EPDP Team Meeting

21 August 2018   Meeting 6

Agenda

1. Roll Call & SOI Updates

2. Welcome and Updates from EPDP Chair

3. Summary of responses to EPDP Input Survey Part 4
   a. Results for Section 8: Miscellaneous
   b. Results for Appendix C: Data Processing Requirements

4. Substantive Discussion of Temporary Specification (beginning with Section 8, Appendix C)
   a. Part 4 of the Survey can be found at https://www.surveymonkey.com/r/9KD5K79
   b. Section 8: Miscellaneous
   c. Appendix C: Data Processing Requirements

5. Overview of Triage Report, including timeline for review

6. Discussion of Next Steps

7. Review action items and questions for ICANN Org, if any

8. Wrap and confirm next meeting to be scheduled for Thursday 23 August at 13.00 UTC. (Initial comments on Triage Report due Friday, 24 August by 19.00 UTC)

High-level Overview of EPDP Input Survey Part 4 Results

Summary of Responses

	ALAC	BC	ISPCP	RySG	IPC	NCSG	SSAC	RrSG	GAC
Miscellaneous	No	No	No	Yes	Yes	No		No	Yes
Appendix C	Yes	Yes	No	Yes	Yes	NSO		No	No
Appendix C	Yes	No	No	Yes	No	No		No	Yes
Appendix C	Yes	No	No	Yes	No			No	No
Appendix C	Yes	Yes	No	Yes	Yes	Yes		No	Yes
Appendix C	Yes	Yes	No	Yes	Yes	No		No	No
Appendix C	Yes	Yes	No	Yes	Yes	No		No	Yes

Substantive discussion of Temporary Specification

Section 8: Miscellaneous

The following questions and issues were raised with respect to Section 8:

1. As Sections 8.2 and 8.3 are relevant to the Temp Spec only, will this language need to be amended or removed in the next iteration?

2. Regarding Section 8.2, should the next iteration reference GNSO processes for any subsequent modifications (or just removed entirely)?

3. Should the text be modified to reflect the relevant relationships, e.g., Joint Controller, Controller, Processor, and relevant flows of registration data, once the EPDP Team discusses these topics?

4. In reference to the referral of GAC advice in Section 8.2, should the language: (1) be modified to include all relevant GAC advice or (2) require further clarification?

5. In reference to Section 8.1, should the text be amended to reflect
(a) that third party obligations will not be created outside of what is required for minimum GDPR compliance?
(b) the other third party obligations will arise?

Appendix C: Data Processing Requirements - Preamble

The following questions and issues were raised with respect to the preamble of Appendix C:

1. Is this inclusion of language, which is based on but not exactly the same as articles of the GDPR, strictly necessary?

2. Should this language be amended to broadly refer to general data protection principles instead of specific references to the GDPR?

3. Should language be examined using the domain name lifecycle as a reference, i.e., should the EPDP team examine all of the processes at different stages by different parties for collection, updating, publication, access and retention, for both purpose and conformity to the GDPR?

4. Should this language be modified as it currently only references some, but not all, of the bases for processing personal data?

5. Should we replace "...such access will at all times comply with the requirements of the GDPR." with "...such access will comply with the requirements of the GDPR, as applicable"?

6. Should "EBERO" be a party instead of an activity?

7. Within the table, for Public RDDS/WHOIS field, should the language "performance of a contract" be added as a legal justification for Registrar/Registry/ICANN?

Appendix C: Data Processing Requirements – Section 1

The following questions and issues were raised in reference to Appendix C, Section 1:

1. Should the reference to "obligations to applicable laws and regulation" be deleted in deference to providing certainty and the already existing , WHOIS conflicts with local laws policy?

2. Should the language be amended as it may be misleading since Art.6 of the GDPR is not the only legal basis that can be applied to processing?

3. Is this paragraph describing principles useful as it does not describe specific data handling practices, or their monitoring?

4. Should Section 1 be modified to reference data protection principles more broadly, noting that if the GDPR is updated or amended, the language would need to change?

Appendix C: Data Processing Requirements – Section 2

The following questions and issues were raised in reference to Appendix C, Section 2:

1. Does the term "legitimate interest" require further clarity?

2. Does the clause "except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal Data" need further qualification, as not all data disclosures (e.g., to LEA) are subject to this balancing test?

3. Should the EPDP consider submitting the group's agreed-upon legitimate interests (when agreed) as part of an Article 40 Code of Conduct referral to ensure a greater degree of certainty?

