Business Constituency (BC) EPDP Phase 2A Public Comment Form

19 July 2021

Note: This response was drafted by Alex Deacon, Barbara Wanner, Margie Milam, Mark Svancarek, Mason Cole, Andrew Bennett, and Niklas Lagergren. It was approved in accord with the BC Charter.

Preliminary Recommendation #1 (Phase 1 Rec. 17)	Preliminary Rec. 1: No changes are recommended, at this stage, to the EPDP Phase 1 recommendation on this topic ("Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so")

1. Question for Community Input: Is there new information or inputs that the Phase 2A team has not considered in assessing whether to make changes to the recommendation that Registrars and Registry Operators may, but are not obligated to, differentiate between legal and natural persons?

The BC believes that ample legal and practical, real-life information already has been presented to and informed discussions of EPDP Phase 2A work. This has highlighted the critical need for and requirement that Registries and Registrars differentiate between legal and natural persons. We reiterate that the inability of Internet users to identify with whom they are doing business with online, and the increasingly pervasive inability of law enforcement, cybersecurity, and legal professionals to identify criminal actors online through their domain name registration data, continues to severely undermine the security and stability of the Internet.

The BC concurs with the GAC and other SO/ACs that "voluntary" differentiation of legal/natural persons is inadequate. Differentiation between legal and natural persons should be required to ensure a healthy and stable digital ecosystem for the DNS. Steady progress in the European Parliament to finalize NIS2 legislation continues to strengthen this view, with the latest development coming from the Internal Market Committee's (IMCO) adoption on July 12th of Compromise Amendments to what will be a highly influential Opinion in the development of the lead committee's final report (expected on October 14th) and, ultimately, the legislative resolution anticipated for the Parliament's Plenary Session in December.

Compromise Amendment 20 on Article 23 of the NIS2 Directive reveals that the European Parliament expects contracted parties to differentiate legal vs natural persons, and to make public all of the domain registration data for the former. The bold/italicized text below reflects the suggested changes to paragraph 4 of Article 23, and we strongly encourage the entire ICANN community to review the Compromise Amendments in full[1]:

> Member States shall ensure that the TLD registries and the entities providing domain name registration services ***make publicly available***, without undue delay ***and in any event within 24 hours*** after the registration of a domain name, ***all*** domain registration data ***of legal persons as registrants***.

We appreciate that the Phase 2A Report details other benefits contracted parties will gain by making the legal vs natural differentiation. For example, publishing legal persons' data based on differentiation instead of consent significantly reduces the Contracted Parties' liability; and following proper safeguards also lowers the risks associated with publishing registration data for legal entities.

[1] Available at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2021/07-12/p5-CAs_cybersecurityNIS2_EN.pdf

Preliminary Recommendation #2	The EPDP Team recommends that the GNSO Council monitors developments in relation to the adoption and implementation of relevant legislative changes (for example, NIS2), relevant decisions by pertinent tribunals and data protection authorities, as well as the possible adoption of the SSAD to determine if/when reconsideration of this question (whether changes are required to the EPDP Phase 1 recommendation "Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so") is warranted. The GNSO Council is expected to consider not only input on this question and any new information from GNSO SG/Cs but also ICANN SO/ACs to help inform a decision on if/when this question is expected to be reconsidered.

2. Question for Community Input: Is this recommendation necessary for the GNSO council in considering future policy work in this area? If yes, in what ways does this monitoring assist the Council?

Yes -- it is critical that the GNSO Council continue this work. NIS2 legislation will be the most prominent -- but not the only – clarification from elected officials and regulators when it comes to the requirements for "registries and entities providing domain name registration services for the TLD [to] have policies and procedures in place to ensures that the database infrastructure includes accurate, verified and complete information."[2]

The importance of GNSO Council monitoring of these developments is only increasing. The development of incremental drafts and compromise amendments at the committee level for NIS2 signal that the legislation will address and impact the issue of legal vs natural differentiation along with many other issues material to existing and future policy work around WHOIS, including accuracy, critical data elements, timely publication of non-personal data, and timely reply to legitimate access seekers. ICANN should be keenly aware that key stakeholders, including regulatory authorities in Europe and the United States, are keeping a close eye on the European Parliament's engagement on these issues via NIS2. Forthcoming opinions and even decisions by tribunal and privacy regulatory authorities are likely and could accelerate as a result of the NIS2 proceedings.

