EPDP Team F2F Meeting Day 3

Friday, 18 January 2019
Notes and Action Items

Outcomes from Day 3 – EPDP Team F2F – Toronto

Following review of public comments received, the EPDP Team agreed to the below principles. No objections were registered.

The text provided below will not be included in the Final Report as recommendations; the EPDP Support Staff will circulate draft recommendation text for EPDP Team review and discussion shortly. to include the below Purposes and Recommendations, as worded below, in its Final Report. No objections were registered.

Principles for Redaction of Registrant Organization Field

1. Registrars MAY begin redacting the Registrant Organization field immediately.
2. Registrars MUST notify all Registered Name Holders that the Registrant Organization field will be treated as non-personal data beginning on [a date to be agreed upon during the implementation of this Policy], and accordingly, it will be redacted from the freely-accessible directory beginning on [x date]. If the Registered Name Holder would like its Registrant Organization Name published within the freely-accessible database, it must affirmatively consent to the publication by opting in. If the Registered Name Holder affirmatively opts in to the publication of its Registrant Organization, the Registrar may publish the Registrant Organization Field immediately and/or on the agreed-upon date.
3. If the Registered Name Holder does not affirmatively opt in to the publication of its Registrant Organization field, the Registrar will show the Registrant Organization Field but MAY be left blank.
4. Upon (1) the registration of a Registered Name sponsored by Registrar or (2) the transfer of the sponsorship of a Registered Name to Registrar, the Registrar MUST inform all Registered Name Holders that the Registrant Org field will be redacted unless the Registered Name Holder affirmatively opts in to the publication of the Registrant Org field.

Principles for Redaction of Registrant Email Field

1. Everyone agrees that redacting email address is necessary for natural persons.
2. Proposed recommendation for GNSO Council to consider forming a PDP to consider the communications issues with the pseudo-anonymized emails and webforms required by the Temp Spec
3. Contracted parties have to maintain log files associated with communications between the Registry Operator/Registrar and the Registered Name Holder regarding the transmission of email communications from the Registry Operator/Registrar to the Registered Name Holder. ICANN Compliance could then enforce the maintenance of log files if a complaint is filed.
4. Continue temp spec requirement but create an opening where the registrant can consent to publish an email.

Temporary Spec Expiration/Policy Implementation Gap

1. The EPDP Team could consider the adoption of a transitional policy on gTLD registration data that is identical to the Temporary Specification for gTLD Registration Data.

2. The transitional policy will become effective on May 25, 2019 (date of Temp Spec expiration) and will remain in force until the effective date of the Policy on gTLD Registration Policy.

Action Items

Milton to summarize additionally-noted purposes + proposal to the mailing list (completed)

Questions for ICANN org

1. Why was city redacted in the temp spec?

Recommendation 1 - Additional purposes

Research Purpose ("Purpose O")

- Can this purpose be rolled up in Purpose 2 within the broader discussion on access?
- If this purpose is not based on additional data elements, this would likely be an access question rather than a new purpose.
- The Team should examine if the Temp Spec broke anything related to DNS abuse research
- A data map and the access points as well as the control of the data points is needed in the context of this discussion
- Research is a somewhat privileged position. If research is compatible with the purpose for which the data is collected, a new purpose is not needed.
- Where an organization has the data and wants to use it for research, it does not need to obtain consent b/c the processing is covered under the original purpose. However, the organization would need to give the individual to right to opt out. The right to opt out is not absolute – the organization may override the opt out in some circumstances.
- The situation that is less clear – whether the privileged position would apply to a data controller that does not already have the data it wants to use it for research
- The Team could consider including this purpose in Phase 2 of the team's work. Noting this is the Final Report – that we will more thoroughly review this.
- We need a high level of assurance that if ICANN can justify access to data, the Team can consider new purposes in Phase 2
- SSAC's proposed research purpose is ONLY for ICANN to conduct SSR related research. It was not meant to include any other so-called security researcher.
- We also need to do the work to identify what data elements are personal information.

