ICANN | GAC

Governmental Advisory Committee

Status	Final
Distribution	Public
Date	24 August 2020

Governmental Advisory Committee Minority Statement on the Final Report of Phase 2 of the EPDP on gTLD Registration Data

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

Introduction

The GAC sincerely appreciates the efforts of the entire EPDP team, its dedicated Chairs, and ICANN support staff over the past 23 months and acknowledges the considerable time and commitment expended to develop these complex and important policy recommendations regarding access and disclosure of domain name registration data (formerly known as WHOIS). ICANN's Bylaws recognize that WHOIS data is necessary for "the legitimate needs of law enforcement" and for "promoting consumer trust."[1] The GAC has also repeatedly recognized these important purposes, noting that WHOIS data is used for a number of legitimate activities including: assisting law enforcement authorities in investigations; assisting businesses in combatting fraud and the misuse of intellectual property, safeguarding the interests of the public; and contributing to user confidence in the Internet as a reliable means of information and communication.[2]

Recognizing these crucial purposes, ICANN's Temporary Specification for gTLD Registration Data aimed to "ensure the continued availability of WHOIS to the greatest extent possible while maintaining the security and stability of the Internet's system of unique identifiers."[3] The Final Recommendations contain useful elements that are an improvement over the current Temporary Specification governing access to Domain Name Registration data. Nevertheless, the GAC must withhold support for certain Recommendations which in their current form do not strike the appropriate balance between protecting the rights of those providing data to registries and registrars, and protecting the public from harms associated with bad actors seeking to exploit the domain name system.[4] In

[1] ICANN Bylaws, Registration Directory Services Review, §4.6(e).
[2] *See e.g.,* GAC Abu Dhabi Communiqué, Section VII.3 p.11 and 2007 GAC Principles Regarding WHOIS Services.
[3] *See ICANN Data Protection/Privacy Issues* webpage: https://www.icann.org/dataprotectionprivacy
[4] The GAC (along with other stakeholder groups) objected to the following Recommendations: 5 - Response Requirements; 6 - Priority Levels; 8 - Contracted Party Authorization; 14 - Financial Sustainability; 18 - Review of Implementation of Policy

this regard, the GAC highlights that the domain name system is a global public resource that must serve the needs of all its users, including consumers, businesses, registrants, and governments.

In this Minority Statement, the GAC provides input on its public policy concerns regarding the ways that the Final Recommendations:

1) currently conclude with a fragmented rather than centralized disclosure system,
2) do not currently contain enforceable standards to review disclosure decisions,
3) do not sufficiently address consumer protection and consumer trust concerns;
4) do not currently contain reliable mechanisms for the System for Standardized Access/Disclosure (SSAD) to evolve in response to increased legal clarity; and
5) may impose financial conditions that risk an SSAD that calls for disproportionate costs for its users including those that detect and act on cyber security threats.

In addition, as highlighted in our GAC Comment on the Addendum to the Phase 2 EPDP Initial Report, the Final Report does not currently address certain key issues (most notably data accuracy, the masking of data from legal entities not protected under the GDPR, and the use of anonymised emails). The model would also benefit from further clarifying the status and role of each of the data controllers and processors. The GAC requests the GNSO Council to ensure that these important issues are promptly addressed in this EPDP as a next and final Phase 3.

Fragmented Disclosure System

Although the Final Recommendations provide a centralized system to submit requests, it lacks such centralization with regard to disclosing data. The current recommendations create a fragmented system that could lead to inadequate access to registration data and may delay law enforcement, intellectual property, and cyber security investigations. The GAC cautioned against creating "a fragmented system for providing access consisting of potentially thousands of distinct policies depending upon the registrar involved" noting that the "lack of consistent policies to access non-public information causes delays" which may impede investigations and may permit potentially injurious conduct to continue to harm the public.[5] In the GAC's view, this result is not consistent with the GAC's expectation for "a stable, predictable, and workable access mechanisms for non-public WHOIS information."[6] Notably, the Belgian Data Protection Authority acknowledged the potential benefits of a centralized model and explicitly recognized that the GDPR does not prohibit the automation of various functions in a disclosure model. [7]

Nevertheless, the disclosure recommendations:

- rely almost entirely upon the individual assessments and decisions of the more than 2000 ICANN accredited registrars;[8]
- insufficiently address the role of automation and provide for only two categories of automated responses;[9] and

Recommendations Concerning SSAD using a GNSO Standing Committee. *See* Consensus Designations at Annex D to EPDP Phase 2 Final Report.

[5] GAC Barcelona Communiqué (Section IV.2 Other Issues – in reference to Temporary Specification, p.6).

[6] GAC Panama Communiqué, see Rationale of GAC Consensus Advice to ICANN Board (Section V.1, p. 7)

[7] https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority

[8] Recommendation (Rec.) 8

[9] Rec. 9.41 and 9.42

- insufficiently address reliable mechanisms to expand the categories of requests appropriate for automated disclosures in response to future legal guidance or even changes in applicable privacy law.[10]

The currently fragmented system for disclosures combined with a relatively uncertain framework to consider and recommend future centralization, may impede the stability and predictability of the SSAD.