4. Should this language be modified since it only references some, but not all, of the bases for processing personal data? Should the singular reference to children be deleted as it is not possible to tell whether a data subject is a child in current registration data?

5. Does this paragraph add value or should it be deleted?

6. Should the identity of the data controller for WHOIS be identified?

Appendix C: Data Processing Requirements – Section 3.1

The following issues and questions were raised in reference to Appendix C, Section 3.1:

1. Are all parties included in this section about informing data subjects about processing, e.g., ICANN, data escrow agents, and emergency backend registry operators?

2. Should the text be modified to reflect the relevant relationships, e.g., Joint Controller, Controller, Processor, and relevant flows of registration data, once the EPDP Team discusses these topics?

3. With respect to Section 3.1.2, do the terms "necessary and appropriate" require further clarity?

4. With respect to Section 3.1.5, how is this testing to be achieved?

5. Should Section 1, et.seq. be modified to reference data protection principles more broadly, to address changes in GDPR or introduction of other privacy regimes?

Appendix C: Data Processing Requirements – Section 3.2 – 3.7

The following issues and questions were raised in reference to Appendix C, Section 3.2 - 3.7:

1. Are all parties included in this section about informing data subjects about processing, e.g., ICANN, data escrow agents, and emergency backend registry operators?

2. Should the text be modified to reflect the relevant relationships, e.g., Joint Controller, Controller, Processor, and relevant flows of registration data, once the EPDP Team discusses these topics?

3. In reference to Section 3.7, does the language require more detail in terms of how privacy-by-design should be implemented?

Appendix C: Data Processing Requirements – Section 3.8 – 3.11

The following issues and questions were raised in reference to Appendix C, Section 3.8 - 3.11:

1. Are all parties included in this section about informing data subjects about processing, e.g., ICANN, data escrow agents, and emergency backend registry operators?

2. Should the text be modified to reflect the relevant relationships, e.g., Joint Controller, Controller, Processor, and relevant flows of registration data, once the EPDP Team discusses these topics?

3. Should the EPDP Team further discuss the requirements for security measures to ensure the measures fit the sensitivity of the data?

4. In reference to Section 3.8, should the term "natural persons" be changed to "data subjects"?

4. Should the specific examples in Sec. 3.8.1-3.8.8 be deleted as: (1) they are not mandatory, and (2) they are overly specific and may become outdated?

5. In reference to Section 3.9, is further detail needed with respect to the roles of ICANN, the registrar, the reseller, and/or other data processors as well as the GDRP-mandated 72 notice in the event of a breach?

6. In reference to Section 3.10, does the term "international organizations" require further clarity?

Other

- BC strongly supports the inclusion of each of the issues identified in 1-7 to be addressed in the EPDP, with the exception of the accreditation model, since that work is being pursued on a separate track. As discussed earlier, providing definition to what is meant by "continued [and]public access" falls squarely within this PDP and must be explored

- RySG: These issues are not being considered in the Triage exercise. Please note specifically the Objectives & Goals of the GNSO scope document for the EPDP note that these matters are not for initial consideration and the focus of the EPDP team should remain on the Primary queries at this juncture.

- IPC: Apart from the issue identified in point #1 of the annex (related to an accreditation model) which IPC supports continued discussion of the important issues enumerated in the Annex by the EPDP team. We understand that the issued address in #1 is subject to the gating questions defined in the charter.

Overview of Triage Report

- Updated triage report has been shared with the EPDP Team

- Triage Report, per the Charter, is EPDP Team's first deliverable

- The report represents the results from the triage surveys, Part 1 - 4

- Report includes:
  - an executive summary
  - operating methodology
  - the summary table of inputs
  - the issue summaries that were created for each section
  - an appendix with all written comments

- The report does not represent any group's final opinion on any issue - all groups should feel free to revise their input during the course of the EPDP Team's work

- Please review the draft triage report and provide any initial feedback by Friday, 24 August at 19:00UTC.

Wrap Up

- Mid-course corrections to today's meeting

- Now that all surveys are completed, EPDP Leadership will provide a proposed project plan and order of review to the EPDP Team today - to be discussed at next meeting.

- Review actions items and questions for ICANN Org, if any

- Next meeting to be scheduled for Thursday 23 August at 13.00 UTC

Note: Initial Feedback on the Triage Report due by Friday 24 August by 19.00 UTC