Accuracy Reporting System (ARS) Purpose

- The critical difference b/w the ARS purpose and the previously-discussed research purpose is the data is not pseudonymized for the ARS purpose.
- If we have a commitment to also address this purpose in Phase 2, that would be acceptable.
- ICANN is another entity that needs access to the data.

- This is being moved to Phase 2 – it may be a new purpose, or it may come with a new solution on how to address that.

Recommendation 1

- Action: Milton to summarize additionally-noted purposes + proposal to the mailing list
- Small Team will meet next week to thoroughly review the workbooks

Recommendations 8 – 10

What issues are new and merit conversation amongst yourselves that merit further conversation?

- Email – the importance of email for communicating with the RNH and making connections using the email address
- Org field
- There is a conflation – there is the legal question of what you have to delete vs. the policy question of what is impracticable to make a distinction of
- City field

Organization Field

- Concern noted – what is the org field contains personal information, such as the name of the registered name holder
- Contracted parties are not generally sympathetic to organizations who use personal information within their organization name. The individual has probably given up some degree of privacy by doing this. Noting that, a few challenges have been identified by registrars. First, the org field is not standardized across all registrars – some treat it is a legal person, others do not. Second, since the temp spec has gone into effect, the org field has been used as an index for other sources to pierce data. Under GDPR, if a data field is not personal information but could be cross-referenced with other data sources to identify a data subject, then it may become personal data. People may be able to reconstruct and patch together personal data if the org field is not redacted.
- This is a currently an optional field, but many organizations want to be identified, and it's important that the option be available to them. Proposed solution – any registrant can go in and clear the org field.
- If the field is not necessary in the first place, you may need consent to collect it.
- It is unlikely the Team will get consensus on if the info of a legal person can be published. It all boils down to the risk of getting it wrong. There will be org fields that contain PII, but the risk comes from two sources: (1) risk that the data subject gets it wrong; (2) sanctioning by the authorities. Is there a risk that the authorities say you have built a systemic risk into your system? There is also the risk of legacy data vs. new data.
- GAC position: the organization field should not be redacted. Recital 14 – protection is for natural persons and not legal persons. There are other instances where European countries publicly give details including the organization names – there are also national registries that publish the information of legal entities.
- Perhaps give registrant the ability to rectify the information in this field b/c some registrants wish for the info to appear publicly.

- It should be very clear what the implications are of filling out the org field.
- This a binary issue – either the field is redacted or it's not. The only middle ground is trading fields. This is legal vs. policy issue – it's very clear if it is an org name that is legally incorporated, there is no reason to redact it. The arguments being made regarding redaction are the risks to privacy. The registrar example of using this information – sophisticated people are using this data for and how easy it is to come up with individual identification based on any information you have.
- With respect to the systemic risk – that is the reason we have audit systems. ICANN can check data in the ARS, so this is not necessarily a binary question. Is there a benefit to having it or not? DPAs will be looking for controls – and a control is audit – ICANN can set up robust programs like audit to address these problems.
- If we need to supplement our systems with extra educational materials, we are not using privacy and design and privacy by default principles. The Team's process and policy need to protect without having to teach individuals about data.
- For legal vs. natural and for geographic – that could be a PDP for later.
- Guiding question – how much of this systemic risk exists for bad actors using the information to cross-reference
- If a RNH is a company or LLP but includes the name of the individual in the company, such as Donna Karen NY – is that personal data? From a UK point of view, no, this is not personal data, however, different member states may different views, so this is not absolute. The UK view is not enough for all stakeholders involved.
- If this does contain personal data, it doesn't mean it can't be published, it means it has to be justifiable under Art. 6. The legal basis ICANN is looking to is 6(1)(f) – legitimate interests. As the team is likely aware, if you rely on legitimate interest, individuals have to have the right to object.
- Would publication of this information allow cross-referencing – that goes to whether publishing this info will affect the justification under 6(1)(f)? Are we going something here that makes is harder to rely on 6(1)(f) in other situations? Would need to look into this further.
- Data minimization – if you could achieve objectives w/o doing this, does that mean you cannot do it? The answer is no. This is more a concept of proportionality. This all turns on if this is justifiable under 6(1)(f).
- There are too many types of organizations

Options for going forward:

1. Recommendation to go forward and try to solve some of these issues.
2. Go forward with optional but note the risks to registrant
3. If you do go forward with optional, reset for legacy (existing users)

Multi-step process:

1. As soon as possible, including this EPDP, begin redacting Registrant org field.
2. Notify all registrants on some future date (1 Jan, for example), registrant org will be treated as non-personal data and will be publicized globally, and in the intervening time, they need to confirm they want it published (informed consent). For registrants who consent, the info could be published immediately or on the agreed-upon date.
3. If registrant does not agree to have their info public says they don't want to put it in there – registrar could blank out registrant org field, so it is published, but empty.

