**EPDP Phase 2 Legal Questions, Batch 2**

**Priority 1 - SSAD Questions**

1. In order to inform our group’s discussion on whether reverse lookups by any accredited party be allowed and be part of our policy recommendations, we would like to understand better whether reverse lookups can be compliant with GDPR in the following scenarios.

In our current deliberations it was agreed that, disclosure requests relate to non-public registration data for a given domain name: a query is made for one domain name and – if disclosure is permissible – non-public registration data is returned for this very domain name.

Reverse lookups are different in that a query is made for any data element that is not publicly available in the registration data, but may be present as part of the non-public registration data. This may include e-mail addresses, a registered name holder name or a phone number. If reverse lookups were allowed, the SSAD could then potentially return numerous domain names associated with the given data element and resulting in the disclosure of non-public registration data for multiple domain names as well as other personal information contained in the domain names themselves or the use thereof. For example, a reverse query for a domain name holder may not only return his business domain names but also those used for private purposes. Further, a query for a more generic string sch as “John Smith” as registered name holder name may return results for multiple registered name holders.

Reverse lookups can be helpful to investigate patterns of abusive or criminal behavior.

Our group recognizes that reverse lookups can be more impactful for data subjects. Hence, we are seeking your advice on a staggered approach to limit disclosure to what is necessary for the requestor to conduct their work while limiting the impact on the data subjects involved.

Scenario 1:

1. The accredited requestor must:
a. provide evidence that multiple (alternative suggestion: at least one) domain name(s) are involved in illegal / abusive conduct
b. identify at least one domain name for which it believes is involved in the illegal /abusive conduct and
c. cite an appropriate legal basis under GDPR to support its request, as well as all other information required for submitting “ordinary requests” to the SSAD.

For example, victims of online fraud often share their experiences in online fora. Credible information published by multiple users in a trusted forum suggesting that a data element is linked to multiple domain names could suffice as a basis for triggering a reverse lookup. These requirements (a-c) are intended to prevent the reverse lookups from being misused as mere “fishing expeditions” or based on guesses. The SSAD will initially only produce the number of domain names associated with the given data elements by TLD and by registrar. No further information will be returned. This shall help the requestor to determine whether there is smoke or there is fire.

2. If the requestor wishes to proceed, a manual review / balancing of rights is required to determine whether investigating the alleged abusive behavior or criminal activity allows the disclosure of information on multiple domain names and whether proceeding to the next steps already unjustifiably impacts the rights of the data subjects involved. This may be the case where multiple domain names are used (for example) to publicize political speech and where the requestor might try to suppress such free speech or help convict those exercising free speech Or in other cases where the impact on the data subject outbalances the legitimate interests of the requestor.

If the manual review and balancing test is affirmative, only a list of domain names is returned, not the non-public registration data for all listed domain names.
The requestor may then proceed to file disclosure requests for individual domain names and these will be dealt with according to “ordinary” disclosure requests for individual domain names.\*\*

Scenario 2:

Dispute Resolution Providers appointed by ICANN, e.g. for UDRP cases, should be able to request disclosure of domain names registered by a given registered domain holder including non-public registration data for multiple domain names where the dispute resolution policy allows for multiple domain names to be included in one complaint, and where the multiple infringing domain names are to be submitted as evidence by the complainant to support a finding by the panelist of bad faith by the registrant.

Alternate proposal: Allow for DRPs to make requests to check whether the data of any given domain name matches an already obtained data set. No data would be disclosed, only the fact whether the data set matches that used in the query.

\*\*The EPDP Team kindly asks to advise if the proposed approach is unnecessarily conservative. One aspect e.g. the legal committee has discussed is whether evidence of two domain names involved in abusive behavior shall be required or whether one domain name shall be sufficient.

**Priority 2 Questions**

**Privacy/Proxy and Pseudonymized Emails**

1. The group has discussed the option of replacing the email address provided by the data subject with an alternate email address that would in and of itself not identify the data subject (Example: 'sfjgsdfsafgkas@pseudo.nym'). With this approach, two options emerged in the discussion, where (a) the same unique string would be used for multiple registrations by the data subject ('pseudonymisation'), or (b) the string would be unique for each registration ('anonymization'). Under option (a), the identity of the data subject might - but need not necessarily - become identifiable by cross-referencing the content of all domain name registrations the string is used for.

From these options, the following question arose:

1. Under options (a) and/or (b), would the alternate address have to be considered as personal data of the data subject under the GDPR and what would be the legal consequences and risks of this determination with regard to the proposed publication of this string in the publicly accessible part of the registration data service (RDS)?

