EPDP Team Meeting

30 August 2018 Meeting #9

Agenda

1. Roll Call & SOI Updates

2. Welcome and Updates from EPDP Team Chair

3. Review proposed next steps and action items on Section 4.4 - Lawfulness and Purposes of Processing gTLD Registration Data.

   Develop specific recommendation for amendments to the temporary specification for:
   a) Registrar / Registry / ICANN processing of data: clarifying the elements proposed in the ICANN-developed specification
   b) Third party processing where more specificity was requested

4. Begin discussion on Appendix C – Data Processing Requirements
   a) Preamble
   b) gTLD Processor Activity Chart
   c) Section 1 (Principles for Processing)
      Section 2 (Lawfulness of Processing)
   d) Sections 3.1, 3.1.1 – 3.1.6 (Specific Controller Processing requirements)
   e) Sections 3.2 – 3.11 (Specific Controller Processing requirements)

5. Confirm action items and questions for ICANN Org, if any

6. Wrap and confirm next meeting to be scheduled for Tuesday 4 September at 13.00 UTC.

Review proposed next steps and action items on Section 4.4 - Lawfulness and Purposes of Processing gTLD Registration Data

Agenda item #3

§4.4 – Purposes of Processing gTLD Registration Data

Three topics:

- Addressing concern about the italicized text in: “Personal Data included in Registration Data may be Processed … *only for the following legitimate purposes,”* and other wording issues
- Data processing purposes: Registrar-Registry contracts and support of registrants.
- Data processing purposes: Third-party access and uses of data

Wording issues

The concern that “Personal Data included in Registration Data may be Processed … *only for the following legitimate purposes,”* could be seen as limiting as GDPR interpretation and other privacy regimes evolve.

To address this §4.4 could be reworded from:

4.4.Personal Data included in Registration Data may be Processed … and *only for the following legitimate purposes: …*

> 4.4.2 Providing access to accurate, reliable, and uniform Registration Data based on legitimate interests not outweighed by the fundamental rights of relevant data subjects, consistent with GDPR;

to

4.4.Personal Data included in Registration Data may be Processed … *and for legitimate interests not outweighed by the fundamental rights of relevant data subjects, consistent with GDPR;:*

> ~~*4.4.2 Providing access to accurate, reliable, and uniform Registration Data based on legitimate interests not outweighed by the fundamental rights of relevant data subjects, consistent with GDPR;*~~

Data Processing: Registrar-Registry-ICANN Contract Purposes

4.4.1. – Ability for Registered Name Holder to exercise its rights
4.4.3. – Enabling mechanism for identifying and contacting registered name holder
4.4.4. – Payment and invoicing
4.4.5. – Notification of technical issues
4.4.6. - Notification of commercial or technical changes
4.4.7. – Technical & administrative points of contact
4.4.11. – Safeguarding in case of failure
4.4.12. – Dispute resolution services
4.4.13. – ICANN Contractual Compliance

Based on comments made during the Triage session, it was apparent that the RrSG sought rewording of many of these elements, where the result would capture many of the same data elements but in a way that matched the data flow of domain registrations and domain-name life cycle.

The data processing requirements (App C) and the data elements collected and displayed (App A) will both consider the domain-name life cycle states.

Data Processing: Third-Party Purposes

4.4.2. – Providing access based on legitimate interests not outweighed by the fundamental rights

4.4.8. – Supporting a framework to address consumer protection, investigation of cybercrime, DNS abuse, IP protection

4.4.9. – Framework to address LE needs

4.4.10. – Provision of zone files to Internet users

For these third-party purposes, personal data processed in the context of Whois can be made available to third parties who have a legitimate interest in having access to the data, provided that appropriate safeguards are in place to ensure that the disclosure is proportionate and limited to that which is necessary and the other requirements of the GDPR are met, including the provision of clear information to data subjects.

It is not anticipated that this group can do that balancing, i.e., whether these purposes have a corresponding legal basis

The EPDP Team was asked to provide greater clarity for §4.4.8, i.e., describe how data would be used to address the enumerated purposes in that section so that the data provided met the need and is appropriately limited.

Note that any discussion on the safeguards and limitations in relation to access necessary to ensure GDPR compliant disclosures would happen after the gating questions have been answered.

Review of Appendix C – Data Processing Requirements

Agenda item #5

APPENDIX C

(DATA PROCESSING REQUIREMENTS)

question for the group:

WHAT ROLE DOES THE APPENDIX PLAY IN THE POLICY WE ARE DEVELOPING?