4. New registrants – registrars would be obligated to inform registrants that this is how the org field would be used and registrants would have to OPT IN to publish.

Straw proposal to move forward with – exact language of recommendation to be agreed upon later.

City Field

- Is the city field PII?
- The city field, in smaller cities, can be used to identify people.
- Rr/Ry – on its own right, it's not a huge issue.
- NCSG: we're not in favor of publishing the city, and we should not look at items in isolation. With respect to a law suit, we are talking about what must be published, not what is accessed.
- City helps you determine which law applies by looking at the precedent of the court system.
- If the Team recommends for the City field to be published, the NCSG will register its opposition.
- The NCSG will withdraw its opposition to redacting the state field, in return for redacting the city field. Most questions of jurisdiction (95%) are resolved via nation and province – 95%
- If you go down to city, with cross-referencing info – you can get close to identifying people. The net gain of do you really need to publish this is unclear, especially given the info can be disclosed lawfully.
- Law enforcement prosecutes based on district, so this presents a difficulty – but there are workarounds (as previously noted)
- We do not have a full consensus pathway forward.

Email field

- The utility and value of email is important and should be redacted, other comments – email is personal information and should definitely be redacted. This may be another binary ditch.
- Pro-email publication: option to tell the registrant to not use a personal email. This unduly burdens parties trying to amicably resolve disputes. See the potential risk of unsolicited emails, but think this risk is outweighed by other concerns.
- There are some concerns with the use of web URLs and the pseudo-anonymous emails the Temp Spec requires. There is advice from DPAs on role-based emails could be used for registrants who want to do that. The Team could consider continued discussion for pseudo-anonymous email or anonymous emails.
- The publication of a real email address may outweigh the balancing – it is not just a spam issue – you are publishing an attack vector. A proposal to address concerns about the perceived ineffectiveness of the web form – if it's required for the CPH who is making the web form available, it is required that they maintain logs, and the party has reason to believe registrar is not doing what it is supposed to do, this could be actionable.
- Why are we spending time on whether the email should be redacted? It is a question of how to maintain communication considering the redaction of email. What is not happening that needs to happen?
- For the avoidance of doubt, the IPC – not arguing for fully unredacted email addresses – there are concerns with mechanisms described in the Temp Spec. No response to an email sent does not mean that no email was sent.
- One other proposal – challenge IPC highlighted is legitimate – keep language in temp spec – make a recommendation to GNSO to have another working group explore this further.

- There should be an option that the real email be shown.
- Registrars – there should always be an opt-in to having an email published.

There is no means in the Temp Spec to OPT IN to publishing email.

1. Everyone agrees that redacting email address is necessary.
2. Proposed recommendation for GNSO Council to consider forming a PDP to consider the communications issues
3. Policy recommendation – contracted parties have to maintain logs similar to abuse and if a party believes the messages are not being delivered, ICANN compliance may enforce compliance with keeping logs (to confirm message was sent).
4. Continue temp spec but create an opening where the registrant can consent to publish an email.

- Is there a separate workbook for that issue – maintaining logs?
- Registries would have heartburn over transferring consent to registries, and that there is no expectation that registries would not be publishing that information.

Legal vs. Natural

- Would the team consider adding a field, requiring the team to distinguish if it is a legal person or a natural person?
- if, after affirmatively acknowledging it's a legal entity, then perhaps their information could be published.
- The study could look at the cost, exemplars of other industries that allow. The terms of the study should not be spelled out here.
- There are already some examples of registries who do this, so perhaps we can take a look at there.
- Note: just b/c people are doing it, does not mean they are doing it correctly.
- Also note the study should also explore privacy risk to registrants and also the risks of NOT differentiating.