**Legal vs. Natural**

1. As a follow-up to the previously provided memos on [Accuracy](https://community.icann.org/download/attachments/102138857/ICANN%20-%20Memo%20on%20Accuracy.docx?version=1&modificationDate=1550152014000&api=v2) and [Legal vs. Natural](https://community.icann.org/download/attachments/102138857/Natural%20vs.%20Legal%20Memo.docx?version=1&modificationDate=1548874825000&api=v2) 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:**

Does the accuracy principle only take into account the interests of the data subject and [a] controller (e.g., ICANN’s or the contracted parties’ interest in maintaining the security and stability of the Internet’s unique identifiers), or does the principle also consider 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)

**Question 2:**

The Legal vs. Natural person memo discusses a “risk of liability” if additional steps are not taken to ensure the accuracy of data. How do you characterize the level of risk of liability - low, medium, or high?  What is the threshold for “reason to doubt” registrant self-identification that triggers this risk of liability? Is the risk in Paragraph 17 the same or different than the risk discussed in Paragraph 23? Would detailed notice at the time of registration and ongoing renewals reduce the risk that data subjects will wrongly self-identify to a negligible level?

* “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 vs. Natural)
* “When a registrant identifies as either a natural or a legal person, this self-identification will determine whether the data provided is made publicly available by default. If there is a **reasonable risk** that data subjects will wrongly self-identify, then failing to make the consequences of the self-identification known to data subjects could **result in liability** for failing to meet the Lawfulness, Fairness and Transparency Principle.” (emphasis added) (Paragraph 23 – Legal vs. Natural)

2.Registration data submitted by legal person registrants may contain the data of natural persons.  A Phase 1 memo stated that registrars can rely on a registrant's self-identification as legal or natural person if risk is mitigated by taking further steps to ensure the accuracy of the registrant's designation.

As a follow-up to that memo: what are the consent options and requirements related to such designations?  Specifically: are data controllers entitled to rely on a statement obligating legal person registrants to obtain consent from a natural person who would act as a contact and whose information may be publicly displayed in RDS? If so, what representations, if any, would be helpful for the controller to obtain from the legal person registrant in this case?

As part of your analysis, please consult the GDPR policies and practices of the Internet protocol (IP address) registry RIPE-NCC (the registry for Europe, based in the Netherlands).  RIPE-NCC’s customers (registrants) are legal persons, usually corporations.  Natural persons can serve as their contacts, resulting in the data of natural persons being displayed publicly in WHOIS.  RIPE-NCC places the responsibility on its legal-person registrants to obtain permission from those natural persons, and provides procedures and safeguards for that.  RIPE-NCC states mission justifications and data collection purposes similar to those in ICANN's Temporary Specification.  Could similar policies and procedures be used at ICANN?

 Please see these specific references:

1) “How We're Implementing the GDPR: Legal Grounds for Lawful Personal Data Processing and the RIPE Database”:

[https://labs.ripe.net/Members/Athina/gdpr-legal-grounds-for-lawful-personal-data-processing-and-the-ripe-database [labs.ripe.net]](https://urldefense.proofpoint.com/v2/url?u=https-3A__labs.ripe.net_Members_Athina_gdpr-2Dlegal-2Dgrounds-2Dfor-2Dlawful-2Dpersonal-2Ddata-2Dprocessing-2Dand-2Dthe-2Dripe-2Ddatabase&d=DwMFaQ&c=FmY1u3PJp6wrcrwll3mSVzgfkbPSS6sJms7xcl4I5cM&r=8K75qGdDlOta4kh6k2F0jrT195M3tF3J_Fxcz6EvuG2kYKDeA67ZTEnthHXAPVXH&m=lm9kGn8JwDnJnbIoNg4je0dwEcDgveT_fksb7KE3MsY&s=JjRQGYCd0W_N54phYbjtCv9Bxt1nS4buSJcvPJf_6vw&e=)

2)  “How We're Implementing the GDPR: The RIPE Database”: [https://labs.ripe.net/Members/Athina/how-we-re-implementing-the-gdpr-the-ripe-database [labs.ripe.net]](https://urldefense.proofpoint.com/v2/url?u=https-3A__labs.ripe.net_Members_Athina_how-2Dwe-2Dre-2Dimplementing-2Dthe-2Dgdpr-2Dthe-2Dripe-2Ddatabase&d=DwMFaQ&c=FmY1u3PJp6wrcrwll3mSVzgfkbPSS6sJms7xcl4I5cM&r=8K75qGdDlOta4kh6k2F0jrT195M3tF3J_Fxcz6EvuG2kYKDeA67ZTEnthHXAPVXH&m=lm9kGn8JwDnJnbIoNg4je0dwEcDgveT_fksb7KE3MsY&s=P3RxR6-R3MLf69vdiLp4krKwIoY7I7DCUBIhoLT8cog&e=)

If time permits, also see the policies of ARIN, the IP address registry for North America.  ARIN has some customers located in the EU.  ARIN also publishes the data of natural persons in its WHOIS output.  ARIN’s customers are natural persons, who submit the data of natural person contacts.

