EPDP Phase 2 Legal Questions, Batch 2

Legal vs. Natural (and Accuracy)

1. As a follow-up to the previously provided memos on Accuracy and Legal vs. Natural persons, the EPDP team requests the following clarification on the scope of the GDPR accuracy principle under Article 5.1(d). As a reminder, one proposal to address the issue of treating all registration data as containing personal data is to allow registrants to self-identify as legal persons at the time of registration. Contracted parties would rely on this self-identification (which could be inaccurate) when deciding whether to redact the registration data.

Question 1:

Whose rights and interests are intended to be served by the Accuracy Principle? We understand that the Accuracy Principle is intended to protect the Data Subject (here, a registrant or registrant contact) from harm resulting from the processing of inaccurate information. Likewise, we understand that the Accuracy Principle may be intended to serve the interests of [a] controller (e.g., ICANN's or the contracted parties' interest in maintaining the security and stability of the Internet's unique identifiers). Is the principle also intended to serve the interests of third-parties (in this case law enforcement, IP rights holders, and others who would request the data from the controller for their own purposes)?

In responding to this question, can you please clarify the parties/interests that we should consider in general, and specifically when interpreting the following passages from the prior memos:

- Both memos reference "relevant parties" in several sections. Are the "relevant parties" limited to the controller(s) or should we account for third-party interests as well?
    - "There may be questions as to whether it is sufficient for the RNH or Account Holder to confirm the accuracy of information relating to technical and administrative contacts, instead of asking information of such contacts directly. GDPR does not necessarily require that, in cases where the personal data must be validated, that it be validated by the data subject herself. ICANN and the **relevant parties** may rely on third-parties to confirm the accuracy of personal data if it is reasonable to do so. Therefore, we see no immediate reason to find that the current procedures are insufficient." (emphasis added) (Paragraph 19 – Accuracy)
    - "In sum, because compliance with the Accuracy Principle is based on a reasonableness standard, ICANN and the **relevant parties** will be better placed to evaluate whether these procedures are sufficient. From our vantage point, as the procedures do require affirmative steps that will help confirm accuracy,

unless there is reason to believe these are insufficient, we see no clear requirement to review them." (emphasis added) (Paragraph 21 - Accuracy)

  - "If the **relevant parties** had no reason to doubt the reliability of a registrant's self-identification, then they likely would be able to rely on the self-identification alone, without independent confirmation. However, we understand that the parties are concerned that some registrants will not understand the question and will wrongly self-identify. Therefore, there would be a risk of liability if the **relevant parties** did not take further steps to ensure the accuracy of the registrant's designation." (emphasis added) (Paragraph 17 – Legal v. Natural)

- Similarly, the Legal vs. Natural person memo refers to the "importance" of the data in determining the level of effort required to ensure accuracy. Is the assessment of the "importance" of the data limited to considering the importance to the data subject and the controller(s), or does it include the importance of the data to third-parties as well (in this case law enforcement, IP rights holders, and others who would request the data from the controller for their own purposes)?

  - "As explained in the ICO guidance, "The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you are using the data to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy." (Paragraph 14 – Legal vs. Natural)

Territorial Scope

1. The Legal Committee seeks guidance as to whether the Right to Be Forgotten Case regarding the reach of GDPR, and the recent guidelines published by the EDPB on Geographic Scope [edpb.europa.eu], affect The advice given in Phase 1 Regarding Territorial Scope, in Sections 6.2- 6.9?

a.

2. In light of this ECJ decision and the Geographic Scope Guidelines, would there be less risk to EEA-based contracted parties (or non EEA-based contractual parties with respect to processing subject to GDPR) if an SSAD operated by ICANN and based in ICANN's Los Angeles Headquarters provided recommendations to contracted parties to disclose redacted data of registrants located outside of the EU where such data may or may not be processed by entities ~~processors or additional controllers~~ inside the EU or otherwise subject to the GDPR, for legitimate purposes (such as cybersecurity investigations and mitigation) and/or other fundamental rights such as intellectual property infringement investigations (See EU Charter of Fundamental Rights Article 17, Section 2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

WHOIS ACCURACY

Following the review of your previous memo on WHOIS Accuracy, the EPDP Legal Committee requests clarification on the following issues:

1.

The memo provides, in ¶15, that GDPR's Accuracy Principle "requires controllers to take 'reasonable steps' to ensure that personal data is accurate and up to date." The memo also cites the United Kingdom Information Commissioner Office's guidance:

> The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you are using the data to make decisions that may significantly affect the individual concerned ***or others***, you need to put more effort into ensuring accuracy. [emphasis added]. Memo at ¶7.

Finally, the memo provides:

a. controllers collect registration data in part to ensure the security, stability and resiliency of the Domain Name System in accordance with ICANN's mission through the enabling of lawful access for legitimate third-party interests [ICANN Purpose, Final Report EPDP at p. 21] and
b. the current Registrar Accreditation Agreement (RAA) requires registrars to take certain steps to ensure the accuracy of data provided by registered domain name holder (registrants)

In light of these conclusions and observations, in addition to the requirements set forth in the current Registrar Accreditation Agreement:

2. What additional reasonable steps should ~~data controllers~~ [ICANN and/or contracted parties] take to ensure the accuracy of the data submitted with regard to the purposes for which they are processed?
3. What additional reasonable steps should ~~data controllers~~ [ICANN and/or contracted parties] take to ensure the overall appropriate levels of data accuracy? In particular, would it be advisable for ICANN and/or contracted parties ~~data controllers~~ to implement the methods identified[1] in Bird and Bird's January 25, 2019 memo on liability related to a registrant's self-identification as a natural or non-natural person in order to ensure the overall appropriate levels of data accuracy?

4. If statistics indicate that overall levels of data accuracy fall below a reasonable threshold (to be determined), would that demonstrate that the data controller's methods to ensure data accuracy are not reasonable?

[1] a) Confirmation emails seeking certification of the accuracy of the data submitted, b) Independent verification, c) Communicating consequences of submitting inaccurate data (under RAA, can suspend or cancel registration under certain circumstance).