2020-05-07 EPDP- Phase 2 call #56

The meeting of the GNSO Temp Spec gTLD RD EPDP – Phase 2 is scheduled on Thursday, 07 May 2020 at 14:00 UTC for 2 hours.

For other times: https://tinyurl.com/yd527psd

PROPOSED AGENDA

1. Roll Call & SOI Updates (5 minutes)
2. Confirmation of agenda (Chair)
3. Welcome and housekeeping issues (Chair) (5 minutes)
   a. Update on SSAD model cost estimate and schedule for review

4. Recommendation #6 – CP Authorization (45 minutes)
   a. Review remaining discussion items (6-22) gleaned from input provided on recommendation #6 discussion table [docs.google.com]
   (see discussion items attached)
   b. Confirm next steps

5. Recommendation #7 Authorization Automated & Recommendation #16 Automation
   1. Review ‘cannot live with’ items identified (see updated recommendations [docs.google.com])
   2. Confirm next steps

6. Recommendations not considered by EPDP <<< reminder: homework on this recommendation is due by 5 May 2020, 23:59 UTC
   a. Review discussion items gleaned from input provided on recommendations not considered by EPDP [docs.google.com]
   b. Confirm next steps

7. Wrap and confirm next EPDP Team meeting (5 minutes):
   a. Tuesday 12 May at 14.00 UTC. TBD
   b. Thursday 14 May at 14.00 UTC. Topics to be addressed: Acceptable Use, Query Policy, Terms of use, Data Retention
   c. Confirm action items
   d. Confirm questions for ICANN Org, if any

BACKGROUND DOCUMENTS

Recommendation 6 Discussion Items - 22Apr2020v1

See email invite with zoom webinar room URL for attendees (observers)

RECORDINGS

Audio Recording
Zoom Recording
Chat Transcript

GNSO transcripts are located on the GNSO Calendar
PARTICIPATION

Attendance
Apologies: Matthew Crossman (RySG), Chris Disspain (ICANN Org Board Liaison)
Alternates: Beth Bacon (RySG)

Notes/ Action Items

Action Items

1. EPDP Team members to review the cost estimate and provide advance questions via the email list by COB Monday, 11 May.
2. EPDP Team members who have not completed their homework on Recommendation 7 and 16 (automation) and Recommendations not considered by COB Tuesday, 12 May.
3. EPDP Team to review and provide input on the discussion table for Recommendation 4 (third party justification) and Recommendation 14 (retention) by COB Tuesday, 11 May.
4. Support Staff to update Recommendation 6 based on today’s discussion and post for EPDP Team review by COB Monday, 11 May.