3) ARIN "Data Accuracy": [https://www.arin.net/reference/materials/accuracy/ [arin.net]](https://urldefense.proofpoint.com/v2/url?u=https-3A__www.arin.net_reference_materials_accuracy_&d=DwMFaQ&c=FmY1u3PJp6wrcrwll3mSVzgfkbPSS6sJms7xcl4I5cM&r=8K75qGdDlOta4kh6k2F0jrT195M3tF3J_Fxcz6EvuG2kYKDeA67ZTEnthHXAPVXH&m=lm9kGn8JwDnJnbIoNg4je0dwEcDgveT_fksb7KE3MsY&s=DOP1W8-coJ5GL4C6NL2umOQTFaaa3hISZ_mxhF7HFwg&e=)

4) ARIN Registration Services Agreement, paragraph 3: [https://www.arin.net/about/corporate/agreements/rsa.pdf [arin.net]](https://urldefense.proofpoint.com/v2/url?u=https-3A__www.arin.net_about_corporate_agreements_rsa.pdf&d=DwMFaQ&c=FmY1u3PJp6wrcrwll3mSVzgfkbPSS6sJms7xcl4I5cM&r=8K75qGdDlOta4kh6k2F0jrT195M3tF3J_Fxcz6EvuG2kYKDeA67ZTEnthHXAPVXH&m=lm9kGn8JwDnJnbIoNg4je0dwEcDgveT_fksb7KE3MsY&s=vNYCjbgMw_MmaPMiwqygL3syqrs9GqG_mmTZVpoIjoA&e=)

"Personal Data Privacy Considerations At ARIN": [https://teamarin.net/2018/03/20/personal-data-privacy-considerations-at-arin/ [teamarin.net]](https://urldefense.proofpoint.com/v2/url?u=https-3A__teamarin.net_2018_03_20_personal-2Ddata-2Dprivacy-2Dconsiderations-2Dat-2Darin_&d=DwMFaQ&c=FmY1u3PJp6wrcrwll3mSVzgfkbPSS6sJms7xcl4I5cM&r=8K75qGdDlOta4kh6k2F0jrT195M3tF3J_Fxcz6EvuG2kYKDeA67ZTEnthHXAPVXH&m=lm9kGn8JwDnJnbIoNg4je0dwEcDgveT_fksb7KE3MsY&s=KlSoVh8AH6aCxEBNTX5SsqDBgwzhKCWxVRcIRCcBdKg&e=)  especially the first two paragraphs

**Territorial Scope**

In light of 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]](https://urldefense.proofpoint.com/v2/url?u=https-3A__edpb.europa.eu_sites_edpb_files_files_file1_edpb-5Fguidelines-5F3-5F2018-5Fterritorial-5Fscope-5Fafter-5Fpublic-5Fconsultation-5Fen.pdf&d=DwMGaQ&c=FmY1u3PJp6wrcrwll3mSVzgfkbPSS6sJms7xcl4I5cM&r=8K75qGdDlOta4kh6k2F0jrT195M3tF3J_Fxcz6EvuG2kYKDeA67ZTEnthHXAPVXH&m=Hp7wVK2hs6CZqta2UKooi45XgWxs_ewi2xZAubx2Mmg&s=AWC8WQzJteguKr-GfwwJlZbhdpg_11Ofi6vOiFU0IJ8&e=),

Does this ruling and the Guidelines affect:

1.      The advice given in [Phase 1 Regarding Territorial Scope](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Furldefense.proofpoint.com%2Fv2%2Furl%3Fu%3Dhttps-3A__nam06.safelinks.protection.outlook.com_-3Furl-3Dhttps-253A-252F-252Fcommunity.icann.org-252Fdownload-252Fattachments-252F102138857-252FICANN-252520-2D-252520Memo-252520on-252520Territorial-252520Scope-252520.docx-253Fversion-253D1-2526modificationDate-253D1552176561000-2526api-253Dv2-26data-3D02-257C01-257CMarksv-2540microsoft.com-257C0fc10369b86b4fb54cdb08d745d81ad8-257C72f988bf86f141af91ab2d7cd011db47-257C1-257C1-257C637054666773951714-26sdata-3D85hB3n-252BgHO5zltdzTm5Pmd-252FUeu0T7OL-252F4bywkCcb7dg-253D-26reserved-3D0%26d%3DDwMGaQ%26c%3DOGmtg_3SI10Cogwk-ShFiw%26r%3DqQNCXqU_XE2XIdXbawYmk-YDflYH6pd8ffXlzxU37OA%26m%3DqgqaikAoSyJzElcg7C-u09feQBWajzhT1JT2LBv05jg%26s%3D8TCbK69KiXCKrPpNO-KL9rKcsRkCISjzvCof8uKQBRs%26e%3D&data=02%7C01%7CMarksv%40microsoft.com%7C2925832daae546b63e0408d745f74dba%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637054800792839937&sdata=exadgrNqqCKVQ%2FLTBKZXXJMnBkfDjA9SNSTaJuX%2FH4Q%3D&reserved=0), in Sections 6.2- 6.9?

2.      The advice given in Q1-2 with respect to liability (Section 4 of the memo)?

3.      In light of this ECJ decision and the [Geographic Scope Guidelines](https://urldefense.proofpoint.com/v2/url?u=https-3A__edpb.europa.eu_sites_edpb_files_files_file1_edpb-5Fguidelines-5F3-5F2018-5Fterritorial-5Fscope-5Fafter-5Fpublic-5Fconsultation-5Fen.pdf&d=DwMGaQ&c=OGmtg_3SI10Cogwk-ShFiw&r=qQNCXqU_XE2XIdXbawYmk-YDflYH6pd8ffXlzxU37OA&m=VH1lTBbXRHuGBzmHv6MDdFMGJFp4rxC3HNks7yXp8Ag&s=Wm0q2xFIYFO65E1T_FPWz5HfiNnV_iNT5JBbHTsyVQM&e=), using the same assumptions identified for Q1 and Q2, would there be less risk to EEA-based contracted parties if:

A.      an SSAD operated by ICANN (as opposed to the EEA-based contracted party) based in ICANN’s Los Angeles Headquarters allowed automated disclosure responses for redacted data of registrants located outside of the EU where such data may or may not be processed by processors or additional controllers inside the EU or otherwise subject to the GDPR, for legitimate, 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](https://urldefense.proofpoint.com/v2/url?u=https-3A__nam06.safelinks.protection.outlook.com_-3Furl-3Dhttps-253A-252F-252Feur-2Dlex.europa.eu-252Flegal-2Dcontent-252FEN-252FTXT-252F-253Furi-253DCELEX-253A12012P-252FTXT-26data-3D02-257C01-257CMarksv-2540microsoft.com-257C2925832daae546b63e0408d745f74dba-257C72f988bf86f141af91ab2d7cd011db47-257C1-257C1-257C637054800792819948-26sdata-3DRxgqL9eYdRavnaFqIDjzDOT4GPHJRSsmQ1-252Favz10vKw-253D-26reserved-3D0&d=DwMGaQ&c=5VD0RTtNlTh3ycd41b3MUw&r=_4XWSt8rUHZPiRG6CoP4Fnk_CCk4p550lffeMi3E1z8&m=VLG2NlF9SKlO5Br01dwddo_lA4oncgv7PkSSSsw8ZV4&s=fPD2dxvOeBSKNBXQT0rUNkNPmaova0kNQcFCii_4G6Y&e=)

**WHOIS ACCURACY**

1. Can you provide further information and explanation on the reference to third parties mentioned in para 19 in which "ICANN and the relevant parties may rely on to confirm the accuracy of personal data if it is reasonable to do so"? Please describe these third parties and their contemplated role. Do they become in such a scenario data processors?
2. Bird & Bird’s memo on the meaning of the GDPR’s Accuracy Principle concluded that this Principle “requires controllers to take ‘reasonable steps’ to ensure that personal data is accurate and up to date. Memo at ¶15.

This memo also cited to 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 observed that:

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 RAA,

1)            What additional reasonable steps should data controllers take to ensure the accuracy of the data submitted with regard to the purposes for which they are processed?

2)            What additional reasonable steps should data controllers take to ensure the overall appropriate levels of data accuracy?  In particular, would it be advisable for data controllers to implement the methods identified 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:

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)

in order to ensure the overall appropriate levels of data accuracy?

3)            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?