EPDP Team F2F Meeting Day 2

Wednesday, 17 January 2019

Notes and Action Items

Outcomes from Day 2 – EPDP Team F2F – Toronto

Following review of public comments received, the EPDP Team agreed to include the below Purposes and Recommendations, as worded below, in its Final Report. No objections were registered.

Purpose 2

Contributing to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission through enabling responses to lawful data disclosure requests.

Recommendation 2

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[1] and DNS abuse cases.[2]

There is a need to confirm that disclosure for legitimate purposes is not incompatible with the purposes for which such data has been collected.

[1] Purpose 2 should not preclude disclosure in the course of investigating intellectual property infringement.
[2] The EPDP recognizes that ICANN has a responsibility to foster the openness, interoperability, resilience, security and/or stability of the DNS in accordance with its stated mission (citation required). It may have a purpose to require actors in the ecosystem to respond to data disclosure requests that are related to the security, stability and resilience of the system. The proposed Purpose 2 in this report is a placeholder, pending further legal analysis of the controller/joint controller relationship, and consultation with the EDPB. The EPDP recommends that further work be done in phase 2 on these issues, including a review of a limited purpose related to the enforcement of contracted party accountability for disclosure of personal data to legitimate requests.

Purpose 7

Enabling validation to confirm that Registered Name Holder meets gTLD registration policy eligibility criteria voluntarily adopted by Registry Operator and that are described or referenced in the Registry Agreement for that gTLD.[1]

[1] The EPDP Team's approval of Purpose 7 does not prevent and should not be interpreted as preventing Registry Operators from voluntarily adopting gTLD registration policy eligibility criteria that are not described or referenced in their respective Registry Agreements.

Action Items:

Action item #1: Review inputs provided during the discussion on recommendation 13 and provide update language for review during the meeting on Friday.

EPDP Team Outcomes Day 2

Notes and action items – Day 2

Taking Stock of Prior Day

- Add time to meet with John Jeffrey to discuss the Controller memo produced by ICANN Org
- Add some time on the agenda for tomorrow to discuss the format of the Final Report

Recap Day 1 Outcomes and Review Day 2 Agenda and Objective

- See notes from yesterday's meeting and agenda for today

Frame Prioritized Issues for Day 2

- Commence with Purpose 2 and Recommendation 2
- Substantial time already spent on purpose 2 and recommendation 2
- Focus on what has changed and what new perspectives have been offered in the public comment.
- Current language is result of compromise and acknowledging each other's concerns and priorities.
- Questions to consider: What do I need, what are my interests, what I would like to see happen – how would others respond to this? How can I modify my approach to a path that everyone can live with?
- What needs to be addressed now and what can be addressed in phase 2?
- RySG/NCSG/RrSG – are of the view that this potential purpose should be deleted that collecting data for the sole purpose of disclosing it is not valid.
- ALAC – this is necessary and part of ICANN's mission and responsibility.
- GAC – access should not have any impact on security, stability and security. Need to reconsider wording and structure of purpose.
- BC – data is not just collected for the purpose of disclosing, but if data is collected, it should be allowed to be disclosed. Purpose would benefit from more specificity, for example, breaking out in two parts (disclosure to LE and civil disclosure)

- SSAC – objective of this purpose is to explain to data subject that data may get shared outside of our eco system. If this purpose is not maintained, it should be considered how this is addressed.
- ISPCP – if it is confirmed that purpose as written is considered legally compliant, concerns would be addressed. Understands this as a placeholder for the phase 2 discussions. Will need to be more nuanced in phase 2 discussions as current reference to third parties would imply 6(1)f as a legal basis which would exclude LE who need to use 6(1)c. May need to consider who the requestor is.
- IPC – purpose aligns with a 6(1)f under GDPR and the ICANN framework. Important and practical to maintain this purpose. May need to break this down to separate out LE and third party disclosure.
- Legal counsel input: will need to confirm this in writing, but some immediate reactions are 1) reactive disclosure – do you need this purpose to facilitate this, to ensure that registrars respond to requests? No, it is clear that if a controller has personal data for the purposes of running its business and it receives a request from a third party who is entitled to disclosure of the data under the principles of 6.1 you can do so – this purpose is not required. Legitimate interests are not the only requirement on article 6. 6(1)f is the obvious condition to look to for disclosure – appropriate condition also confirmed by case law, but this may not cover all third parties. Also need to accommodate disclosures under other conditions. 2) Do you have to explain this to individuals? Yes, this does have to be clear to individuals. A controller has to make clear under articles 13 and 14, which require controllers to explain the purposes and other material facts, you also need to inform data subject about the recipients of the data. If you are aware that this may include others like LE or intellectual property investigations, this needs to be disclosed. In other sectors this is typically disclosed in privacy notices. 3) Could registrars and others have a purpose for collecting data in order to disclosure it? Can disclosure be a purpose in its own right? GDPR doesn't stop you from doing this if your purpose as an organization is to share data. As a matter of principle, GDPR doesn't stop you from having a purpose to make data available to people – policy question is whether this is a purpose for registrars for why they collect the data, not a legal question. 4) Is this a purpose for ICANN? That is also not a data protection question, that is the result of ICANN's mission.
- Board Liaison: ICANN's mission is clearly stated in the Bylaws and references access to registration data for the secure and stable operation of the DNS.
- BC: how to enable ICANN Org to enforce legitimate access in a consistent manner – the idea is that this purpose would allow for that. Is this purpose required for that and does it benefit us? Objective is to build a global policy that is consistent across the globe.
- Legal Counsel input: if you have an organization who is requesting WHOIS data from one of the participants, what are the rules that apply to that organization? Would they become subject to GDPR? When you look at access to WHOIS data you need to look it at both from the perspective of the organization releasing the data as well as the organization requesting data. The requesting organization would also need a lawful basis to access the data, which may be under a different legal basis than the organization releasing it. LE has a different layer on top. For LE in the EU it is governed by a separate directive. Further work should be undertaken by ICANN in that space. GDPR has its own rules to when it applies and when it doesn't – recipient is not necessarily subject to GDPR. Other questions boil down to how does ICANN and all stakeholders in the room to put in place a system for how ICANN Org can enforce access requirements. Registrars / registries will need to make a determination under 6(1) whether to disclose or not. Further thought needed on what is needed to allow for ICANN Org to set up and manage a possible access model. Will need to come back to the team in writing.

- Legal Counsel input: GDPR requires that personal data has to be collected for specified… as far as registrars and registries are concerned, one alternative form of wording would be to include wording that disclosure in appropriate circumstances is not incompatible with the purposes for which the data was obtained. If the concern is not about ensuring that disclosure can take place, but being able to require disclosure, that is a different point. There has been discussion about ICANN's role and responsibilities vs. that of CPs and others which does impact on this. If this is ICANN's purpose, it does need to get articulated and spelled out.
- Various options were discussed and worked on during the deliberations.
- To address concerns, add a footnote in recommendation 2 – when purpose 2 was written, it was not intended to preclude IP interests. Proposed language for footnote: "Purpose 2 should not preclude disclosure in the course of investigating intellectual property infringement".

EPDP Team Outcome on Purpose 2 and Recommendation 2:
Concerns expressed in the public comment period were considered and addressed. No other objections were noted to the updated purpose 2 language and recommendation 2 as follows:

Purpose 2
Contributing to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission through enabling responses to lawful data disclosure requests.

Recommendation 2 alternative
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[1] and DNS abuse cases.[2]

There is a need to confirm that disclosure for legitimate purposes is not incompatible with the purposes for which such data has been collected.

[1] Purpose 2 should not preclude disclosure in the course of investigating intellectual property infringement.
[2] The EPDP recognizes that ICANN has a responsibility to foster the openness, interoperability, resilience, security and/or stability of the DNS in accordance with its stated mission (citation required). It may have a purpose to require actors in the ecosystem to respond to data disclosure requests that are related to the security, stability and resilience of the system. The proposed Purpose 2 in this report is a placeholder, pending further legal analysis of the controller/joint controller relationship, and consultation with the EDPB. The EPDP recommends that further work be done in phase 2 on these issues, including a review of a limited purpose related to the enforcement of contracted party accountability for disclosure of personal data to legitimate requests.

- Purpose 7 gTLD registration policy eligibility criteria

Current Purpose 7: Enabling validation to confirm that Registered Name Holder meets optional gTLD registration policy eligibility criteria voluntarily adopted by Registry Operator.

- Issues
    - confusion about optional and voluntary
    - request to add "and incorporated into registry agreement"

Proposed Revised Purpose 7: Enabling validation to confirm that Registered Name Holder meets ~~optional~~ gTLD registration policy eligibility criteria voluntarily adopted by Registry Operator ***and that are described or referenced in the Registry Agreement for that gTLD***. [Note: Not technically accurate or complete to say "as incorporated into the registry agreement."]

Proposed Footnote: The EPDP Team's approval of Purpose 7 does not prevent and should not be interpreted as preventing Registry Operators from voluntarily adopting gTLD registration policy eligibility criteria that are not described or referenced in their respective Registry Agreements.

- This is not about additional data that is added to RDDS. Any Registry who would want to publish this data in RDDS would need to go through an RSEP.
- Note, RSEP may need to be added to the list of policies to be reviewed following adoption of the recommendations to ensure consistency.

EPDP Team Outcome on Purpose 7
Concerns expressed in the public comment period were considered and addressed. At least one member of the NCSG did not support the revised purpose 7. No other objections were noted to the updated recommendation language and the new footnote:

Enabling validation to confirm that Registered Name Holder meets gTLD registration policy eligibility criteria voluntarily adopted by Registry Operator and that are described or referenced in the Registry Agreement for that gTLD.

Footnote at the end of the purpose statement: The EPDP Team's approval of Purpose 7 does not prevent and should not be interpreted as preventing Registry Operators from voluntarily adopting gTLD registration policy eligibility criteria that are not described or referenced in their respective Registry Agreements.

- Recommendation 13 – Controller Agreement

- See small team proposed updated language
- See memorandum circulated by ICANN Org earlier this week – controllership is not determined through a policy but a factual analysis is needed to determine if parties involved jointly determine the purposes for the processing activities.
- Code of conduct have specific meaning in RAA that would trigger specific process – need to consider rewording to be used.
- What was the task that was set for legal counsel that resulted in the memo? Would be helpful to see data mapping that was undertaken to make this determination. Further work to be undertaken here, especially to compare notes with contracted parties which could impact the

determination of controller or joint-controller. Were asked to consider the legal issues, not specifically to go into one direction or another.

- How should feedback be provided? EPDP Team to develop questions for ICANN Org consideration.
- Support for path to obtain legal certainty through submission of code of conduct to EDPB.
- Important to nail down ICANN's role. Should consider putting a qualifier in the different recommendations, e.g. on the assumption that…
- Consider scheduling a follow up call with ICANN Org and those interested to address follow up questions / concerns.
- Review of proposed updated language: some expressed concern with moving away from recommending JCA as that may leave uncertainty. As recommendation says 'subject to legal advice' it is still possible to move away from JCA. Others indicated that it is important to leave flexibility as one size fits all
- Joint controller doesn't mean equal responsibilities – those are to be documented in the agreement.
- Updated language proposed by small team: The EPDP Team recommends that ICANN Org negotiates and enters into required data protection agreements such as a Data Processing Agreement (GDPR Art. 28) or Joint Controller Agreement (Art. 26), as appropriate, with the Contracted Parties. In addition to the legally required components of such agreement, the agreement shall specify the responsibilities of the respective parties for the processing activities as described therein. Indemnification clauses shall ensure that the risk for certain data processing is borne by either one or multiple parties that determine the purpose and means of the processing.
- Suggestion to remove reference to "data processing agreement' in small team proposed language.
- Suggestion to update language by adding 'The EPDP Team recommends that ICANN Org enters into a Joint Controller Agreement (Art. 26) unless legal advice or other input indicates a different form of agreement would be more appropriate'.

Action item #1: Review inputs provided during the discussion on recommendation 13 and provide update language for review during the meeting on Friday.