EPDP Phase 2 - Meeting #56

Proposed Agenda

Thursday 7 May 2020 at 14.00 UTC

1. Roll Call & SOI Updates (5 minutes)
2. Confirmation of agenda (Chair)
3. Welcome and housekeeping issues (Chair) (5 minutes)
   a. Update on SSAD model cost estimate and schedule for review
      - EPDP Team to submit questions/comments in advance of Tuesday’s meeting via the list
      - Xavier will present a high-level overview of the cost estimate
      - The meeting is not mandatory; however, we recommend one member from each represented group attends
      - The nature of the document is to inform the debate- we should not argue over suggested numbers, as these are estimates
   b. Update on public comment proceedings for Initial Report and Addendum
      - Both public comment proceedings (Phase 2 Initial Report and Addendum) have closed.
      - For the initial report, only two additional comments were received and they have been incorporated into the corresponding PCRTs and discussion documents.
      - On the wiki page, rows highlighted in green represent the comments the Team has reviewed
      - For the public comment on the addendum report, staff is working on the compilation. We have received 21 total substantive submissions: 7 groups (2 did not submit), 12 organizations, and two individuals.
      - The addendum PCRTs will be posted to the public comment wiki page – Support Staff expects to complete these by tomorrow.
      - Regarding the calendar, if we do not count this meeting, there are seven meetings remaining. Seven meetings will not provide the group enough time to review all of the comments and suggestions on the remaining outstanding recommendations. Therefore, beginning the week of 18 May, we begin two meetings per week (Tuesday/Thursday) so that we can review all comments by 30 June.
4. Recommendation #6 – CP Authorization (45 minutes)
   a. Review remaining discussion items (6-22) gleaned from input provided on recommendation #6 discussion table (see discussion items attached)
      - Question 5 – can further details be provided regarding the definition of necessary?
      - The reason this language is provided is to reflect the concept of data minimization
      - This definition comes from the opinion of Bird & Bird
      - How this applies to compliance is an implementation issue
      - Answer to ICANN org is review the B&B memo to put the definition in a broader context
      - Should not be handing off the data minimization to the IRT
      - Questions 6 – 8
• Data protection authorities should not be a referral mechanism – that is not their role
• It is not the role of DPAs to get involved in these requests, but there should be an appeals mechanism built into the policy for wrongful denials
• There are other examples of appeal mechanisms in ICANN in the new gTLD process or the UDRP that we could look to – ICANN should create a lightweight mechanism in addition to what already exists
• Who is the decision maker? In the hybrid model, it is the CP. However, the definition of necessary is in the policy so that everyone has an understanding of what can be disclosed.
• Concern over who can compel disclosure – there would have to be significant assurances that the panel would have sufficient expertise in the relevant jurisdictions
• In this situation, who would be held liable for the release of data?
• Understand there is a desire to get a second opinion, the second opinion does not exist b/c where would the liability exist? Unlike that a controller would agree to this
• Not all contracted parties will be subject to GDPR, however the policy will give the ability to all CPs whether the law warrants it or not to deny these requests. Sympathetic to concerns raised here, in many cases – the law will not justify the decision that is made.
• Not all registrars are going to comply – so there should be a data trust or advisory board that will hear the cases and dismiss the spurious ones and act on the bad actors. GDPR cannot take this on. The problem is that if you set up a mechanism, the liability would pass to ICANN as co-controller for establishing the mechanism.
• Support the idea for an advisory panel – if a CP has a pattern of cases found against them, this could feed into a compliance inquiry
• Planning to build a secure logging mechanism for the SSAD – if there is a controller that has an unusually high rate of rejecting requests that are well-formed, that is data to be fed to an advisory panel for systemic offenders
• This is not an appeals mechanism but a request for reconsideration mechanism to give the CP a notice that it may not have handled the balancing test properly. We have to look at what the legal basis for the disclosure is. The vast majority of disclosures will be based on 6(1)(f) – the question is how can you force someone to do that they are entitled but not legally obliged to do? We need to have contractual language whereby CPs who systemically do not apply the requirements properly, ICANN compliance can sanction them. Where the discretion is recognized is an appropriate fashion, the disclosure decision needs to rest with the contracted party.
• Courts are available here, but would a court in the appropriate jurisdiction hear the case in a timely manner? Since the decision rests on the CP and they are not obliged under the GDPR, then it must be contractual language that CPs are obliged to release the data unless there is an overriding reason why they cannot
• It is possible that some registrars may routinely reject or accept every disclosure request. Based on the way some individuals used WHOIS in the past, there may be hundreds or thousands of requests per day. The idea that every discrete request will be subject to reconsideration will not scale. There should be a way to deal with patterns of rejection. Appeals and sanctions need to be considered at a much higher level. If requestors are entitled to this, data subjects must also be entitled to this.
• If there is a cost associated with reconsideration, this will likely be not be abused. Reconsideration cannot only go back to the CP b/c a reconsideration will not change the original determination. Support an advisory panel.
• Could the mechanism take care of systemic issues?
• There is merit to exploring higher level appeals rather than a case-by-case basis
• Supportive of requestors going back to CP on their balancing test – keeping systemic abuse in check is important in any process – do, however, have concerns if a CP says they will say no to every request. Phase 1 requires a balancing test – if they do not do this, the CP is not following the consensus policy.
• There should be a separate lane for systemic issues and the occasional one-off when the requestor would like a second look
• In response to Q8, it’s important to consider how the requestor will communicate with the CP – whether it’s a request for additional information, or how the information is delivered back to the requestor
• This is a pitfall the Team has overlooked – do not think the CP can just casually fire off any sort of disclosure information in an email back to a requestor. Consider whether there is an in-band response where the SSAD relays a response to the requestor in a secure fashion, or if there is an out of band response. Need to figure this out and consider the operational time required to make this happen.
• Initial Report suggests that disclosed data should be sent to requestor in a secure manner. Here, the question is if additional information is needed to make the determination – how should this work?
• When the CGM receives the request and passes it to the CP, it opens a ticket for that. It does makes sense that if the CP needs further information, it goes through the CGM for that information. If that additional information that is relayed to the contracted party contains personal information, the solution for that would be encryption.
• There should be a feedback loop for trackability and evidence that there has been communication – it should go through the central system, and encryption should be employed. Central Gateway would make an RDAP request with a password.
• The Team is getting a bit technical for what we’ve been asked to do here.
• Response to Question 9:
• This calling out of a specific interest is ill-advised.
• This is a common reason for denial of requests, which is why this text was added. This language is verbatim from PPSAI – this is important for IPC.
• The argument for taking this out is that one particular type of request is being singled out.
• This is a limitation on the CP – you are giving a special dispensation to one group. This is a perfectly fine example to deny a disclosure request.
• The word “solely” is meaningful here. Object to taking this clause out.
• The concern raised earlier deals with a malformed request, not a rejection based on IP infringement
• If the SSAD is a shortcut to avoid legal process, then it should say so.
• “nor can approval or refusal”
• Adding approval does not work here. If you want to reject requests just because they relate to content on the website, there is a big problem here. Many CPs may want to automate the request solely based on IP infringement on a website.
• If groups do want automated disclosure if there is alleged intellectual property infringement – refusing is unjust for IP infringement, but approval is also unjust in this instance. If this cannot be accepted, this is disincentivizing other groups from approving the original language.
• The “or approval” may be misconstrued to prevent automation of these cases. If we add a footnote that could help. If approval is solely based on IP allegation, what else would be required? We have spent a year discussing what would be required, like accreditation, lawful basis, etc. That is what makes the additional language extraneous.
• If you have gotten through the gateway, provided proof of your trademark and provided an allegation of infringement – that does not take into account that evidence would have already been provided to support the request. Maybe add [without adequate supporting documentation]
• Add “disposition of the request” instead of “refusal”
• Question 10 response
• Phase 1 recommendation on legal v. natural is about the public system database, it is not about what is disclosed here. The proposed language should remain.
Concern here – if we were talking about only GDPR, this might make sense, but there are other privacy laws out there and there are some jurisdictions that do not provide legal entities with the same protections and rights as natural individuals.