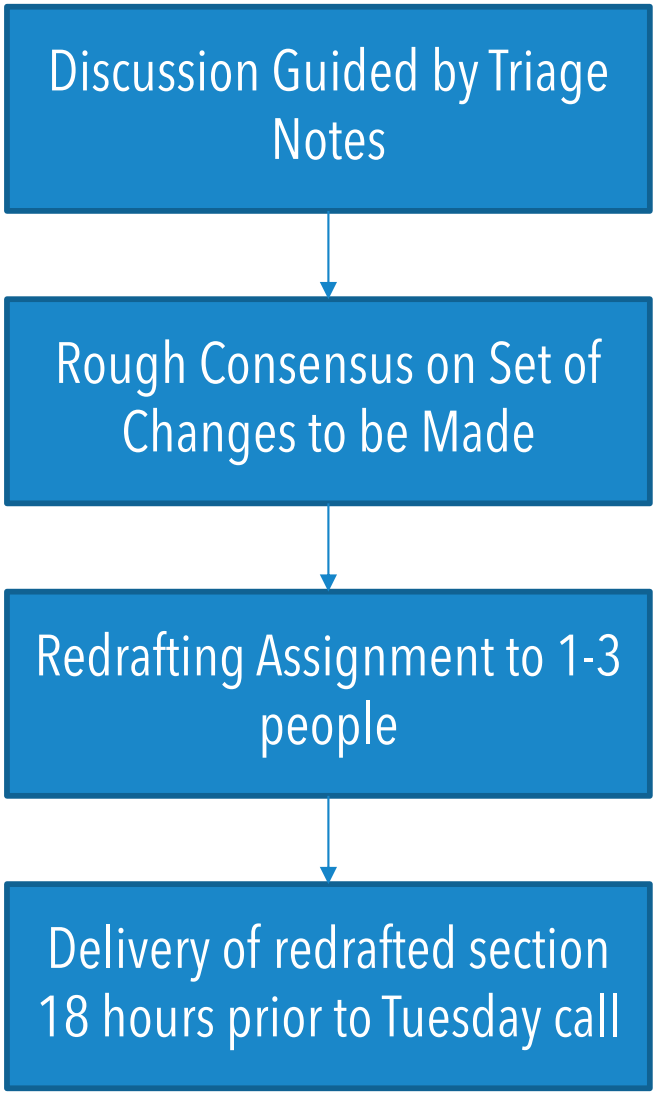
(THROUGH THE WORK OF THIS EPDP TEAM)

APPROACH TO MODIFICATION OF APPENDIX C: DATA PROCESSING REQUIREMENTS

for each of these sections….

- Preamble
- Chart
- Principles for & Lawfulness of Processing
- Specific Controller Processing Requirements

follow this process:



Appendix C: Preamble

The following questions and issues were raised with respect to the preamble of Appendix C. Please also refer to the DSI here: https://go.icann.org/2wpsqdQ

1. This language is based on but not exactly the same as GDPR article.
    a) What purpose does it serve vis-à-vis the purpose of the Temporary Specification?
    b) Should it be amended to match the GDPR, simply refer to the pertinent GDPR section, or be deleted?
2. Recommended amendments to the existing language:
    a) Should this language be amended to broadly refer to general data protection principles instead of specific references to the GDPR? What would such language look like?
    b) Should we replace "... where Personal Data may be accessed, such access will at all times comply with the requirements of the GDPR." with "...where Personal Data may be accessed, such access will comply with the requirements of the GDPR, as applicable"?

gTLD Processing Activity Chart

1. Should this language be modified as it currently only references some, but not all, of the bases for processing personal data? I.e., is the role of this chart as an exemplar or a checklist?

2. 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?

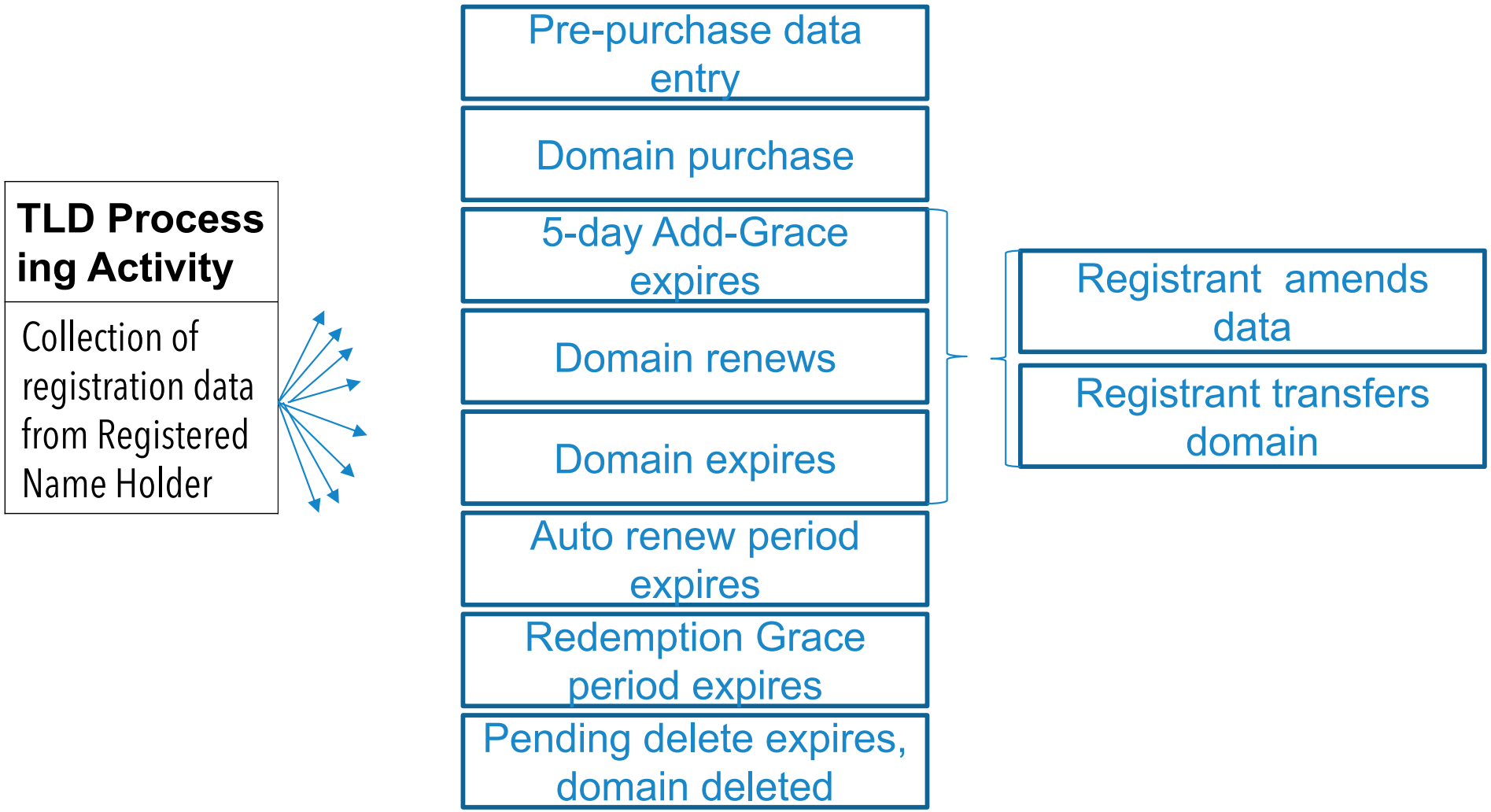
3. Specific amendments:

   a) Should "EBERO" be a party instead of an activity?

   b) 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?

Transfer of registration data to Emergency Back-end Registry Operator (EBERO)	No role	Processor (Performance of a Contract)	Controller (Legitimate Interest)
Public RDDS/WHOIS	Controller (Legitimate Interest)	Controller (Legitimate Interest)	Controller (Legitimate Interest)

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?



gTLD Processing Activity Chart

Appendix C, 1-2: Principles & Lawfulness

The following questions and issues were raised in **Principles for Processing**:

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 Section 1 be modified to reference data protection principles more broadly:
   a) To include principles from GDPR sections other that Ar6.6
   b) To accommodate future change in GDPR
   c) to reference data protection principles more broadly

The following questions and issues were raised in **Lawfulness of Processing**:

1. Should there be an LEA carve-out to 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?
2. Should we submit this group's agreed-upon legitimate interests / Purposes as part of an Article 40 Code of Conduct referral?
3. Should this language be modified since it only references some, but not all, of the bases for processing personal data?
4. 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?

Appendix C: 3.1-11 Specific Controller Processing Req’ts

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.seg. be modified to reference data protection principles more broadly, to address changes in GDPR or introduction of other privacy regimes? \

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

Appendix C: 3.8-11 Specific Controller Processing Req’ts

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

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

3. 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?

4. 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?

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

Wrap Up

Agenda item #6 & #7

Wrap Up

Review actions items and questions for ICANN Org, if any

Next meeting to be scheduled for Tuesday 4 September at 13.00 UTC