

ICANN | GAC

Governmental Advisory Committee

Status	Final
Distribution	Public
Date	10 September 2021

Governmental Advisory Committee Minority Report on the Final Report of Phase 2A of the Expedited Policy Development Process (EPDP) on gTLD Registration Data

Note: The At-Large Advisory Committee (ALAC), the Business Constituency (BC), and the Intellectual Property Constituency (IPC) support the views expressed in this comment.

Introduction and Overall Comment	1
Recommendation #1 Fields to Facilitate Differentiation between Legal and Natural Person Registration Data	4
Recommendation #2 Guidance for Contracted Parties who Choose to Differentiate	4
Recommendation #3 Codes of Conduct and Example Scenarios	5
Recommendation #4 Pseudonymized Email addresses	5

Introduction and Overall Comment

The GAC appreciates the considerable time and commitment demonstrated by the EPDP Phase 2A team, its leadership and ICANN support staff to develop these complex and important policy recommendations regarding the treatment of domain name registration data from legal entities and pseudonymized email contacts. While the GAC acknowledges the usefulness of many components of the Final Recommendations, the GAC remains concerned that almost none of the Final Recommendations create enforceable obligations. They therefore fall short of the GAC's expectations for policies that would require the publication of domain name registration data that is not protected under the EU's General Data Protection Regulation (GDPR) and create an appropriate framework to encourage the publication of pseudonymized email contacts with appropriate safeguards.

For context, as the GAC has highlighted in prior inputs,¹ law enforcement, consumer protection, and others tasked with protecting the public from malicious actions facilitated by the DNS, need quick and effective access to domain name registration data. Up until May 2018, such access was publicly available via the WHOIS system. In response to

¹ See [GAC input on EPDP Phase 1 Final Report](#) (20 February 2019), [GAC Input Phase 2 Initial Report](#) (24 March 2020), and [GAC Comment on the Addendum to the Phase 2 Initial Report](#) (5 May 2020). See also [GAC Abu Dhabi Communiqué](#) (1 November 2017), [GAC San Juan Communiqués](#) (15 March 2018), and [GAC Barcelona Communiqué](#) (25 October 2018).

the GDPR, ICANN implemented policies that permit the masking of much of this data, even data that is not protected by the GDPR. Because the GDPR does not protect the contact information of legal persons, many stakeholder groups including the GAC questioned why ICANN policies permitted the redaction of unprotected information in RDS/WHOIS outputs. Therefore, the GAC and other stakeholder groups urged the development of more precise policies that would protect personal data while publishing non-personal data, including registration data related to legal entities, thus recognizing that publishing unprotected domain name registration data benefits the public interest.

The scope of the work under EPDP Phase 2A followed up on these concerns and focused on two topics, namely:

1. the differentiation of legal versus natural persons' registration data, and
2. the feasibility of unique contacts to have a uniform anonymized² email address.

Under the first topic, the questions addressed were as follows:

- i. Whether any updates are required 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");³
- ii. What guidance, if any, can be provided to Registrars and/or Registries who differentiate between registrations of legal and natural persons.

Under the second topic "feasibility of unique contacts to have a uniform anonymized email address", the EPDP Team addressed the questions of:

- i. Whether or not unique contacts to have a uniform anonymized email address is feasible, and if feasible, whether it should be a requirement; and,
- ii. If feasible, but not a requirement, what guidance, if any, can be provided to Contracted Parties who may want to implement uniform anonymized email addresses.

The GAC believes that the Final Phase 2A Recommendations provide several constructive components including:

1. the creation of data fields to flag/identify legal registrants and personal data;
2. specific guidance on what safeguards should be applied to protect personal information when differentiating between the domain name registrations of legal and natural persons;
3. encouragement for the creation of a Code of Conduct that would include the treatment of domain name registration data from legal entities;
4. encouragement for the GNSO to follow legislative developments that may require revisions to the current policy recommendations, and
5. useful context and guidance for those who wish to publish pseudonymized emails.

