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.

Submitting Organization Information

a. Please identify your SO/AC/GNSO Stakeholder Group / GNSO Constituency:

Noncommercial Stakeholders Group (NCSG)

b. Please identify the member(s) of your SO/AC/GNSO Stakeholder Group / GNSO Constituency who is (are) participating in this EPDP Team:

Amr Elsadr, Ayden Férdeline, Farzaneh Badii, Julf Helsingius, Milton Mueller, Stephanie Perrin

c. Please identify the members of your SO/AC/GNSO Stakeholder Group / GNSO Constituency who participated in developing the perspective(s) set forth below:

Amr Elsadr, Ayden Férdeline, Farzaneh Badii, Julf Helsingius, Kathy Kleiman, Milton Mueller, Raphaël Beauregard-Lacroix, Stefan Filipovic, Stephanie Perrin, Tatiana Tropina

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 NCSG's representatives on the EPDP Team, and then shared with the NCSG's 800+ individual and organizational members for review, input, and further refinement. It was then reviewed and endorsed by the NCSG Policy Committee in accordance with our charter and internal operating procedures.

e. Please identify a primary point of contact with an email address in case any follow-up is needed:

The NCSG's representatives on the EPDP can be reached at: epdp@lists.ncsg.is

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.
Thank you for this opportunity to provide input.

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?

The answer to this question is highly dependent on who the third party is and the jurisdiction in which they operate and the jurisdiction in which other parties, including the data subject, are resident in. The NCSG does not consider it appropriate for the EPDP team to attempt to tackle this question, because the activities of third parties fall well and truly outside of our knowledge and control. We stress that simply because third parties have expressed their need to access personal information does not justify disclosure. Under the GDPR and other data protection laws and regulations, the legitimate interest of the third party should be interpreted narrowly and established with a clear and specific outcome in mind. Rather, the NCSG recommends that the following questions instead be asked:

- **Over the past 12 months, have the legitimate interests enumerated by third parties been used by registrars to disclose the personal information of domain name registrants?**
- **Do the use cases that involve third parties processing personal information provide a concrete outcome or benefit?**
- **Can the outcome of disclosure be achieved through other means?**

a2) What legal bases exist to support this access?

Legal bases are specified in Article 6 of the GDPR. They are limited and specific, and do not apply to each requesting entity every time (a particular conflation that we have argued against multiple times). We have gone over this at some length already in the EPDP. We will not repeat ourselves here, except to stress that there is no blanket clause that can be used to create a simple, unified access engine.

a3) What are the eligibility criteria for access to non-public Registration data?

This is not a precise question. A party is not by its very identity eligible or ineligible, it depends on the purpose and whether that purpose is legitimate and proportional. The purposes are described in Article 6, thus a legitimate, authenticated third party who qualifies to request under one of these purposes is "eligible". Then the request must be evaluated for scope and proportionality. We caution against using consent. Many jurisdictions are finding that consent it difficult to manage, as individuals who data is requested are unlikely to be capable of fathoming the extent of onward transfer and use, in an age of big data.

a4) Do those parties/groups consist of different types of third-party requestors?

The disclosure of personal information to a third party requestor is variable and dependent upon the stated legal basis of the request. It is vital that the disclosing party determine the identity of the requestor, and assures that this requestor in fact represents the organization or entity that he/she purports to represent, and that the purposes for disclosure of personal data are accurately stated.

Obviously, given that anyone can request access to personal data if they have a valid and legitimate purpose to request it, and the DNS does have a public function and impact (as opposed to, for instance, someone requesting access to somebody else's health or financial data), there could be an infinite number of types of individuals or groups requesting access to data. We do not see the value in attempting to forecast the scope of the potential user group.

a5) What data elements should each user/party have access to based on their purposes?

The data elements that would be released to a third party would depend on the nature of the specific request and would vary from case to case. The NCSG supports the proportionate release of personal information in justified circumstances, and would not support more personal information than necessary being shared with a third party.

We note Article 6(f) requires that "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." This requires that, in appropriate cases, the "purposes" of the requestor be weighed against the danger to the data subjects (registrants), especially when their fundamental rights and freedoms are involved.

We note that complexities for processing of Whois requests are likely to arise in cases involving "sensitive data" under Article 9 -- where the "processing of personal data" reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" as well as "data concerning health or data concerning a natural person's sex life or sexual orientation." Accordingly, for certain human rights, LGBTQ, minority political and religious organisational registrants, their members (often named as contacts in the Whois with their addresses) will require a more thorough evaluation prior to disclosure of data that may well impact their rights and freedoms.

As discussed above, the jurisdiction of the requestor may raise issues and possible dangers. An EU resident serving as a webmaster/Whois contact/member of a LGBTQ group may also be a Nigerian or Kenyan citizen (countries where LGBTQ activities are now banned and heavily penalized). What danger exists in relation to the disclosure of data, and danger to "fundamental freedoms and rights" should the request arise in

Nigeria or Kenya? Similar concerns arise in response to requests of Whois data from countries which engage in collective punishment against family members (e.g., even if the organization's registrant is unreachable, family members might be reachable once a member's name is disclosed). The danger to minority religious and political groups by a third party in a jurisdiction hostile to that minority -- dangers of arrest, death, persecution for association with the protected organization -- would require an inquiry beyond the "stated legal basis of the request."