As the BC has stated in previous comments, the SSAD fails to provide guidance to contracted parties about how to address data accuracy and distinctions between legal and natural persons. Further, the SSAD is inflexible and lacks the ability to evolve with anticipated legislative developments in the EU and elsewhere and updates to data privacy laws that may have a significant impact on obligations to disclose registrant data. Thus, ongoing work by the GNSO Council is imperative to inform appropriate changes to the SSAD, which ideally will create a more centralized and adaptable disclosure framework, and mandate disclosure by contracted parties.

[2] Secretariat of the Committee on the Internal Market and Consumer Protection, "Compromise amendments on the Draft Opinion on the measures for a high common level of cybersecurity across the Union, repealing Directive (EU)", *Compromise Amendment 20 on Article 23, Paragraph 3.*

Preliminary Recommendation #3	The following additions are made to the EPDP Phase 1 recommendations: Recommendation #5 The following optional data element (optional for the Registrar to offer to the Registrant and collect) is added to the data elements table: [Please refer to the Data Elements Tables on pp. 5-6.] For the purpose of the Legal person and non-personal data field, which is optional for the Registrar to provide to the Registrant to self-designate, Registrars should advise the Registered Name Holder at the time of registration what the consequences are of self-designating as a legal or a natural person and to provide non-personal data only (or provide appropriate consent if personal data is involved), consistent with preliminary recommendation #3, point 4. The EPDP Team recommends that the applicable updates are made to the Registry Registration Data Directory Services Consistent Labeling and Display Policy and the RDAP profile consistent with this recommendation. The EPDP Team expects ICANN org to consult with the EPDP Phase 2a IRT, or the IRT that has been assigned the responsibility for implementing this recommendation, and if applicable the GNSO Council, about these changes. For clarity, the existence of this standardized data element does not require a Contracted Party to differentiate between legal / natural person type or personal / non-personal data. As part of the implementation, it should be considered whether for those Contracted Parties that choose not to differentiate, the data field is not visible in RDDS or automatically set to "unspecified".

3. Question for Community Input: Should a standardized data element be available for a Contracted Party to use? If yes, why? If no, why not? Why is harmonization of practices beneficial or problematic?

Yes -- The BC urges that a standardized data element be made available for contracted party use and that Registries/Registrars should be required to use it. Harmonizing this data element will create a more consistent and reliable WHOIS database, which may be accessed by third parties for legitimate purposes. This will facilitate more effective and prompt response to DNS abuse, cybercrime activity, intellectual property violations, and other activity that threatens consumer welfare.

The standardization of the data element must extend to standardization of publication of the data element. A standardized data element must be defined to create an updated RDAP profile consistent with the recommendation. This is true whether the data element is published in the public RDDS, or redacted and transmitted alongside personal data disclosed from SSAD. Regarding the latter option, we note that such a data element will never contain personal data, and therefore should never be redacted; we include both options only for completeness.

4. Question for Community Input: If yes, what field or fields should be used and what possible values should be included, if different from the ones identified above?

The BC regards the above guidance to contracted parties who wish to differentiate as sufficient. No other fields or values are required. That said, it would be useful if the same Natural/Legal distinction were available to Technical Contact fields as well as Registrant data fields.

5. Question for Community Input: If such a standardized data element is available, MUST a Contracted Party who decides to differentiate use this standardized data element or should it remain optional for how a Contracted Party implements this differentiation?

If such a standardized data element is available, a Contracted Party should be required to use it. As the BC notes in question 3, Harmonizing this data element will create a more consistent and reliable WHOIS database, which may be accessed by third parties for legitimate purposes. This will facilitate more effective and prompt response to DNS abuse, cybercrime activity, intellectual property violations, and other activity that threatens consumer welfare.

