IPC EPDP Phase 2A Minority Statement

Data protection law, including the GDPR, does not apply to non-personal data. In fact, while the GDPR is admittedly somewhat ambiguous, it may not even apply to personal data pertaining to legal entities.[[1]](#footnote-1) Accordingly, databases like WHOIS/RDDS, which serve a multitude of public interest purposes, should only redact data which are demonstrably personal data requiring disparate treatment due to data protection law. However, the EPDP Phase 2A inexplicably and inappropriately shifted the “burden of proof” or at least “burden of persuasion” to those advocating for the common-sense outcome: non-personal data should not be concealed. The IPC notes that the EPDP Phase 2A began its work on the wrong foot entirely by taking on this inappropriate burden and by attempting to provide guidance rather than create binding consensus policy. This is not the role of the PDP - which is designed to develop consensus policy binding equally on all contracted parties. The IPC further notes a troubling trend in multistakeholder policy development throughout the EPDP’s numerous phases: little success is possible when some stakeholders are only willing to act exclusively in their own interests with little regard for compromise in the interest of the greater good. Now more than ever we need to bring our stakeholders together in the interest of the security, stability, and resiliency of the DNS and “promoting the global public interest” as set forth in ICANN’s Articles of Incorporation. Finally, we note that the “consensus” designation ascribed to EPDP Phase 2A recommendations inadequately reflects the division within the working group on these outcomes, and does not reflect that the EPDP Phase 1 Recommendation 17.3 “The EPDP Team will determine and resolve the Legal vs. Natural issue in Phase 2” remains unresolved without a requirement to differentiate.

Specific comments on the EPDP Phase 2A follow.

1. Rely on registrant self-designation

One of the most common-sense disappointments in the EPDP Phase 2A recommendations is the concept that contracted parties should not be required to rely on what a registrant tells them about the nature of the RDS data, and either publish or redact the data accordingly. Legal advice confirmed this common sense assessment, calling the data “low sensitivity”, the risk “low”, and even in the event of erroneous publication based on a registrant’s incorrect self-designation, that “an order to correct the issue (likely accompanied by a reasonable period in which to implement changes), rather than a fine, seems most likely, finding “no examples of enforcement in relation to this.”[[2]](#footnote-2)

Operating on the basis of such legal advice, a group truly working in the public interest should have easily agreed to publish data that was identified by the data subject as non-personal data. And yet no such agreement emerged.

1. Common data element

The IPC clearly supports the development of a common data element - or elements - to reflect whether RDS data pertains to a legal entity or a natural person registrant and/or whether the data itself contains personal data. While underwhelming as the most impactful outcome of Phase 2A, the IPC is supportive and appreciative of the multistakeholder model coming to consensus on this standardized data element.

That being said, the IPC and colleagues from other Constituencies and Advisory Committees strongly believe that such a standardized data element should be mandatory, especially in the absence of the common-sense publication of data according to registrant representation. While we are encouraged by the agreement to develop this data element, we doubt the likely positive impact of this compromise if such a data element never achieves widespread use by contracted parties. In fact, the IPC is frankly disappointed and discouraged that the Phase 2A team could not agree on any greater use of this data element. Possibilities ranged from optional collection for new domains only to mandatory collection and publication of the field for all domains under management. Yet the bare minimum - optional collection - was the only outcome with the possibility of gaining consensus. This is especially disappointing given that the field itself is not personal data, and therefore no risk exists to publish it. Furthermore, contracted parties never provided any reason for opposing mandatory collection or publication of this data element. They merely repeated “we don’t see the value” (presumably to them as registries and registrars) when presented with the rationale provided by non-contracted parties, which includes: utility for the SSAD, indication of whether to submit an SSAD request or one-off registry/registrar request, information about whether the data was redacted for cause or out of convenience to the contracted party, among others.

1. Future Code of Conduct work

Finally, although it was potentially out of scope for this EPDP Phase 2A, the Final Report contains a provision requiring ICANN to consider the guidance presented in any future engagement with the European Data Protection Board on a Code of Conduct. As an initial matter, the recommendation is weak insofar as it does not actually mandate the creation of a Code of Conduct. Furthermore, the recommendation is phrased ambiguously to include controllers and processors, with a separate sentence alluding to “the community.” More troublingly, when the IPC insisted that the Final Report clarify that groups representing RDS data requestors be included explicitly as controllers and processors (for their own purposes), some contracted parties objected, referring to requestors as “third party interests.” In the ICANN multistakeholder environment, the community, especially the diverse community represented within and across the GNSO, must not be relegated to “observer” status on something so impactful as the legal status of RDS data which is so fundamental to the security, stability, and resiliency of the DNS.

1. Registrant-based pseudonymous email address

The IPC continues to believe that a registrant-based pseudonymous email address should be published on a mandatory basis in WHOIS/RDDS. Legal guidance obtained by the EPDP Phase 2A team identified the risk of such publication as “moderate” given that such data could be used to identify a natural person registrant when combined with other personal data. However, the public interest benefits of such publication outweigh the data subject’s privacy rights as the ability to use pseudonymized registrant-based email addresses is critical in facilitating cross-domain ownership correlation to address large-scale security threat networks, phishing schemes, and intellectual property-infringing sites. We note that publication of pseudonymized registrant-based email addresses would appear to comply with the GDPR, and note that several European entities in the DNS supply chain actually publish *actual* registrant email addresses without running afoul of GDPR, as noted in the legal guidance provided to the EPDP.[[3]](#footnote-3) In the event that the European Data Protection Board or an individual Data Protection Authority identifies this approach as being non-compliant with GDPR, the policy could be reverted to the current requirement of publishing an anonymized email address or link to web form, with disclosure of actual email address in response to valid third-party requests.

1. Conclusion

In conclusion, although the IPC is supportive of the consensus achieved to create a standardized data element to reflect the (legal vs. natural) nature of the registrant and/or the registration data, the EPDP Phase 2A Final Report fails to accomplish its ultimate goal. The EPDP Phase 1 Recommendation 17.3 required that, in addition to optional differentiation, “The EPDP Team will determine and resolve the Legal vs. Natural issue in Phase 2.” Unfortunately, this topic remains unresolved. Requiring ICANN to coordinate the technical community in the creation of a data element which contracted parties are free to ignore altogether falls far short of “resolving” the legal vs. natural issue. And failing to require differentiation of personal and non-personal data fails to meet the overarching goal of the EPDP to “preserve the WHOIS database to the greatest extent possible” while complying with privacy law.

1. “This Regulation does not cover 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.” GDPR Recital 14 [↑](#footnote-ref-1)
2. <https://community.icann.org/display/EOTSFGRD/EPDP+-P2A+Legal+subteam> [↑](#footnote-ref-2)
3. “In its Whois database, EURid publishes the email addresses of domain name registrants in the .eu TLD (both natural persons and legal entities).... Similarly, while RIPE-NCC relies on consent to publish personal information about tech/admin contacts, it publishes personal information about resource holders on the grounds that ‘facilitating coordination between network operators is the one purpose that justifies the publication of personal data in the RIPE-NCC database and that it is clear that the processing of the personal data referring to a resource holder is necessary for the performance of the registry function, which is carried out in the legitimate interest of the RIPE community and the smooth operation of the Internet globally (and is therefore in accordance with article 6.1.f of the GDPR).’” Bird & Bird memo of 27 April 2021, EPDP Phase 2A Initial Report at 56-57. [↑](#footnote-ref-3)