ICANN | GAC

Governmental Advisory Committee

| | |
|---|---|
| **Status** | Final |
| **Distribution** | Public |
| **Date** | 5 May 2020 |

# Governmental Advisory Committee Comment on the Addendum to the Initial Report of Phase 2 of the EPDP on gTLD Registration Data

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

## Introduction

The GAC appreciates the efforts over the past 21 months and acknowledges the considerable time and commitment by the EPDP team and ICANN support staff to develop these complex and important policies in a timely manner. Nevertheless, the recently released Addendum to the Phase 2 Recommendations does not adequately address several crucial issues, including:

1. the treatment of domain name registration data from legal entities,
2. the accuracy of domain name registration data,
3. the display of data registered with privacy proxy service providers, and
4. the feasibility of unique contacts to have a uniform anonymized email address.

The GAC has issued advice and contributed input that highlights the importance of these issues.[1] The GAC would like to explain why these issues remain important and urges the EPDP team to either address these issues in its Final Report or at least recommend a clear and definite path to resolve these key issues.

[1] *See* GAC Input on EPDP Phase 1 Final Report at: https://gac.icann.org/reports/epdp-initial-report-gac-Input-21dec18.pdf, Joint GAC-ALAC Statement on EPDP at: https://gac.icann.org/publications/public/icann64-joint-gac-alac-statement-epdp-13mar19.pdf and GAC Advice in its Communiqués in San Juan (15 March 2018), Kobe (14 March 2019) and Montréal (6 November 2019).

## The Registration Data of Legal Entities Should Remain Public

As a starting point, as clearly explained by the European Data Protection Board (EDPB) in its letter to ICANN of 5 July 2018, the GDPR only applies to and protects the processing of personal data of natural persons.[2] Information concerning legal persons is not personal data under the GDPR if it does not allow the identification of individuals. Therefore, the contracted parties could make such data publicly available without triggering GDPR concerns. Nevertheless, Recommendation 17 of Phase 1 stated that Registrars and Registry Operators are *permitted* but not *obligated* to differentiate between registrations of legal and natural persons. This does not seem consistent with the objectives set out in the Temporary Specifications which "aim[] to ensure the continued availability of WHOIS to the greatest extent possible"[3] and highlighted the issue of "distinguishing between legal and natural persons to allow for public access to the Registration Data of legal persons, which are not in the remit of the GDPR" as an important issue for further community action. Further, the Charter for the EPDP also tasked the team with considering several aspects of this topic.[4] Results of ICANN research on the feasibility, costs, potential liability, and privacy risks of requiring such a distinction is expected this May. ICANN's legal advisor noted that the percentage of legal registrants is "substantial." A 2013 ICANN-commissioned study indicated that **legal entities comprised the highest percentage category of domain name registrants**.[5] This information is especially important in light of scams promising cures for COVID-19. One method for the public to assess the legitimacy of a website and law enforcement to find out what entities are behind it, is to consult the publicly available domain name registration information, which should include the data of legal entities.

In January 2019, the EPDP team also received legal guidance that noted while some legal entities' domain name registrations contain personal data (*e.g.*, JohnDoe@Acme.com), if the "*contact details are generic, such as info@company.com, then the registration data will not include personal data*" ("*non-personal registrants*"). The law firm observed that because "*non-personal registrants make up a substantial portion of registrants, one solution being discussed is to distinguish these registrants from those that provide personal data*. *Under this approach, registration details would be made publicly available by default for non-personal registrants.*" Noting the concern that individuals may wrongly designate themselves as legal entities, the law firm suggested several steps to reduce the risk of liability, such as:

1. developing language directed to registrants that "*is as clear as possible to help avoid mistakes*";
2. confirming the designation with registrants by "*asking them to re-certify that the contact details do not include personal data*";
3. verifying independently the designation through "*technical means*" (screening for personal information or requiring "*a corporate registration ID number*"); and

[2] The GDPR dos 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 (Recital (14) GDPR. "While the contact details of a legal person are outside the scope of the GDPR, the contact details concerning natural persons are within the scope of the GDPR, as well as any other information relating to an identified or identifiable natural person" (*See* EDPB letter to ICANN of 5 July 2018).