Geographic Differentiation

- Should the approach be identical to legal vs. natural?
- Fragmentation of the Internet around geographic lines is fundamentally at odds with the ICANN model. Can we dispense with this in Phase 1?
- When you think of geographic distinctions, do you differentiate about how individuals and entities have to conform with local law?
- A contracted party physically located in the EU and a contracted party who is not physically located in the EU but has customers in the EU is a different use case.
- Registrars are able figure out which taxes to charge me based on my address. Don't understand how one cannot turn on and off a switch to redact or not redact based on a country.
- We were not able in the short time to reach unanimous agreement onto geographic diversity
- Need further discussion on may vs. must for distinguishing based on geography

Question for ICANN org: why was city redacted in the temp spec?

IMPLEMENTATION

Issue of the gap b/w when the Temp Spec expires and the effective date of the new policy.

1. The Temp Spec expires, and nothing takes its place, and there is a free-for-all.
2. The idea that a new temp spec will be adopted, or a new spec be adopted – is not preferred by the CPH constituency.
3. Proposal: bridge b/w Temp Spec and new policy. Acknowledgement from the EPDP Team to allow CPH to engage with ICANN org and bring the solution back to the EPDP Team.

Remedies available:

1. Violate the bylaws
2. Change the bylaws
3. Adopt a new temp spec

- The Team could make a policy recommendation – hold in place the temp spec and when implementation work is done, then there is a policy.
- Leery of sunsetting the policy. Board will be worried about that as well – b/c there could be the risk of no contract followed by no policy
- Wrap existing obligations under a new name – they could adopt it.
- We've been asked to continue or change it – we recommend it continue as a board-approved policy to be replaced.
- Transitional policy would be exactly what is currently in the temp spec. If it expires, there would be an enforcement discussion in the community.
- Recognizing the [problem], the EPDP Team recommends the adoption of the transitional policy until the implementation of the new policy is complete.
- It was completely unrealistic to come up a policy in this short timeframe, but we should take a look at the things needed to be changed in the Temp Spec to make it GDPR compliant

Recommendation 12 – Reasonable Access

Issues at stake:

- People were worried this would be difficult – we were pleasantly surprised when we first tackled this. This is about the processing of the request not the results of the request.
- Where the conversation needs to lie is – enough comfort for both the requestor and the company processing the request.
- Need to make this reasonable, practical, and predictable.
- SSAC is in agreement with how RySG phrased it. If we spent time fleshing out the bullet points, it would be great. If there is a predictable format that the requests come in to the CPH and a predictable format for how they go out, it would be better for everyone.
- GoDaddy public comment –also helpful to add categorization of the requestors to that list.
- This is a placeholder – this is not the complete system of standardized access for disclosure.
- Let's not get overambitious with refining it too much.
- We cannot aim for a standardized form – as long we know core elements that should be present, it should be fine.

- The recommendation says nothing until we have the access model – we came to the conclusion that the current process isn't working for anyone.
- These words were put in three months ago from Small Team 3.
- In terms of the use of the word interim, there are requests that fall outside of the procedure, but this is a decision down the road.

Recommendation 14

- Some comments seemed to imply all data elements would be transferred to compliance irrespective of the request; however, the data table represents the aggregate of any data elements the team can request.
- Minimize data element transfer is OK, but don't be too prescriptive.
- More specificity is needed here.
- This is a recommendation to change contracts and make changes to them.
- What would make registries more comfortable with this recommendation is to have a closer review of the workbooks.
- Need to make sure Compliance is still able to do its job, and also revisit the legal basis.
- ICANN is a controller and does not need to apply for access.
- Action item: Support Staff to recirculate previous memo. Re: updating contractual requirements that refers to the data elements that are no longer required to be collected. (completed)
- The small team will NOT be looking at the lawful basis re: processing activities – that is currently an outstanding question to outside legal counsel.
- What we need is to tweak the language to make the original intention clearer. As a result of our policy rec, there may be changes to the registration involved in the processing activity.