RySG Response to
EPDP Phase 2 Request for SO/AC/SG/C Early Input

Per the request received on 30 May 2019, the RySG is providing the following early input to the EPDP phase 2. Noting the importance of the work being done in this EPDP, the RySG would like to thank the chair, Janis Karklins, ICANN support staff and all the EPDP members for their time and effort. The RySG response includes input on the phase 2 charter questions and sub-questions, items deferred from phase 1 as well as general additional input. The RySG input is in BLUE.

Submitting Organization Information

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

b. Please identify the member(s) of your SO/AC/GNSO Stakeholder Group / GNSO Constituency who is (are) participating in this EPDP Team:
Alan Woods, Kristina Rosette, and Marc Anderson

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 RySG input was open to all members of the stakeholder group for input and review.

d. Please describe the process by which SO/AC/GNSO Stakeholder Group / GNSO Constituency used to arrive at the perspective(s) set forth below:
After receiving the request for early input, an initial brainstorming/drafting session was held that was open to all RySG members. Following that a meeting of the RySG EPDP support team was held to further refine the response. With that as input, support team members completed a draft response. That draft was sent to the full RySG mailing list for review and further edits. Following that review the input document was finalized and submitted. The entire drafting process was done via Google docs and open to all members to participate, edit and comment.

e. Please identify a primary point of contact with an email address in case any follow-up is needed:
Sam Demetriou – sdemetriou@verisign.com

1. Phase 2 Charter Questions

(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?
It is impossible to pre-define what legitimate purposes exist for third parties to access data. Legitimate purposes are limited to the specific circumstances of a particular request, including the type of data involved, the data elements required, the legal basis,

the requestor, the purpose stated etc. The RYSG sees merit in perhaps identifying high level commonalities, however this does not mean we support a 'check box' exercise of Legitimate Purposes, where one size seems to fit all. This would be simply legally unsound. The RySG also notes that this may vary depending on the jurisdiction and who the requestor is.

a2) What legal bases exist to support this access?

Legal bases are limited to those identified in Article 6 of the GDPR.

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

"Access" may only be granted to those who have obtained the fully informed and freely given consent of the data subject.

"Access" may also be granted to specific entities under EU law or Members State law.

"Disclosure" eligibility criteria depend on the stated legal basis of the request:

6(1)a - Consent of the data subject (freely given and fully informed)

6(1)b - disclosure "necessary" to give effect to contract between the data subject and the data controller (in this instance the requestor)

6(1)c - Establishment of a legal obligation on the disclosing controller, i.e. The disclosing controller is required under an EU law / Member State law to disclose the data to a specified requestor.

6(1)d - The requester has established that disclosure is necessary to protect the vital interests of the data subject or another natural person, (NOTE: ICO guidance has confirmed that vital interest is an exceptionally high bar usually equated to immediate threat of loss of life.

6(1)e - The requester, who must verify their request is in the course of their exercising an official authority therein vested, must require disclosure for the performance of a task carried out in the Public Interest. The basis of this processing must be also established in EU or Member State law (Art 6(3)).

6(1)f - The requester must establish necessity, legal basis and provide a valid legitimate interest for disclosure. Eligibility for disclosure is based on the receiving controller's assessment of the request, and the review of all such requirements. The controller may only disclose where the interests and legal basis of the requester are not overridden by the competing interests, rights and freedoms of the relevant data subject, vis a vis the protection of their data.

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

Eligibility is not tied to specific groups of people; eligibility is tied to the legal basis and a consideration of the elements of the individual request. There is a higher degree of viability of such a 'per group' eligibility for those legal bases which require 'official authority'. In such situations it is envisaged that there is potential that where such a legal authority / official authority is sufficiently established, the disclosing controller may not retain discretion in such a disclosure.

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

The required data elements per request must rely upon the specific circumstances of the individual request. At a high level, we do not hold any personal data that might not be potentially released to a 3rd party who has met with the disclosure requirements. Blanket disclosure, however, cannot be permitted based on purpose alone, as necessity for the release of each data element must be established.

a6) To what extent can we determine a set of data elements and potential scope (volume) for specific third parties and/or purposes?
It may be possible to establish sets of data elements which may be a potential 'common' set of data elements based on specific type of requestors, which have identified a particular legal basis; however under the GDPR and in particular with art 6(1)of which shall likely be the basis for the vast majority of cases, there remains a requirement on the 'disclosing' controller to carry out an assessment in any given case of whether or not the legal basis and necessity has been established in that case. This remains a vital aspect of the 'balancing test'.

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?
The technical solution must follow the policy recommendations. The technical solution should support policy, not shape or drive that policy. The RySG recognizes that various work has already been done showing that RDAP is a flexible tool likely to be able to support policy recommendations that will ultimately come out of phase 2.

(b) Credentialing – What are the unanswered policy questions that will guide implementation?
It is as of yet unclear as to the meaning of 'credentialing' in the context of disclosure.

It is accepted that in certain instances, such as under the legal basis of Art 6(1)c , credentialing will be a very efficient manner in which to establish the authenticity of the request and source, and thus the availability of a specific legal power to obtain disclosure. We will, however, caution that under legal basis such as Art 6(1)f, credentialing will be useful to remove the need for the disclosing controller to verify identity, the identity of the requestor is merely one element in the balancing test. Legal basis, necessity and an assessment of all the circumstances of a specific and individual request cannot be circumvented by a credential.

b1) How will credentials be granted and managed?
Should credentialing be deemed appropriate by the working group, credentials must be based upon a well-defined system of applications, verification of applications, and continuing audit. Depending upon the weight to be afforded to the 'credential', there should be scope for suspension and censure for misuse of the credential. Credentials must not be shared by the credentialed person or entity.

b2) Who is responsible for providing credentials?
This is impossible to speculate upon at this time. Regardless, there will, however, need to be a strong legal authorization or agreement which includes adequate, indemnity and a full system of redress between the controller(s)(disclosing) and the certification body.

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

This is impossible to speculate upon at this time. This may not even be necessary in a centralized solution.

(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?
The EPDP Team must address the question of when the purpose associated with a given request for data disclosure (i.e., the user's reason for requesting access to that data) will be assessed. The existing RDDS query process does not currently account for the need to express and assess this data point. The EPDP Team may wish to consider if certain potential users should be excluded from participation based on prior bad conduct or conduct demonstrating an inability to properly secure personal data.

c2) What rules/policies will govern users' use of the data once accessed?
At a minimum, a user to whom data has been disclosed must not (i) use that data for or in connection with any reason other than the reason provided by the user in stating its legal basis and legitimate interest; (ii) disclose that data to any other person not encompassed by the user's credential, legal basis and legitimate interest except in submissions in administrative, regulatory, or judicial proceedings; (iii) use that data beyond any time period stated as a condition of disclosure.

c3) Who will be responsible for establishing and enforcing these rules/policies?
It is premature to determine who will be responsible for establishing and enforcing these rules/policies, but users should not be responsible for doing so.

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?
Graduated sanctions, including prohibitions on requesting further disclosures, termination of credentials and financial penalties, should apply to users who abuse the data.

c5) What kinds of insights will Contracted Parties have into what data is accessed and how it is used?
Data subjects are the customers of Contracted Parties. Contracted Parties must have full visibility into what data has been disclosed, to whom, and in furtherance of what identified interest. Establishing such an 'audit trail' is also a basic requirement under the GDPR (Art 15(1)(c)), and the relevant contracted party in this instance, must be in a position to fully inform the data subject of such a disclosure.

c6) What rights do data subjects have in ascertaining when and how their data is accessed and used?
The entire basis of Data Protection law is to ensure transparency for the data subject regarding the manner in which processing of their personal data occurs. Controllers MUST be able to demonstrate to whom and for what reason any of their personal data was disclosed to any 3rd party.

See Art 15, GDPR

"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

…
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;"

c7) How can a third party access model accommodate differing requirements for data subject notification of data disclosure?
The answer to this question really depends on the level of disclosure that occurs. The creation of any centralized platform for access will likely, from a privacy by design standpoint, necessitate full disclosure of the existence of such an entity whose purpose is the disclosure of registrant data to third parties. Such a notification will have to occur prior to collection of data (i.e. prior to the processing occurs). Expected disclosure on such an organized scale outside of the purpose for which the data is collected, so much so that it necessitates a separate entity to manage, is exceptionally rare and is frankly unusual (this is as opposed to those registers which find a basis in law e.g. company registers, register of directors, electoral registers).therefore the RySG would recommend, if not insist, that any disclosure made via a centralized platform should always be notified to the data subject.

2. Items Deferred from Phase 1

a. *Feasibility of unique contacts to have uniform anonymized email address*
The RySG maintains its viewpoint that an anonymized email address continues to be both an email address and personal data. Creation of an 'anonymized' address therefore does not really create any additional protection for the data subject, merely creates an additional responsibility to protect a new element of personal data, that was created by us.

As such the RySG is opposed to this unnecessary endeavor, as it does not solve, it merely compounds the matter.

b. *Legal vs. Natural persons*
The RySG maintains its support for the first part of Recommendation #17 from Phase 1 and believes that Registrars and Registry Operators should continue to be permitted to differentiate between registrations or legal and natural persons, but not be obligated to do so.

c. *Additional purpose for ICANN's OCTO*
During Phase 1 of the EPDP, ICANN specifically stated that OCTO does not presently require or use personal registration data in its research. The RySG reiterates the comment it made on the Phase 1 draft Final Report, where we noted that the EPDP

Team's inclusion of a Purpose for *potential future* uses of personal data by OCTO would directly contradicts GDPR requirements that Purposes not be speculative. We believe this matter should be given a very low priority in the Phase 2 work.

d. *Display of information of affiliated vs. accredited privacy / proxy providers*
There is neither sufficient delineation nor detail in the use of P&P providers to ensure that the CPHs are not knowingly facilitating personal data breaches. There is no uniformity in the data elements that are populated as a result of the use, by a data subject, of a P&P service. Some instances rely on anonymized outputs (e.g. privacycustomer87687634@Privacy.com) whereas some rely on a generic and single contact. (e.g. Privacyprovider@provider.com). There remains no manner in which all such contacts may be 'published' as to do so would be to knowingly invite breach.

The RySG reiterates our position that this is a matter for a separate PDP or similar to remedy, and not for the EPDP to encroach upon. Such a PDP may then, as necessary with Privacy by default and design in mind, create or impose a system to ensure such an option of publication can be achieved without a high potential for personal data breach.

e. *City Field*
The RySG, noting the legal opinion of Bird & Bird, accepts that there is a heightened risk in the publication of the 'City' field, and would be supportive of redaction until such a time as the risk is lessened.

f. *Data Accuracy and the WHOIS Accuracy Reporting System*
The RySG would like to note that data accuracy and the WHOIS Accuracy Reporting System are completely separate matters.

With regards to the data accuracy (as is referred to Art 5(1)d), we defer to and accept the legal opinion of Bird & Bird, and note that the concept of accuracy under the GDPR is that data must be accurate for the purpose to which such data are to be used, and methods to ensure "accuracy" must be commensurate to that use and purpose, including whether or not the accuracy of the data has a noted impact on the data subject's rights, thus, necessitating a higher degree of verification. In the domain industry, as agreed by Bird & Bird, the use for the data is to ensure contactability. Bird & Bird have concluded that the required verification steps upon registration and the annual requirement to re-verify contact data ensure ongoing contactability. Unless there are specific limitations as to the class of registrants (eg. certain TLD eligibility requirements), where registration is dependant on a heightened degree of verification, then the expected level of accuracy for the registration (i.e. contactability of the registrant) is met. Where contactability is not established, then there is a process for requiring update, and a consequence (suspension) for a failure to do so.

The RySG reminds the EPDP that accuracy of data subject data, is as per the instruction of the data themselves. Should a data subject express to the controller that data held is inaccurate, then under the right to rectification (also Art 5(1)d), then the controller must

ensure that the data held is updated to reflect the instruction of the data subject. We do not retain any additional or heightened expectations of 'accuracy' as is claimed by some members.

1. Additional Input

Design and implementation of standardized, centralized model must be cost neutral for Contracted Parties. Users of the model must bear some costs for using the model.

The RySG believes that any standardized model must be legally compliant and not place a significant operational burden on Contracted Parties. The RySG acknowledges the necessity of some level of automation but believes it will not be possible to develop a fully automated model that is legally compliant. It is worth noting that not all automation has to be on the "back end" of responses to requests. Opportunities exist for automation on the front end that can help the disclosing party process requests more quickly or efficiently.

We must also note that the creation of a centralized model is not a legal requirement for any contracted party. As controllers, we have legal obligations to meet with regards to data protection and we undertake to meet our legal obligations, lest we are censured by the proper authorities. The RySG are engaging in this process in utmost good faith, so as to attempt to make to process more streamlined and predictable for the community as a whole. We will not however merely accept any situation whereby we are forced to accept a system, where we have reason to believe that such a system only serves to unnecessarily heighten our liability, for the 'ease' of others.

We also remind the EPDP team that our goal is to establish a process which is compatible with the law. The existence an indemnity as a 'cushion' against potential illegal action is not an acceptable result. Any contractual obligation which may be agreed c between the contracted parties and ICANN Org, must remain, at a minimum, compatible with applicable law, lest it be rendered unenforceable. The RySG will continue to strive in good faith towards the creation of such a system, but where such a system is not legally possible, we may have to accept that such a system may not be ultimately recommended by the team.