[3] *See ICANN Data Protection Privacy Issues*: https://www.icann.org/dataprotectionprivacy

[4] *See EPDP Team Charter*: https://gnso.icann.org/sites/default/files/file/field-file-attach/temp-spec-gtld-rd-epdp-19jul18-en.pdf (included directions for team to consider 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).

[5] *See WHOIS Registrant Identification Study*: https://gnso.icann.org/sites/default/files/filefield_39861/registrant-identification-summary-23may13-en.pdf: Based on our analysis of the WHOIS records retrieved from a random sample of 1,600 domains from the top five gTLDs,

- 39 percent (± 2.4 percent) appear to be registered by legal persons
- 33 percent (± 2.3 percent) appear to be registered by natural persons
- 20 percent (± 2.0 percent) were registered using a privacy or proxy service.
- We were unable to classify the remaining 8 percent (± 1.4 percent) using data available from WHOIS.

4. ensuring that "*data subjects clearly understand the consequences for them of the registrants' self-identification*."[6]

The clear implication of this legal advice as well as the EDPB guidance is that there is a variety of measures to ensure that registrants accurately designate themselves as legal entities. The fact that many ccTLDs (including those based in the EU) already make certain registrant data of legal entities publicly available demonstrates that such distinction is both legally permissible and feasible.[7]

Consequently, the GAC suggests that the EPDP reconsider its position. Instead of deferring this issue, the EPDP team could focus upon the legal guidance provided to develop reasonable policies to permit the information of legal entities to remain public. The time is now to implement policy that deals with this issue in a manner that promotes public safety and provides useful information to internet users seeking to navigate the internet safely and securely.

## Domain Name Registration Data Should be Accurate

The accuracy of domain name registration data is fundamental to both the GDPR and the goal of maintaining a secure and resilient DNS. The GDPR, as well as other data protection regimes and ICANN's Registrar Accreditation Agreement, require data accuracy and such accuracy is critical to ICANN's mandate of ensuring the security, stability, reliability, and resiliency of the DNS. As stated in the European Commission's letter to ICANN of 7 February 2018: "*[a]s stipulated by the EU data protection legal framework and in line with the obligations of contracted parties under their contracts with ICANN, personal data shall be accurate and kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay […]. To comply with the data quality principle, reasonable steps should be taken to ensure the accuracy of any personal data obtained.*"

The Charter for the EPDP tasked the team with assessing *"framework(s) for disclosure […] to address (i) issues involving abuse of domain name registrations, including but not limited to consumer protection, investigation of cybercrime, DNS abuse and intellectual property protection, (ii) addressing appropriate law enforcement needs . . . "* The effectiveness of Domain Name Registration data for these purposes (indeed for any purpose, including the ability of contracted parties to reach their customers) is of course contingent upon its accuracy. Moreover, the EPDP Phase 1 Final Report stated, "*the topic of accuracy as related to GDPR compliance is expected to be considered further . . .*" Hence, the GAC does not support the GNSO Council's guidance to defer the EPDP's consideration of data accuracy. The GAC further does not support the EPDP's preliminary conclusion not to consider this topic further. Conducting these discussions now would be the most efficient and logical course of action given the crucial role that data accuracy plays in preserving the operability and integrity of the DNS. The GAC therefore encourages the EPDP to reconsider its position in the light of the arguments provided above.

[6] The law firm explained that "*this means that the language provided to registrants should explain, separately from any detailed terms and conditions, that self-identifying as a non-personal registrant will result in registration data being made publicly available.*" *See Advice on liability in connection with a registrant's self-identification as a natural or non-natural person pursuant to the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")* from Bird & Bird.