Could add a sentence about unless expressly prohibited by applicable law

There are some human rights implications are not considered applicable law. May data protection laws that have been passed are not enforced.

There may be a case where non-personal information is redacted as a matter of course, and it does need to be requested. What we are seeking here is some certainty that if you know for a fact that there is non-personal data, it will be disclosed.

Is there anyone who cannot live with the text on the screen?

Do not agree with the term “expressly” and do not think “applicable law” protects important interests. Unless expressly prohibited by applicable law is too high a bar.

- We have been told the scope of the PDP is limited to GDPR, but we widened that to include applicable law, and now are widening it further.
- Suggestion to add: Human Rights implications must be taken into account when making a decision on disclosure – perhaps this should go in the balancing test section.
- Maybe there is a way to create a flag on a registration for a human rights organization
- Support Staff to review and incorporate Stephanie’s suggestion, if possible

b. Confirm next steps

- It is imperative for groups to do their homework.

5. Recommendation #7 Authorization Automated & Recommendation #16 Automation

a. Review ‘cannot live with’ items identified (see updated recommendations)

b. Confirm next steps

6. Recommendations not considered by EPDP

a. Review discussion items gleaned from input provided on recommendations not considered by EPDP

b. Confirm next steps

7. Wrap and confirm next EPDP Team meeting (5 minutes):

a. Thursday 15 May at 14.00 UTC. Topic to be addressed: Acceptable Use, Query Policy, Terms of use, Data Retention

b. Confirm action items

c. Confirm questions for ICANN Org, if any