EPDP Team Meeting

6 September 2018

Meeting #11

Agenda

1. Roll Call & SOI Updates

2. Welcome and Updates from EPDP Team Chair
   - Update on status of GDPR training
   - Update on travel to ICANN63
   - Other updates, if applicable

3. Proposed modifications to section 4.4 - Registrar / Registry / ICANN processing of data
   - Review proposed modifications put forward by the Registrar Team
   - Consider input from EPDP Team members on proposed modifications
   - Agree on next steps

4. Proposed modifications to section 4.4 – introductory paragraph
   - Review proposed modification put forward by Alex Deacon and Thomas Rickert
   - Consider input from EPDP Team members on proposed modifications
   - Agree on next steps

Agenda

5. Status update on modifications to section 4 – Third-Party Legitimate Interests
    - revised language for §4.4.2 (Amr Elsadr)
    - revised language for §4.4.8 (Alex Deacon & Amr Elsadr)
    - revised language for §4.4.9 (Ashley Heineman)

6. Review data matrix formed from RDS work and Thomas's chart
    - High-level overview of chart
    - Discuss proposed amendments to Chart
    - Agree on next steps

7. Introduction to Appendix A

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

9. Wrap and confirm next meeting to be scheduled for Thursday 6 September at 13.00 UTC.)

EPDP Barcelona – Travel Funder of Last Resort

Deferring to all other travel funding methods, travel fund applicants:

- must be a recognized member of the EPDP Team;
- must be able to demonstrate their active participation in the proceedings of the EPDP Team (e.g., minimum attendance of 75% of all scheduled meetings)
- should not be eligible for other community travel support
    - candidates to identify and explain other potential sources of funding they are have considered or for which they might apply
    - partial funding available to those receiving partial funding from another source;
- should disclose recent past funding options and explain why those options are no longer available, if applicable; and,
- must demonstrate that their attendance is critical to the success of the EPDP Team meeting or an aspect of the meeting that cannot be achieved by participating remotely
- must demonstrate that no alternates are expected to attend & able to replace the member

Additionally, companies / organizations that customarily fund travel of a person that is now an EPDP member are expected to continue that practice absent some change that would require funding.

GDPR Training

1) Online, self-paced module via IT Governance
    1) Can be done at participant convenience
    2) Immediately (more or less) available
2) Follow on sessions for a deeper dive, specific questions on select topics
    1) Becky Burr
    2) Soliciting others

Topic	Entry Date (E) _____ Target Date (T)	Action Item	Responsible EPDP Team Member
Triage Report	4 September 2018 _____ 6 September 2018	EPDP Team to review the latest version of the triage report as circulated by Kurt to the mailing list and provide input before Thursday 6 September with the goal to send the report the following day.	
Purposes for Processing Data: §4.4, (introductory paragraph), Appendix A.4. and Appendix C2 - correction to add other GDPR “legitimate purposes	4 September 2018 _____ 6 September 2018	Redrafting §4.4 (introductory paragraph), Appendix A.4. and Appendix C2.	Alex Deacon Thomas Rickert
Purposes for Processing Data: §4.4 relocating § §4.4.2, 4.4.8, 4.4.9	4 September 2018 _____ 6 September 2018	EPDP Team to provide comments on Kurt’s email with proposals for relocating § §4.4.2, 4.4.8, 4.4.9 to a different section of the Temporary Specification.	
Data Processing Requirements: Appendix C	4 September 2018 _____ 6 September 2018	Provide an illustrative joint controller agreement so that the team can differentiate between the operational elements and the policy-related elements.	Thomas Rickert
Data Processing Requirements: Appendix C	4 September 2018 _____ 6 September 2018	Review appendix C and indicate what aspects may need a specific mention in the policy recommendations regarding disclosure of data to third parties	Margie Milam

Topic	Entry Date (E) _____ Target Date (T)	Action Item	Responsible EPDP Team Member
Purposes for Processing Data: §4.4, 4.4.1-4.4.13	31 August 2018 _____ 4 September 2018	Registrars to rewrite section 4.4 to align the purposes for data processing with current data collection processes and the domain name lifecycle. It is requested that the draft be completed in time for the meeting on Tuesday, 4 Sept so that the rest of the team can review it.	James Bladel Matt Serlin Emily Taylor
Purposes for Processing Data: §4.4.2	31 August 2018 _____ 5 September 2018, 22:00UTC	Propose revised language for §4.4.2.	Amr Elsadr
Purposes for Processing Data: §4.4.8	31 August 2018 _____ 5 September 2018, 22:00UTC	Propose revised language for §4.4.8.	Alex Deacon Amr Elsadr
Purposes for Processing Data: §4.4.9	31 August 2018 _____ 5 September 2018, 22:00UTC	Propose revised language for §4.4.9.	Ashley Heineman

Proposed modifications to § § 4.4.1; 4.4.3-4.4.7; 4.4.11-4.4.13

Registrar / Registry / ICANN processing of data

- Proposed revisions due by Wednesday 5 September at 22.00 UTC

Discussion

a) Registrars to present approach to further edits (today)

b) Brief discussion (today)

c) Email discussion and close out (Tuesday, 11 September)

Proposed Temporary Specification §4.4

4.4 However, such Processing must be in a manner that complies with applicable data protection laws, including on the basis of a specific identified purpose for such Processing. Accordingly, Personal Data included in Registration Data may be Processed on the basis for the purpose of domain name registrations in compliance with applicable data protection laws, and only for the following legitimate purposes:

4.4.1 Reflecting the rights of a Registered Name Holder in a Registered Name and ensuring that the Registered Name Holder may exercise its rights in respect of the Registered Name;

4.4.2 Enabling a reliable mechanism for contacting the Registered Name Holder for a variety of legitimate purposes more fully set out below;

4.4.3 Enabling a mechanism for the communication or notification to the Registered Name Holder of technical issues with a Registered Name;

4.4.4 Supporting a framework to address issues involving domain name registrations, including but not limited to: law enforcement investigation, DNS abuse, and tailored mechanisms designed to protect intellectual property interests (as provide for by Section 4.4)

4.4.5 Coordinating dispute resolution services for URS and UDRP, and;

4.4.6 Handling contractual compliance monitoring requests (which include provisions for contracted parties to invoke non-binding arbitration and other procedures to address conflicts with law), audits, and complaints submitted by Registry Operators, Registrars, Registered Name Holders, and other Internet users

Proposed modifications to section 4.4 – introductory paragraph

Discussion

a) Alex Deacon and Thomas Rickert to present approach to further edits (today)

b) Brief discussion (today)

c) Email discussion and close out (Tuesday, 11 September)

Insert Proposed Edits (when available)

Status update on modifications to § § 4.4.2, 4.4.8 & 4.4.9

Third-Party Legitimate Interests

Discussion

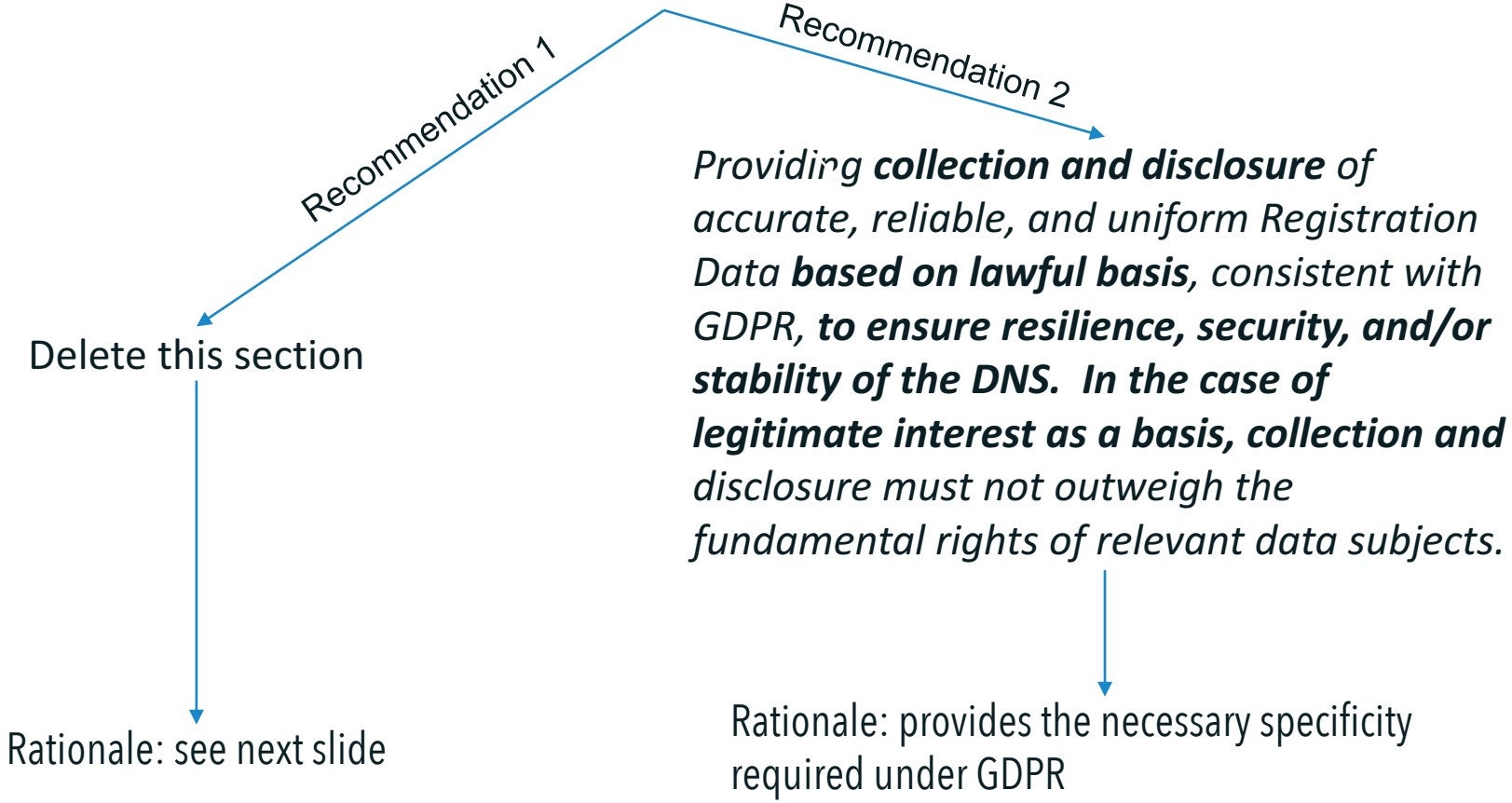
a) Amr Elsadr, Ashley Heimeman, Alex Deacon to present approach to further edits (today)
   - revised language for §4.4.2 (Amr Elsadr)
   - revised language for §4.4.8 (Alex Deacon & Amr Elsadr)
   - revised language for §4.4.9 (Ashley Heineman)

b) Brief discussion (today)

c) Email discussion and close out (Tuesday, 11 September)

§4.4.2 – recommended changes

§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*



Proposal 1: delete §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*

Rationale: Many group members' statements that §§ 4.4.2, 4.4.8, 4.4.9 and 4.4.10 are better placed under a different heading than *"Lawfulness and Purposes of Processing gTLD Registration Data,"* as these sections are not really purposes. With that in mind:

Feedback submitted in response to the survey and subsequent discussions supported a view that §4.4.2 is vague, broad, and insufficiently specific to serve as a purpose for lawful processing of gTLD Registration Data.

If 4.4.2 does not actually serve to clarify a lawful purpose for processing gTLD Registration Data, what purpose it does serve? §4.4.2:

- creates an obligation to provide access to gTLD Registration Data
- describes conditions that need to be fulfilled before access to gTLD Registration Data may be provided; that they be *"based on legitimate interests not outweighed by the fundamental rights of relevant data subjects, consistent with GDPR"*
- describes obligatory characteristics of the gTLD Registration Data to which access shall be provided; that the data will be *"accurate, reliable, and uniform"*

Given that, §4.4.2 appears to serve as a guiding principle under which access may be provided to certain third-parties, which will need to be deliberated upon. However, these principles describe already existing requirements, in the section 4 heading.

Finally, it seems to me that the characteristics of gTLD Registration Data being being accurate, reliable and uniform are already detailed requirements in the 2013 RAA's WHOIS Accuracy Program Specification, and the Consensus Policy of "thick" WHOIS under consistent labelling and display.

Conclusion: §4.4.2 is unhelpful, vaguely drafted, and redundant

§4.4.9 – recommended changes

Providing a framework to address appropriate law enforcement needs;

original

new

Enabling the prevention and detection of cybercrime and illegal DNS abuse to promote the resilience, security, stability and/or reliability of the DNS and the Internet. Enabling the prevention of unlawful conduct to meet the legitimate needs of law enforcement and public authorities promoting consumer trust in the DNS and the Internet and safeguarding registrant data.

Location of 4.4.9 in the Temporary Specification

Proposed: This text should remain under section 4.4 (i.e., not be moved) as this section is a list of ICANN's and the Contracted Parties' legitimate purposes for processing data. This reference to this purpose influences / touches upon at least two stages of their processing (i.e., collection and disclosure).

To be clear, we are *not seeking the collection of additional WHOIS data elements*. However, we do want to ensure that the collection of existing WHOIS data fields continue to be maintained.

The collection and disclosure of information, as it aligns with efforts to combat cybercrime and other illegal DNS abuse, is fully consistent with ICANN bylaws and therefore fits within ICANN's purposes. (see below).

Lastly, our initial text reflects a concerted effort to not conflate ICANN's purposes with that of LEA/government authorities. It is our view that the interests and lawful basis of third parties (such as LEA/government authorities) should be articulated elsewhere as appropriate.

ICANN Bylaws (excerpts):

Section 1.2. COMMITMENTS AND CORE VALUES

(a)(i) Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet.

Section 4.6. SPECIFIC REVIEWS - (e) Registration Directory Service Review…

(ii) The Board shall cause a periodic review to assess the effectiveness of the then current gTLD registry directory service and whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust and safeguarding registrant data.

Data Elements

Matrix mashup: Thomas Rickert's and RDS work

Objective

- Charter Questions associated with data collection, what data:
  - registrars be required to collect for each of the following contacts: Registrant, Tech, Admin, Billing?”
  - is collected because it is necessary to deliver the service of fulfilling a domain registration, versus other legitimate purpose"

Then update the matrix by considering Charter Question sets regarding:

- Transfer of data from registry to registrar (charter question c)
- Transfer of data from registrar/registry to data escrow provider (charter question d)
- Transfer of data from registrar/registry to ICANN (charter question e)
- Publication of data by registrar/registry (charter question f)

All data elements currently required (just for comparison)	Data elements the Registrar must collect to perform the contract (6 I b GDPR - "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract")	6 I f: "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."
	Registry-Registrar-ICANN Contract Purposes (Currently: 4.4.1, 4.4.3, 4.4.4, 4.4.5, 4.4.6, 4.4.7, 4.4.11, 4.4.12)	Third Party Legitimate Interests (Currently: 4.4.2, 4.4.8, 4.4.9, 4.4.10)
Domain Name	Domain Name	Domain Name
Registry Domain ID		
Registrar Whois Server	Registrar Whois Server	Registrar Whois Server
Registrar URL	Registrar URL	
Updated Date	Updated Date	Updated Date
Creation Date	Creation Date	Creation Date
Registry Expiry Date	Registry Expiry Date	
Registrar Registration Expiration Date	Registrar Registration Expiration Date	Registrar Registration Expiration Date
Registrar	Registrar	Registrar
Registrar IANA ID	Registrar IANA ID	
Registrar Abuse Contact Email	Registrar Abuse Contact Email, must be role contact	Registrar Abuse Contact Email
Registrar Abuse Contact Phone	Registrar Abuse Contact Phone, must be role contact	Registrar Abuse Contact Phone
Reseller	Reseller	
Domain Status	Domain Status	Domain Status
Registry Registrant ID		
Registrant Fields • Name • Organization (opt.) • Street • City • State/province • Postal code • Country • Phone • Phone ext (opt.) • Fax (opt.) • Fax ext (opt.) • Email	Registrant Fields • Name • Organization (opt.) • Street • City • State/province • Postal code • Country • Phone • Phone ext (opt.) • Fax (opt.) • Fax ext (opt.) • Email	Registrant Fields • Name • Organization (opt.) • Street • City • State/province • Postal code • Country • Phone • Phone ext (opt.) • Fax (opt.) • Fax ext (opt.) • Email
2nd E-Mail address		
Admin ID		
Admin Fields • Name • Organization (opt.) • Street • City • State/province • Postal code		Admin Fields • Name • Organization (opt.) • Street • City • State/province • Postal code

Introduction to Appendix A

Agenda Item #8

Appendix A - Registration Data Directory Services

1. Registration Data Directory Services

2. Requirements for Processing Personal Data in Public RDDS Where Processing is Subject to the GDPR

3. Additional Provisions Concerning Processing Personal Data in Public RDDS Where Processing is not Subject to the GDPR

4. Access to Non-Public Registration Data

5. Publication of Additional Data Fields

Registration Data Directory Services (§1)

- All parties agree that RDAP will be implemented. Should the date for SLA definition (31 July 2018) be deleted or amended since it has passed? Will any date be germane in the successor document?
- There is some uncertainty as to whether a search capability is / should be a contractual requirement. Is the Search Capability paragraph (which places GDPR-required restrictions on the use of search) necessary?
- Do the restrictions in this section address the risks associated with the aggregation of data?

Requirements for Processing Personal Data (§2.1 – 2.3)

EDBP advice (legal persons):

- *The GDPR does not apply to the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person. While the contact details of a legal person are outside the scope of the GDPR, the contact details concerning natural persons are within the scope of the GDPR, as well as any other information relating to an identified or identifiable natural person.*

- *The mere fact that a registrant is a legal person does not necessarily justify unlimited publication of personal data relating to natural persons who work for or represent that organization, such as natural persons who manage administrative or technical issues on behalf of the registrant.*

- *For example, the publication of the personal email address of a technical contact person consisting of firstname.lastname@company.com can reveal information regarding their current employer as well as their role within the organization. Together with the address of the registrant, it may also reveal information about his or her place of work.*

- *In light of these considerations, the EDPB considers that personal data identifying individual employees (or third parties) acting on behalf of the registrant should not be made publically available by default in the context of WHOIS. If the registrant provides (or the registrar ensures) generic contact email information (e.g. admin@domain.com), the EDPB does not consider that the publication of such data in the context of WHOIS would be unlawful as such.*

Req’ts for Processing Personal Data (§§2.1–2.3, §3)

- Is §2.1 (when coupled with §3) is overly broad in that:
  - GDPR data restrictions can be applied globally and include entities (registrars, registries, registrant) located outside the EEA, and
  - data restrictions need not be applied to Legal persons where personal data is not included in the record? (Can legal/natural distinctions be made a priori? Is attempting to distinguish these differences implementable?)

- § 2.3**:** Should data in addition to what is specified in the Temporary Specification as personal data be redacted (e.g., organization name, city, postal code) or taken off the redacted list (e.g., email address)?

- The Temporary Specification mentions "consent" without a requirement or specification for such. Should this group take that up?

Requirements for Processing Personal Data (§2.4)

EDBP advice (admin / technical contact)

The EDPB considers that registrants should in principle not be required to provide personal data directly identifying individual employees (or third parties) fulfilling the administrative or technical functions on behalf of the registrant. Instead, registrants should be provided with the option of providing contact details for persons other than themselves if they wish to delegate these functions and facilitate direct communication with the persons concerned. It should therefore be made clear, as part of the registration process, that the registrant is free to:

(1) designate the same person as the registrant (or its representative) as the administrative or technical contact; or

(2) provide contact information which does not directly identify the administrative or technical contact person concerned (e.g., admin@company.com).

Access to Non-Public Registration Data (§4)

EDPB Advice (logging):

- *Appropriate logging mechanisms should be in place to log any access to non-public personal data.*
- *Demonstrable compliance with such logging is the security obligation of controllers*
- *Active communication (pushing) of log information to the registrant or third parties is not required. ICANN and other controllers must ensure that logging information is not disclosed to unauthorized entities, in particular with a view of not jeopardizing legitimate law enforcement activities.*
- *Data subject rights, including the right of access, must however be accommodated unless one of the exceptions under the GDPR applies or if national legislation provides for a restriction in accordance with the GDPR (article 23).*

Should these logging requirements be included in the Policy?

Access to Non-Public Registration Data (§4)

§4.1: See Alex Deacon's recommendation above; should this section be modified as not all disclosure of data will take place on the basis of Art. 6(1)(f) of the GDPR?

§4.2:

- What is meant by "reasonable" access? Should "reasonable" be deleted?
- There is concern that individual decisions or rulings will be construed as rules of law and be implemented haphazardly by registrars. Instead, should case law be interpreted and the appendices tho this Policy be updated via some mechanism?

Publication of Additional Data Fields (§5)

- Should there should be some measure of standardization of the output for additional data fields?
- Given Alan Woods' recommendation for removing Appendix C, should reference to it here be deleted?

Next Steps

- Each group to formulate positions on these questions or other issues.
- Depending on the importance of the issue (remember our categorization of issues) we will take these up in a meeting or in an online forum)
- Timing depends on progress of previous issues and will be discussed at the end of the meeting.

Wrap Up

Agenda item #9 & #10

Wrap Up

Review actions items and questions for ICANN Org, if any

Next meeting to be scheduled for Tuesday 11 September at 13.00 UTC