[7] *See e.g.,* Belgium (.BE), European Union (.EU), Estonia (.EE), Finland (.FI), France (.FR), Norway (.NO), etc.

## Recommendations Related to the Handling of Data Protected by Privacy/Proxy Service Providers Should be Implemented Without Delay

The EPDP team has developed recommendations concerning the treatment of domain name registration data protected by privacy/proxy service providers but noted that its recommendation must not be implemented until related PPSAI policy is implemented.[8] At the same time, the ICANN Org, with the support of the ICANN Board, has stalled implementation of the PPSAI recommendations.[9] Hence, there is a standoff.

The GAC has emphasized the importance of implementation of the Privacy Proxy Services Accreditation Issues (PPSAI) policy "*given the impact of unregulated and unaccountable privacy proxy services on the stability and security of the DNS*."[10] While Privacy Proxy Services may serve legitimate purposes,[11] a U.K. study noted that a "*significant percentage of the domain names used to conduct illegal or harmful Internet activities are registered via privacy or proxy services to obscure the perpetrator's identity.*"[12]

At the least, there should not be unnecessary delays to implementing policies that support clear labeling of when privacy proxy services are in use and eliminate barriers to legitimately accessing such data. We recommend that the EPDP ask the Board to eliminate the current timing conundrum by permitting the PPSAI implementation to resume and thereby clearing the path to implementation of the EPDP team's related privacy proxy recommendations.

## Recommendation Concerning Feasibility of Unique Contacts to have a Uniform Anonymized Email Address

The EPDP Team received legal guidance noting that the publication of uniform masked email addresses results in the publication of personal data. Based on that legal advice, the EDPD concluded that "*wide publication of uniform masked email addresses is not currently feasible under the GDPR*." The GAC wishes to note that the legal advice actually rightly pointed out that pseudonymization is "*a useful Privacy Enhancing Technique/privacy by design measure*."[13]

Therefore, the GAC considers that the publication of uniform masked email addresses is a potentially useful privacy enhancing solution (even if the data would still be considered as personal data), which should be further considered. Advice/guidance on this particular matter could also be sought from the EDPB. The Belgian Data Protection Authority, in its letter to ICANN of 4 December 2019, explicitly encouraged ICANN to take note of the draft Guidelines recently issued on 10 November 2019 by the EDPB on Data Protection by Design and by Default, which recognize that controllers could implement technical measures such as pseudonymization under appropriate circumstances.[14]

---

[8] *See Addendum to Initial Report of Phase 2 EPDP on gTLD Registration Data*: https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-addendum-26mar20-en.pdf.

[9] *See* ICANN org letter to the GNSO Council on 5 September 2019: https://www.icann.org/en/system/files/correspondence/namazi-to-drazek-et-al-05sep19-en.pdf and ICANN Board response to the GAC Montréal Communiqué: https://www.icann.org/en/system/files/files/resolutions-montreal66-gac-advice-scorecard-26jan20-en.pdf

[10] *See Section 6. Importance of Accreditation of Privacy/Proxy Services and Validation of Registration Data Using Them*: *https://gac.icann.org/file-asset/public/gac-comments-rds-whois2-review-final-report-23dec19.pdf* .

[11] For example, to protect "[o]rganizations within a religious, political or ethnic minority, or sharing controversial moral or sexual information." *See* https://whois.icann.org/en/privacy-and-proxy-services

[12] *See* https://www.icann.org/public-comments/whois-pp-abuse-study-2013-09-24-en

[13] *See* Bird& Bird Memo, "*Batch 2 of GDPR questions regarding a System for Standardized Access/Disclosure ("SSAD"), Privacy/Proxy and Pseudonymized Emails*" (February 4, 2020).

[14] *See* Belgian DPA letter to ICANN (December 4, 2019): https://www.icann.org/en/system/files/correspondence/stevens-to-_marby-04dec19-en.pdf citing https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf