Small Team #1 – Charter Question H – Applicability of Data Processing Requirements (natural vs. legal person)

For EPDP Team consideration:

The small team deliberated on the following proposed responses to the charter questions and preliminary recommendations in relation to this charter question but please note the positions as outlined below were expressed in relation to the preliminary recommendation. As such this these preliminary recommendations do NOT have the consensus support of the small team but are provided here to illustrate the discussions to date.

h) **Applicability of Data Processing Requirements – Draft responses**

h3) Should Contracted Parties be allowed or required to treat legal and natural persons differently, and what mechanism is needed to ensure reliable determination of status?

We seem to have agreed that yes, contracted parties should be allowed to treat legal and natural persons differently but the mechanism by which this should or can be done should be further explored.

h4) Is there a legal basis for Contracted Parties to treat legal and natural persons differently?

We agreed that under GDPR there is a legal basis. While the focus of this EPDP is GDPR compliance, we did note that not all jurisdictions have this same distinction so we have to make sure our policy recommendations are flexible enough to take this into account.

h5) What are the risks associated with differentiation of registrant status as legal or natural persons across multiple jurisdictions? (See EDPB letter of 5 July 2018).

The main risk seems to be that while legal persons don't have the same protections under GDPR, natural persons employed by a legal person (and who may be designated as the registrant, admin or technical contact) are still natural persons with rights/protection under GDPR. This risk may be minimized through educational resources as recommended below.

Draft Policy Recommendation for inclusion in the Initial Report

The EPDP Team recommends that:

- The distinction between legal and natural persons is useful and necessary for GDPR and other data protection laws. However, the EPDP Team recognizes that there are challenges of making this distinction in the context of domain name registrations as well as the potential implementation of any kind of mechanism that would apply to hundreds of millions of pre-existing registrations.

- The EPDP Team recommends that GDD staff who will be tasked with the implementation of these policy recommendations already commence research by investigating how ccTLDs

currently distinguish between natural and legal persons so that this information can serve as a starting point for the Implementation Review Team.

- The EPDP Team recommends that an Implementation Review Team explores in a timely manner how this distinction can be made in the context of domain name registrations in a satisfactory way. Once the Implementation Review Team has completed its work and has a satisfactory manner in which contracted parties are able to distinguish between legal and natural persons, contracted parties will be required to distinguish between legal and natural persons.

- The Implementation Review Team should also consider the timeline needed to implement this requirement which could follow a phased approach whereby implementation would start immediately following completion of the further work and agreement on a satisfactory manner to distinguish between legal and natural persons for new registrations while existing registrations would be phased in upon renewal or by other means.

- The Implementation Review Team will also recommend which data fields (if any) need to be added to accomplish this distinction. This could require further liaising with the IETF if data fields in RDAP need to be added or changed.

- The EPDP Team recommends that registries, registrars and ICANN develop (educational) resources available that help registrants understand the distinction between a domain name that is registered by a natural person vs. legal person / entity. (educational resources). These resources and communications should also encourage legal persons to provide non-personal information for their email address and other contact information.

Positions expressed in relation to the Preliminary Recommendations

- IPC: After consulting further with my constituency and consistent with previous comments the IPC has made on this topic (including our Early Input comment [1]), we do not agree that contracted parties should have the option to apply GDPR to data where processing is not subject to the GDPR (as currently specified in Appendix A.3 of the temp spec) and believe contracted parties MUST make the distinction between natural and legal persons.
- BC: The BC supports the comments of the IPC
- ALAC: My personal position is that I strongly agree. I am requesting a position form the ALAC. I believe that that this issue must be settled within the EPDP and not in some future group. Although an IRT will surely have some involvement in finalizing the details, it cannot be left to the IRT to address the really difficult questions.
- RrSG: I support most of Marc's [RySG] points, below. The more we examine this issue, the further afield we stray from the critical path of the ePDP/Temp Spec.
  While it is true that (current) data protection law only applies to natural persons, our existing systems do not have the capability to make this distinction, and developing this capability (and associated rule sets) will take more time than we have.
  I agree with Alan [ALAC] that ultimately we should be moving in this direction. Some Registrars, like GoDaddy, infer that the Registrant is not a natural person if the Registrant Organization Field is not empty, but this is not standard across the industry.
  Given the limited time and scope of this ePDP, I think the most appropriate outcome for our report is to make a recommendation for best practices in using/interpreting the Registrant Organization field, and refer this for follow on policy work.

- RySG: after reviewing this with my registry colleagues I must report that we are unable to support this document or the recommendations in it.
  As a general comment, registries are concerned that this doesn't look at the critical issue of the temporary specification which is compliance with GDPR. The first question the small team considering natural vs. legal should have addressed is what policy recommendations are necessary due to the GDPR. These recommendations seem focused on items not on the critical path to policy recommendations on GDPR compliance needed when the temporary specification expires and are better addressed at a later phase.
  The first recommendation is more of a statement not containing a recommendation. While we agree that a distinction between legal and natural person may be useful and desirable it is not clear that it is necessary.
  The second recommendation is for GDD staff to research ccTLDs who distinguish between legal and natural persons and suggests using that as a starting point. It may be interesting and useful to look at how ccTLDs are doing this however registries disagree with using that as a starting point. There is concern that some of these existing implementations are less than ideal solutions and instead might be more useful in highlighting the potential challenges and pitfalls.
  The next couple bullet points pertain to a recommendation that an implementation review team (IRT) be formed to work on the details of how to distinguish between legal and natural persons. Registries are not supportive of this approach favoring either a separate working group focused on this question or addressing it during a later stage of this working group. This approach leaves too much to the IRT without providing clear policy guidance or direction. Similar to the points raised during our second call, we are concerned that such an IRT would struggle noting the challenges and long timelines plaguing recent IRTs.
  The recommendation for registries, registrars and ICANN to develop education resources is vague. It's unclear how this would be implemented or if it would achieve the apparent goal of encouraging legal persons to provide RDS contact data that does not identify a natural person. This is in response to the challenge that even though legal entities aren't covered under GDPR, the natural persons who own or work for these legal entities are covered. Ultimately this will need to be addressed in the policy recommendations.

Background:

See https://community.icann.org/x/6gO8BQ and https://community.icann.org/x/jwq8BQ for meeting notes.

Small Team #2 – Charter Question H – Applicability of Data Processing Requirements (geographic basis)

For EPDP Team consideration:

---

h) Applicability of Data Processing Requirements – Draft responses

Charter question h1) Should Registry Operators and Registrars ("Contracted Parties") be permitted or required to differentiate between registrants on a geographic basis?

1. The group seems to agree that contracted parties should be permitted to differentiate on a geographic basis, but there is not agreement whether differentiation should be required or explored.
2. The members who believe geographical differentiation should NOT be required identified several concerns. Specifically, those not in support noted:

- the actual location of the registrant is not alone dispositive of whether GDPR applies especially because of the widespread industry use of additional processors (e.g., backend registry service providers and resellers for registry operators and registrars, respectively).
- data subjects need to be informed at the time of collection about how their personal data is being processed, i.e. what data is collected, to whom it is transferred, how long it is stored etc. Also, information on the data subject's rights needs to be provided, such as the right of access, right to rectification, right to erasure and the right to data portability. Not having a common approach for all registered name holders would give some RNHs these rights, while others would not get such rights. That would potentially lead to two classes of RNHs, which should be avoided.
- ICANN is about "one world - one Internet", i.e., global standards and interoperability. Such interoperability would be lost and fragmentation in the marketplace would occur if there were no requirement for taking a single approach at the global level.
- there are significant liability implications for Contracted Parties if they are incorrect
- any consensus policy needs to be commercially reasonable and implementable, and in the current market place, differentiation based on geographic location will be difficult to scale
- ICANN policies should not create competitive advantages for some contracted parties over others - such as a policy may result in certain ICANN accredited Registrars and/or gTLD Registry Operators to seem less appealing to customers (RNHs) due to their establishment in jurisdictions with less stringent privacy protection

3. The members who believe geographical differentiation SHOULD be required; however, they identified several concerns. Specifically, those in support of required differentiation noted:

- When GDPR was adopted, the global nature of the DNS was not taken into account. It therefore may be shortsighted of the EPDP Team to just focus on GDPR.
- Applying GDPR to all registrants would undermine the role of sovereign states to be able to enforce their own laws and regulations.

