Updated: 10 Feb 2020

Priority 2 Topics	Next Steps & proposed timing by EPDP Leadership
Display of information of affiliated vs. accredited privacy / proxy providers Phase 1 rec: "In the case of a domain name registration where an "affiliated" privacy / proxy service used (e.g. where data associated with a natural person is masked), Registrar (and Registry where applicable) MUST include in the public RDDS and return in response to any query full non-personal RDDS data of the privacy / proxy service, which MAY also include the existing privacy/proxy pseudonymized email. Note, PPSAI is an approved policy that is currently going through implementation. It will be important to understand the interplay between the display of information of affiliated vs. accredited privacy / proxy providers. Based on feedback received on this topic from the PPSAI IRT, the EPDP Team may consider this further in phase 2".	• EPDP Support Staff to reach out to GDD colleagues who support the PPSAI IRT (which is currently on hold) to obtain information on if/how the display of information of affiliated vs. accredited privacy / proxy providers is dealt with in the context of the implementation of the PPSAI recommendations (before ICANN66) **COMPLETED** • Response received on 3 December (see https://mm.icann.org/pipermail/gnso-epdp-team/2019-December/002868.html) confirming that " the PP IRT was considering a proposed requirement that all privacy and proxy service providers include a label, which would flag each registration as a privacy/proxy registration and identify which provider is associated with that registration, in the existing WHOIS output "registrant organization" field. (See Draft PPAA, distributed to PP IRT 12 Sept 2018, at Section 3.15). This requirement would apply to all privacy and proxy service providers, regardless of whether the provider is affiliated with a registrar or registry operator or operating independently of any other contracted party. The draft privacy and proxy service provider accreditation agreement does not distinguish between requirements for registrar-affiliated and non-affiliated privacy and proxy service providers, at the direction of the PPSAI IRT. The draft requirements would require all privacy and proxy service providers to become accredited to continue offering those services. This requirement for accreditation would be enforced through the registrar, on the grounds that accredited registrars could not knowingly accept registrations involving a privacy or proxy service from an unaccredited provider (See PPSAI recommendation 1, note, p. 7, https://gnso.icann.org/sites/default/files/filefield_48305/ppsai-final-07dec15-en.pdf).

	Following the completion of the EPDP Phase 2 work and the Rec 27 analysis, the existing draft PPSAI materials will need to be revisited to ensure consistency with the EPDP-recommended requirements, and to ensure the requirements and processes fit together in a manner that will create a transparent, predictable, and reasonable process for all parties involved. • **Based on input received, EPDP Support Staff recommends the EPDP Team to consider the following recommendation**: Following the implementation of the PPSAI recommendations, the EPDP Team recommends that EPDP Phase 1 recommendation #14 ("In the case of a domain name registration where an "affiliated" privacy/proxy service used (e.g. where data associated with a natural person is masked), Registrar (and Registry where applicable) MUST include in the public RDDS and return in response to any query full non-personal RDDS data of the privacy/proxy service, which MAY also include the existing privacy/proxy pseudonymized email.) applies to all accredited privacy and proxy services.
Legal vs. natural persons Phase 1 rec: 2) The EPDP Team recommends that as soon as possible ICANN Org undertakes a study, for which the terms of reference are developed in consultation with the community, that considers: • The feasibility and costs including both implementation and potential liability costs of differentiating between legal and natural persons; • Examples of industries or other organizations that have successfully differentiated between legal and natural persons; • Privacy risks to registered name holders of differentiating between legal and natural persons; and • Other potential risks (if any) to registrars and registries of not differentiating.	• EPDP Support staff to confirm expected next steps and timing to conduct and publish study results (before ICANN66). (COMPLETED) • Session scheduled at ICANN66 to review draft Terms of Reference – see slides presented. • See update provided by Karen Lentz during Jan LA F2F meeting (https://community.icann.org/x/WgVxBw) • The following questions are under review by the legal committee: 1. 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?

3) The EPDP Team will determine and resolve the Legal vs. Natural issue in Phase 2.	"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? • EPDP Team to review results of study (when available) and responses to legal questions (if sent) and reconsider whether Contracted Parties should be allowed or required to treat legal and natural persons differently, and what mechanism is needed to ensure reliable determination of status.
City field redaction From phase 1 rec: The EPDP Team expects to receive further legal advice on this topic, which it will analyze in phase 2 of its work to determine whether or not this recommendation should be modified.	• Legal committee to review and analyze legal advice received on this topic and recommend next steps to the EPDP Team, which could include modification of the phase 1 recommendation, maintaining phase 1 recommendation as is, and/or additional legal guidance to help inform a determination on whether or not the recommendation should be modified.

Data retention From phase 1 rec: In order to inform its Phase 2 deliberations, the EPDP team recommends that ICANN Org, as a matter of urgency, undertakes a review of all of its active processes and procedures so as to identify and document the instances in which personal data is requested from a registrar beyond the period of the 'life of the registration'. Retention periods for specific data elements should then be identified, documented, and relied upon to establish the required relevant and specific minimum data retention expectations for registrars. The EPDP Team recommends community members be invited to contribute to this data gathering exercise by providing input on other legitimate purposes for which different retention periods may be applicable.	• EPDP Support staff to confirm status of ICANN org's process and procedures review (before ICANN66) (Status: response received on 2 November: see https://mm.icann.org/pipermail/gnso-epdp-team/2019-November/002747.html) (COMPLETED) • EPDP Team to consider whether updates are needed to phase 1 data retention recommendation. • At a minimum, the EPDP Team would need to reconfirm its original recommendation, which was adopted on an interim basis, that registration data must be retained for a period of fifteen months following the life of the registration plus three months to implement the deletion, i.e., 18 months.
Potential OCTO Purpose From phase 1 rec: the EPDP Team commits to considering in Phase 2 of its work whether additional purposes should be considered to facilitate ICANN's Office of the Chief Technology Officer (OCTO) to carry out its mission (see https://www.icann.org/octo). This consideration should be informed by legal guidance on if/how provisions in the GDPR concerning research apply to ICANN Org and the expression for the need of such pseudonymized data by ICANN."	• EPDP Support Staff to follow up with ICANN org whether status of input provided during phase 1 has changed and/or whether any legal guidance has been obtained in relation to ICANN org having a qualified research position under GDPR (prior to ICANN66) (**Status: message sent – awaiting response**) • Based on feedback received (once received), EPDP Team to determine next steps.

Feasibility of unique contacts to have a uniform anonymized email address From the Annex to the Temporary Specification: Addressing the feasibility of requiring unique contacts to have a uniform anonymized email address across domain name registrations at a given Registrar, while ensuring security/stability and meeting the requirements of Section 2.5.1 of Appendix A.	• The following question has been submitted to legal counsel: **Privacy/Proxy and Pseudonymized Emails** 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 guidance received on 8 February 2020 (see https://mm.icann.org/pipermail/gnso-epdp-team/2020-February/003065.html). • EPDP Legal Committee to review legal guidance and make recommendation for next steps to EPDP Team.

Accuracy and WHOIS Accuracy Reporting System	• EPDP Team to review correspondence on this topic ICANN org and the GNSO Council:
	  ○ https://www.icann.org/en/system/files/correspondence/marby-to-drazek-05dec19-en.pdf
	  ○ https://gnso.icann.org/en/correspondence/drazek-to-marby-15oct19-en.pdf
	  ○ https://gnso.icann.org/en/correspondence/marby-to-drazek-21jun19-en.pdf)
	• The following question has been submitted to legal counsel:
	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)

	• 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? • 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? • EPDP Team to review response to legal questions (if sent / once available)