Preliminary Recommendation #4	The EPDP Team recommends that Contracted Parties who choose to differentiate based on person type SHOULD follow the guidance below and clearly document all data processing steps. However, it is not the role or responsibility of the EPDP Team to make a final determination with regard to the legal risks, as that responsibility ultimately belongs to the data controller(s). 1. Registrants should be allowed to self-identify as natural or legal persons. Registrars should convey this option for Registrants to self-identify as natural or legal persons (i) at the time of registration, or without undue delay after registration, and (ii) at the time the Registrant updates its contact information or without undue delay after the contact information is updated. 2. Any differentiation process must ensure that the data of natural persons is redacted from the public RDDS unless the data subject has provided their consent to publish or it may be published due to another lawful basis under the GDPR, consistent with the "data protection by design and by default" approach set forth in Article 25 of the GDPR. 3. As part of the implementation, Registrars should consider using a standardized data element in the RDDS, SSAD or their own data sets that would indicate the type of person it concerns (natural or legal) and, if legal, also the type of data it concerns (personal or non-personal data). Such flagging would facilitate review of disclosure requests and automation requirements via SSAD and the return of non-personal data of legal persons by systems other than SSAD (such as Whois or RDAP). A flagging mechanism may also assist in indicating changes to the type of data in the registration data field(s). 4. Registrars should ensure that they clearly communicate the nature and consequences of a registrant identifying as a legal person. These communications should include: a. An explanation of what a legal person is in plain language that is easy to understand. b. Guidance to the registrant (data subject) by the Registrar concerning the possible consequences of: i. Identifying their domain name registration data as being of a legal person; ii. Confirming the presence of personal data or non-personal data, and; iii. Providing consent. This is also consistent with section 3.7.7.4 of the Registrar Accreditation Agreement (RAA). 5. If the Registrants identify as legal persons and confirm that their registration data does not include personal data, then Registrars should publish the Registration Data in the publicly accessible Registration Data Directory Services. 6. Registrants (data subjects) must have an easy means to correct possible mistakes. 7. Distinguishing between legal and natural person registrants alone may not be dispositive of how the information should be treated (made public or masked), as the data provided by legal persons may include personal data that is protected under data protection law, such as GDPR.

6. Question for Community Input: Does this guidance as written provide sufficient information and resources to Registrars and Registry Operators who wish to differentiate? If not, what is missing and why?

The BC regards the above guidance to contracted parties who wish to differentiate as sufficient. However, #7 is not necessary, as the importance of defining a legal person, noting that designation as a legal entity might include personal data, and requiring registrant consent if the latter is the case, has been laid out clearly in points 1-6.

During both EPDP Phase 2 and EPDP Phase 2a the value of "flags" for streamlining both manual and automated processing was discussed. We note the value of updating such flags once a disclosure request has been processed and the absence or presence of personal data has already been determined, which ensures that any future requests for that same non-personal can be automated. Standardized data elements indicating the presence or absence of personal data, whether at the registration level or at the level of individual data fields, function as such flags.

7. Question for Community Input: Are there additional elements that should be included in the guidance?

The BC regards the above guidance to contracted parties who wish to differentiate as sufficient. No other fields or values are required.

8. Question for Community Input: Are there legal and regulatory considerations not yet considered in this Initial Report, that may inform Registries and Registrars in deciding whether and how to differentiate, and if so, how?

As detailed above, the NIS2 legislation, when enacted, will offer further legal protection to Registries and Registrars about differentiation. Other countries active in the DNS -- i.e., Japan, the United States, the United Kingdom -- also may consider regulatory changes that would provide clarity to Registries and Registrars about possible legal exposure when differentiating between legal and natural persons, and how to minimize or even eliminate such exposure. As stated above, it is for this reason that the GNSO Council should continue to monitor legal and regulatory developments in the EU and elsewhere so the EPDP and SSAD can be appropriately updated.

9. Question for Community Input: If a Registrar or Registry Operator decides to differentiate, should this guidance become a requirement that can be enforced if not followed ("MUST, if Contracted Party decides to differentiate")?

Yes, this should be enforced. Failure to enforce risks undermining the guidance and opening the door to Registries/Registrars using other more stringent approaches that discourage Registrant disclosure and cause back-sliding and weakening of the overall framework of the EPDP.

Preliminary Recommendation #5	The EPDP Team recommends that Contracted Parties who choose to publish a registrant- or registration-based email address in the publicly accessible RDDS should ensure appropriate safeguards for the data subject in line with relevant guidance on anonymization techniques provided by their data protection authorities and the appended legal guidance in this recommendation (see Annex E)

10. Question for Community Input: Does this guidance as written provide sufficient information and resources to Registrars and Registry Operators who wish to publish a registrant-based or registration-based email address? If not, what is missing and why?

The BC regards the above guidance to contracted parties who wish to differentiate as sufficient.

Additional Input	Please use this section of the form for comments or issues not addressed in the previous questions.

11. Are there any other comments or issues you would like to raise pertaining to the EPDP Phase 2A Initial Report? If yes, please enter your comments here. If applicable, please specify the section or page number in the Initial Report to which your comments refer.

At ICANN 71, the chair of the EPDP Phase 2A team made clear that if community comments on EPDP Phase 2A do not provide the team with a path to consensus, the GNSO will discontinue this work in accordance with the GNSO's new rules and parameters for PDPs. That outcome not only would be acutely disappointing to the BC and other SO/ACs, but also threaten the security and stability of the DNS. The absence of a framework that provides DNS users with timely access to accurate registration data and evolves as the regulatory and legislative landscape changes will create fertile ground for highly destabilizing cyber behavior.