In addition to noting this concern during this discussion of developing a UAM, we wish to note that there is very scanty information available to domain name registrants currently with respect to who has access to their personal or confidential data, and how. This needs to change drastically under the GDPR.

a6) To what extent can we determine a set of data elements and potential scope (volume) for specific third parties and/or purposes?

This seems to be the wrong question. First, let's figure out who the data controller/joint controllers are. Then, let's do a data protection impact assessment (DPIA) for requestors who want access routinely to certain types of data. All we have heard so far is expressions of need/desire for continued access to data, not the demonstration of that need and estimated volumes.

A comprehensive DPIA and associated risk assessment will need to assess the purpose for processing personal information and what data elements, if any, are justified in such a case. The NCSG suggests that the EPDP explore these questions – of fair evaluation of the Article 6(f) proportionality protections for the interests or fundamental rights and freedoms of the data subject *prior to disclosure* as well as well as safeguards against the misuse of registrant data elements – as a matter of priority.

We note that ICANN's ability to enforce against misuse of registrant data elements after disclosure in a global environment will be limited and, hence, protections *prior to disclosure* as mandated by GDPR for personal and sensitive data must be made. A comprehensive risk assessment should be done to determine means to measure the negative impact of information disclosures.

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?

If the EPDP team agrees to having an accreditation model, then we can discuss the best way to implement it. First, the relying parties (i.e. the data controllers/co-controllers, let us assume we are talking about the contracted parties here for the sake of brevity) need to do a risk assessment of the accreditation processes. How can they be assured that an individual who claims to be a law enforcement agent, IP attorney, accredited cybercrime investigator etc. has been reliably accredited to

receive a token? We do not think that accrediting a legitimate purpose will be easy, and are looking forward to discussing this separate problem once we get there.

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

We first need to ask what is the best way of having a harmonized disclosure policy in place, and whether or not credentialing is even necessary?

We do not accept the concept of credentialing if it means a kind of access where, for instance, every law enforcement officer or IP attorney gets a token to get access to a stream of data. We acknowledge the utility of providing credentials for contact points in different agencies or governments, and in certain entities. But it is not clear that we have defined and constrained these terms closely as yet.

b1) How will credentials be granted and managed?

If it is determined by this working group that credentialing is necessary, and that is not a given, we will need to explore what auditing functions are required to ensure that credentials are not abused, misused, stolen, or shared with someone other than the credentialed party. Credentials must not be issued permanently but for a time-limited period with regular re-verification that the party has a need to or is authorized by an entity to request registration data. Credentials must be issued to individuals and not to entities.

b2) Who is responsible for providing credentials?

It would be premature of us to respond to this question at this time. This is a big policy question. Who will take on the responsibility for vouching for the use of credentials by an entity? There is your answer, and there are many associated policy questions, such as who is auditing these processes, what is the fail rate, etc.

b3) How will these credentials be integrated into registrars'/registries' technical systems?

We defer to the registrars and registries to answer this question. Liability hangs from the answers to b2 above.

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

As discussed above, we assume one-time access each request. If there are other assumptions, they need to be interrogated, we suggest a DPIA and complete risk assessment.

c1) What rules/policies will govern users' access to the data?

Foremost, applicable law.

There must be an enforceable attestation that the third party will protect the data in compliance with applicable law, particularly in cases where there is no data protection law in the jurisdiction receiving the data. This includes verification that a third party requestor has the capacity to transmit and store personal information in a secure fashion.

There must also be penalties and sanctions in place for third parties that request registrant data for illegitimate purposes or where it is later found to be unnecessary.

c2) What rules/policies will govern users' use of the data once accessed?

Foremost, applicable law.

Requested data must only be used for the purpose that the user stated was their reason for requesting the data, as supported by a legal basis and, if necessary, their enumerated legitimate interest.

Data must not be retained beyond an agreed retention period (to be determined). The data controller needs to inform the individual concerned that his/her data have been released, in compliance with the applicable DP law.

c3) Who will be responsible for establishing and enforcing these rules/policies?

The data controller(s) are responsible for establishing the terms and conditions of the disclosure, in compliance with relevant law. The recipients must comply with the same provisions, regardless of jurisdiction. It is not the responsibility of the domain name registrant to police this. He/she will have access rights when the data is being held by the recipient, but it should not be simply left to the registrants to manage this.

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?

Significant financial penalties against the requesting third party, and significant financial compensation to the domain name registrant whose personal information has been misused should be considered. Other sanctions, including restrictions on further disclosure requests, may be justified.

C5) What kinds of insights will Contracted Parties have into what data is accessed and how it is used?

There must be a complete audit trail available to any data controller or co-controller.

C6) What rights do data subjects have in ascertaining when and how their data is accessed and used?

All rights guaranteed as per applicable law, including in particular those referenced in Article 15 of the GDPR.

Data subjects must also be notified if and when their data is accessed by a third party, with a rationale offered for the disclosure of their personal information.

C7) How can a third party access model accommodate differing requirements for data subject notification of data disclosure?

Exemptions to the disclosure requirements are routinely managed by countries with data protection law; we can figure this out when we get there. Research is being done on secure untraceable requests, but the rationale for such secure untraceable requests is very restricted in use.

It would be premature for us to respond further to this question.

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.

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.

The NCSG believes that the contracted parties should be permitted to differentiate between legal and natural persons if they so desire, but they should not be obliged to do so, as it is unfeasible in many circumstances.

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.)
(....)