Nevertheless, the final recommendations fall short because they primarily propose *optional* rather than *required* actions, even as applied to information that is not protected under the GDPR such as the non-personal data of legal entities. Optional actions can lead to a fragmented and uncertain system for requesters and data subjects, with different policies across different registrars for how data is protected or disclosed.⁴

For background, a significant percentage of domain names are registered by legal entities and the GDPR generally does not protect their non-personal domain name registration data. Some analysis shows that a considerably larger set of registration information was redacted as compared to what is required by GDPR, *i.e.* "perhaps five times as

² The EPDP team later concluded that the term "pseudonymized" was the more precise term. See "Definitions" on p.24 of the [EPDP Phase 2A Final Report](#).

³ See Recommendation 17 in the Final Report of EPDP Phase 1 at:

<https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf>.

⁴ The GAC has expressed its concerns regarding policies that risk fragmentation in prior inputs including the [GAC Barcelona Communiqué](#) (25 October 2018). See also [GAC Minority Statement](#) on the Final Report of Phase 2 of the EPDP on gTLD Registration Data (24 August 2020).

much as is necessary.”⁵ Indeed, available data suggest that only around 11.5% of domains may belong to natural persons who are subject to GDPR, while contact data from 57.3% of all domains was redacted.⁶ This arguably unnecessary masking of vast amounts of registration data impedes many of the benefits associated with transparency regarding the ownership of domain names.

With regard to the treatment of data from legal persons, the GAC believes that such differentiation should be required for the many different reasons (as noted below) which benefit the public.

First, the publication of non-public domain name registration data concerning legal entities would increase the information available to those entities tasked with protecting the public. Given the prevalence of internet-based crimes, publishing the registration data of legal entities would aid law enforcement, consumer protection, and cybersecurity professionals’ ability to quickly and more effectively investigate illicit activities facilitated by the DNS, including efforts to combat cybercrime. In addition, publication permits law enforcement or National Computer Emergency Response Teams to 1) quickly identify the jurisdiction/ location of businesses that are a victim of cybercrime and 2) provide at scale, legal entities with notification and protective messaging in the event that their domains have been compromised.

Second, requiring registrars to publish the domain name registration data of legal entities would significantly reduce the number of requests for disclosure of domain name registration data and the challenges associated with obtaining responses to disclosure,⁷ because that data set would already be publicly available. Third, making non-personal data available to the public generally increases trust in the DNS by permitting transparency as to the ownership of domain names, including those domains that facilitate sensitive online communications and transactions.

Finally, the legal guidance received underscores the low risks associated with registration data from legal entities. To the extent that personal information is included in a legal entities’ registration data, it is likely to be “low sensitivity” because it relates to an employee’s work details rather than their private life.⁸ Moreover, if the proper safeguards are followed, the legal risks associated with such publication, even in the event of inadvertent mistakes, seem low.⁹

In **summary**, we maintain that a process of differentiation, by the Contracted Parties between data of legal persons and data of natural persons needs to be made mandatory. The Final Report does not sufficiently reflect the various interests at stake in the discussion on differentiation and the subsequent publication of non-protected information. The GAC believes that the public interest outweighs commercial concerns, particularly because the publicly available information would promote the stability, security and resilience of the DNS.

The following comments identify specific concerns with regard to the Final Recommendations.

⁵ See Executive Summary of the WHOIS Contact Data Availability and Registrant Classification Study (25 January 2021) at <https://www.icann.org/en/system/files/correspondence/chapin-to-botterman-25jan21-en.pdf>.

⁶ Ibid.

⁷ See Section 5.3.1 of the [Draft Report](#) of the RDS Review Team (31 August 2018) and [joint survey](#) from the Anti-Phishing and Messaging Malware and Mobile Anti-Abuse Working Groups (18 October 2018).

⁸ See 6 April 2021 [Bird & Bird Memorandum](#).

⁹ Ibid.

Recommendation #1 Fields to Facilitate Differentiation between Legal and Natural Person Registration Data

The GAC urged for the creation and use of data fields to flag legal registrants and the presence or absence of personal information in their data sets. Such flagging mechanisms would provide a necessary first step for differentiation. Recommendation 1 includes several obligations with regard to the creation of fields to facilitate differentiation between legal and natural person registration data and identify whether that registration data contains personal or non-personal data. In addition to creating these fields, there are further obligations:

- for ICANN to coordinate the technical community, for example the RDAP WG, to develop any necessary standards associated with such field(s);
- for the SSAD, consistent with the EPDP Phase 2 recommendations, to support the fields in order to facilitate integration between SSAD and the Contracted Parties' systems; and
- for the fields to support specific values related to the status of legal persons and the presence or absence of personal data.

The GAC especially values the precision of this Recommendation in specifying precisely what values should be included in these fields. The GAC though believes that Recommendation 1 would be more effective in creating the necessary infrastructure for differentiation if it:

1. required contracted parties to not just create but also to use these fields;
2. provided specific timelines for making these fields operable; and
3. ensured that the fields will operate within the current and contemplated systems for data collection and disclosure.

For clarity, the GAC thinks that requiring contracted parties to populate these fields for all future registrations, irrespective of whether the contracted parties elect to differentiate in their treatment of data from natural versus legal entities, is efficient and in the public interest because it would provide a basis to flag and identify data that may be the subject of future expedited SSAD requests or future legal obligations.¹⁰

The GAC also notes that a voluntary use of such a field is inconsistent with previous phases of the EPDP where measures such as redactions of data were applied to the whole system rather than relying on individual contracted party decisions.

Recommendation #2 Guidance for Contracted Parties who Choose to Differentiate

The EPDP team created the guidance for differentiation based upon the applicable principles of the GDPR and extensive legal advice. Notably, the legal advice identified very specific safeguards to mitigate the risk of wrongful disclosure and observed that in any event, the data involved was not as sensitive as other categories of personal information because it related to work, rather than private life. Finally, the legal advice observed that if the safeguards were followed, then even inadvertent disclosure of personal information would be unlikely to result in enforcement action. Because the guidance adopted the advised safeguards, the resulting liability risks are low, and discussed previously, the benefits to the public are high.

For the reasons identified above, the GAC believes that Recommendation should have required the contracted parties to differentiate between legal and natural entities, and accordingly should have also required contracted parties to apply the applicable guidance identified in Recommendation 2 and publish all non-personal data of legal

¹⁰ In this regard, the GAC welcomes the Final Report's encouragement to the GNSO to assess whether future policy work is necessary in light of legislative developments. For example, the EPDP noted the current discussions and expected adoption of the Revised Directive on Security of Network and Information Systems ("NIS2"). See "Proposal to the GNSO Council" on p.15 of the [EPDP Phase 2A Final Report](#).

entities in the publicly available data. The GAC also believes that the safeguards reflected in Recommendation 2 are more aptly referred to as “Best Practices.”

Recommendation #3 Codes of Conduct and Example Scenarios

The GAC welcomes the EPDP team’s Recommendation that the team guidance set forth in Recommendation 2 should be considered by any possible future work within ICANN by the relevant controllers and processors in relation to the development of a GDPR Code of Conduct. The GAC notes that stakeholders affected by such a Code should be given the opportunity to participate in developing the Code including potential requesters (and therefore potential processors) of domain name registration data.

The GAC also appreciates the guidance provided by the specific scenarios. The GAC believes that the logic and clarity of these three scenarios would be improved if they required publication or non-disclosure under the applicable scenarios. Each scenario sets forth specific conditions which logically mandate either publication or non-disclosure of domain name registration data and hence the use of the word “should” rather than “must” in these scenarios is misplaced.

Recommendation #4 Pseudonymized Email addresses

Regarding unique contacts and pseudonymized email addresses, the GAC welcomes steps to provide guidance on publishing an email address through the data protection method of using anonymizing techniques and notes the reduced levels of risk this provides to publication as highlighted in the legal memos received by the EPDP team.¹¹ Though the GAC acknowledges there are certain risks involved with publishing even pseudonymized information, GDPR Recital 28 highlights the use of pseudonymization as a method to reduce these risks to data subjects and help controllers and processors to meet their data-protection obligations. Moreover, pseudonymized emails are widely used by privacy/proxy services with little to no impact experienced by many data subjects. The GAC also notes the benefits that such publication of pseudonymized emails would provide, particularly with regard to facilitating quick and effective communications with domain name registrants. There have been reports that certain web forms have not been effective mechanisms to communicate with registrants.

¹¹ See 9 April 2021 Bird & Bird Memorandum on [Options for contact address masking](#), and 4 February 2020 Bird & Bird Memorandum on [Questions regarding a System for Standardized Access/Disclosure \("SSAD"\). Privacy/Proxy and Pseudonymized Emails](#).