- Businesses are always required to take into account local laws when choosing to do business with various countries; therefore, cost is not necessarily a persuasive argument to not require differentiation.
- The Expert Working Group developed a rules engine; perhaps the group can recommend future exploration of the EWG rules engine to see if it is feasible.

4. Some expressed that one option for future exploration could be to consider the EWG rules engine to see if this is a feasible differentiation mechanism or if a differentiation mechanism could be developed in the future.

For background, the EWG Report reflected the consensus position of experts convened by the ICANN Board of Directors in 2012 to propose a new policy for WHOIS that complied with applicable privacy regulations, including GDPR. The EWG Report states:

The RDS could provide for a legal compartmentalization. Specifically, data elements could be tagged according to the applicable law for the data subject (i.e., the Registrant) and treated accordingly. To achieve this legal compartmentalization, the RDS could implement a "rules engine" that would apply the applicable data protection laws to each specific transfer. More specifically, "rules engine" refers to a feature that could be implemented within the RDS to manage (a) the storage, collection and processing of domain name information based on Registrant, Contact, Registrar, Registry, and RDS jurisdictions (represented by the following data elements: Registrant and Contact Country Code, Registrar and Registry Jurisdictions), and (b) data protection laws of the applicable jurisdictions, in accordance with ICANN's future defined policy for the RDS.

The EWG then made the following recommendation:

107. An information system to apply data protection laws (i.e., a "rules engine") and localization of RDS data storage must be considered as two means of implementing the high level of data protection required. This must be ensured through standard contractual clauses, which flow from a logical privacy policy for the RDS ecosystem.

Charter question h2) Is there a legal basis for Contracted Parties to differentiate b/w registrants on a geographic basis?

Yes, there is a legal basis for contracted parties to differentiate b/w registrants on a geographic basis. However, the location of the registrant alone is not a dispositive indicator if the GDPR applies. If the controller or any processor is within the EU, the GDPR will also apply.

Small Team #3 – Charter Question J – Temporary Specification and Reasonable Access

For EPDP Team consideration:

Draft Policy Recommendation for inclusion in the Initial Report

The EPDP Team recommends that the current requirements in the Temporary Specification in relation to reasonable access remain in place until work on a system for Standardized Access to Non-Public Registration Data has been completed, noting that the term should be modified to refer to "parameters for responding to lawful disclosure requests". Furthermore, the EPDP Team recommends that criteria around the term "reasonable" are further explored as part of the implementation of these policy recommendations addressing:

- [Practicable]* timelines criteria for responses to be provided by Contracted Parties;
- Format by which requests should be made and responses are provided;
- Communication/Instructions around how and where requests should be submitted;
- Requirements for what information responses should include (for example, auto-acknowledgement of requests and rationale for rejection of request);
- Logging of requests.

[*Some concern expressed that timeliness that should not be translated into requirements that are impractical for contracted parties]

BACKGROUND – notes & action items from small team #3 meeting

Notes & Action items

These high-level notes are designed to help the EPDP Team navigate through the content of the call and are not meant as a substitute for the transcript and/or recording. The MP3, transcript, and chat are provided separately and are posted on the wiki at: https://community.icann.org/x/2IpHBQ.

1. Roll Call & SOI Updates (5 minutes)

- Attendance will be taken from Adobe Connect - Attendees: Alan Woods (RySG), Alex Deacon (IPC), Ashley Heineman (GAC), Benedict Addis (SSAC), Farzaneh Badii (NCSG), Hadia Elminiawi (ALAC), Kurt Pritz (Chair), Mark Svancarek (BC), Rafik Dammak (GNSO Council Liaison), Thomas Rickert (ISPCP), Volker Greimann (RrSG Alternate)
- Please remember to mute your microphones when not speaking, and state your name before speaking for transcription purposes.
- Please remember to review your SOIs on a regular basis and update as needed. Updates are required to be shared with the EPDP Team.

j). Temporary Specification and Reasonable Access
j1) Should existing requirements in the Temporary Specification remain in place until a model for access is finalized?

