6
Footnote: The topic of accuracy as related to GDPR compliance is expected to be considered further as well as the WHOIS Accuracy Reporting System.

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.

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.

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. 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.)

(....)