- The team will try to focus on the nature of what makes access reasonable without going into specifics as that is to be covered as part of the system for standardized access to non-public registration data, as part the charter.
- Focus on the questions that are posed as part of the charter.
- Should Temp Spec requirements remain in place for now? Yes, way it is currently phrased is as far as it can be put for now. Access must be reasonable but cannot delve much further as who could test what reasonable is - who would enforce that? Not ICANN's place to interpret what is in effect a legal obligation (balancing test and assessing legitimate interest). ICANN could maybe look at time limits - what is obviously reasonable from a timing perspective, but anything else would need to go to a Data Protection Authority. What are high level requirements that can put on contracted parties that do not stray into the legal arena?
- Need to distinguish between legal issues and more practical/high level such as time limits, form for making requests, response to the request, were reasons given for not providing access.
- Need to maintain the elements that ensure predictability in requesting and receiving a response to access requests.
- Also need to consider cross-border transfers of data, applicability of jurisdiction.
- Consider adding or changing lawful to reasonable. Also, should a different term be used like disclosure? Access sounds like a self-service, which is not what is intended here. For example, Parameters for responding to lawful disclosure requests? Temp spec only makes references to access for third party legitimate interests, there are also other reasons for which data may be disclosed such as UDRP (6.1b), LE requests (6.1c), protecting vital interests (6.1d), so catalogue of legal basis for disclosure, or just change to lawful disclosure. Some note that reasonable should be kept in there.
- Timelines may differ depending on the nature of the requests, for example, life/death situations would require a shorter turnaround time than other requests.
- What criteria should be considered? Depends on the party that is asking and the party that must provide a response. May be difficult to do this further than 'reasonable'.
- Temp Spec requirements should remain in place until overall framework has been developed. Issue is in current environment that there is no consistency as to what reasonable currently means - what is the process and what can be expected? Some methods to ensure that there is at least a response. Such criteria could include timeliness criteria, including timeline to provide a response, criteria around what is required in a request (currently each registrar has its own set of requirements), if request is rejected, should contain rationale to why it was rejected. Mechanism by which to make the request, incl. instructions, could also be part of this.
- Ensure predictability around access and make role of CPs easier.
- Criteria: conforms to local law and the balancing test, appropriate to the purpose, responsive, has to be legible, auditable.
- Reasonable access cannot be defined by EPDP it's a legal question. J1(a)(2) criteria as laid out by law and a standard disclosure framework. Is this possible before other charter questions have been answered?
- Objective is to find criteria that are win-win for both requestors as well as contracted parties.
- Not objective of EPDP Team to consider every single LE jurisdiction - can only do it in general terms in compliance with GDPR.
- Where is the group at: get terminology as precise as possible (using disclosure instead of access), everyone agrees with question j1 - yes, should remain in place, beyond legal issues and balancing that CPs will be responsible for, concrete suggestions for criteria (timeliness,

responsiveness, what needs to go into a request as well as response) that should be developed around reasonable disclosure.

- Possible draft recommendation:
  The EPDP Team recommends that the current requirements in the Temporary Specification in relation to reasonable access remain in place until work on a system for Standardized Access to Non-Public Registration Data has been completed, noting that the term should be modified to refer to "parameters for responding to lawful disclosure requests". Furthermore, the EPDP Team recommends that criteria around the term "reasonable" are further explored as part of the implementation of these policy recommendations addressing:
  - [Practicable]* timelines criteria for responses to be provided by Contracted Parties;
  - Format by which requests should be made and responses are provided;
  - Communication around how and where requests should be submitted;
  - Requirements for what information responses should include (for example, rationale for rejection of request);
  - Logging of requests.

  [*Some concern expressed that timeliness that should not be translated into requirements that are impractical for contracted parties]

Action item #1: Staff to put notes and draft recommendation up as a google doc for small team to review and further edit before this is shared with the EPDP Team.

Action item #2: Small team to provide input by Sunday 13 October COB in view of sharing proposed recommendation with the EPDP Team early next week.