Lack of Enforceable Standards to Review Disclosure Decisions

The GAC acknowledges that under applicable data protection rules, including the GDPR, contracted Parties will likely remain responsible for the decision whether to disclose domain name registration data, and may face certain liability risks related to that decision. The GAC understands that contracted Parties have therefore sought to maintain control over the decision whether to disclose domain name registration data. The GAC notes, however, that those decentralized decisions whether to disclose data are largely exempt from challenge and enforcement action, notably via ICANN Compliance.[11]

Registration data is important for the security and stability of the DNS and there is a real concern that contracted parties may inadvertently or purposely not properly weigh the public interest for the requestor to obtain such data. ICANN's CEO recently conveyed this very concern to the European Data Protection Board, pointing out that "[d]ue to a lack of legal certainty, registrars, as controllers, are likely to evaluate privacy and data protection in absolute terms, without considering other rights and legitimate interests, to avoid possible regulatory sanctions or a judgment against them."[12] Denials of legitimate requests for access to domain name registration data have real consequences. The GAC noted in its Barcelona Communiqué that surveys and studies indicated that the implementation of the Temporary Specification in response to the GDPR had a negative effect on law enforcement and cyber-security professionals' ability to investigate and mitigate crime using information that was once publicly available in the WHOIS system.[13]

The current recommendations do not provide a mechanism for the review of disclosure decisions. The proposed system does not include at this stage a role for ICANN Compliance to review substantive challenges to disclosure decisions. Instead, ICANN Compliance plays a limited role to review complaints regarding failure to abide by the *procedural* requirements or systemic abuse.[14] As a result, the SSAD Recommendations promote a system that risks encouraging a conservative approach to disclosure decisions to reduce liability risks and does not adequately provide for a robust review of disclosure decisions within ICANN's enforcement mechanisms. Granting contracted

[10] Rec. 8.17 and 18

[11] Rec. 8, Rec. 5.3 and 5.4. ***See also*** May 22, 2020 letter from ICANN CEO to European Data Protection Board, https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf.

[12] *See* May 22, 2020 letter from ICANN CEO to European Data Protection Board, https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-22may20-en.pdf ("The uncertainty about how to balance legitimate interests in access to data with the interests of the data subject leaves much to the subjective judgment and discretion of the registrar, as the controller receiving an access request, on whether to grant or refuse access to the non-public gTLD registration data.").

[13] *See* also section 5.2.1 in the Final Report of the Registration Directory Services 2 Review Team (3 September 2019) and joint survey from Anti-Phishing and Messaging Malware and Mobile Anti-Abuse Working Groups (18 October 2018).

[14] Rec. 5.3-5.5. Moreover, the implementation guidance does not even require contracted parties to adjust their analysis regarding disclosure decisions "to address applicable case law interpreting GDPR, guidelines issued by the EDPB or revisions to GDPR or other applicable privacy laws that may occur in the future." *See* Rec. 8.17. The Guidance uses the word "SHOULD" rather than "MUST" and hence is not enforceable (see 19 December 2019 email to the EPDP Team from ICANN representatives discussing enforceability of "SHOULD" and "MUST").

parties full discretion in reviewing disclosure requests may undermine the obligation to ensure the continued viability of domain registration data as a tool to vindicate the rights and interests of the public, agencies tasked with protecting the public, and commercial and intellectual property constituencies. The GAC believes that this current proposed approach may impede the stability and predictability of the SSAD.

Prioritize Requests that Raise Consumer Protection Concerns

The GAC is concerned about the inadequate prioritization for consumer protection requests (raising issues related to phishing, malware and fraud)[15] which raise important public concerns that often require immediate action.[16] The current recommendations place consumer protection requests in the lowest of three priority levels. Moreover, the corresponding service level requirements that govern response times to Priority 3 requests provide for lengthy response times: within five-days during the first six months of implementation and then the response time doubles to 10-days thereafter.[17] This lack of prioritization and long response times could lead to significant harms that frauds and cyber-attacks can quickly cause. The GAC would recommend designating consumer protection requests to Priority 2.

Even if one accepted the current Priority 3 designation, the suggested operation of Recommendation 6 causes concern. The GAC welcomes the fact that the Recommendation requires the requestor's ability to flag requests that raise consumer protection concerns ("Requestors MUST have the ability to indicate that the disclosure request concerns a consumer protection issue. . ."). [18] However, the Recommendation does not include a similarly enforceable requirement for the contracted parties to prioritize the consumer protection related requests over others at the same priority level. Rather than using the word "MUST", the Recommendations state that contracted parties "SHOULD" prioritize these requests.[19] However, ICANN Compliance expressly informed the EPDP team that the use of the word "SHOULD" does not create an enforceable obligation[20]. Hence, this Recommendation is internally inconsistent in that it requires the ability to identify consumer protection issues but fails to require the contracted parties to act on this designation. EPDP team discussions on this issue reflected that this goal could be accomplished simply by using a sorting mechanism. Consumer protection related requests raise issues that affect the overall security of the DNS and hence the GAC recommends making this prioritization mandatory rather than permissive.

Reliable Mechanisms for SSAD to Improve

The SSAD, like any new system, would face challenges in its implementation and application and would need to respond in a timely manner. Mechanisms may require adjustment, demands from data requesters may ebb and flow, and new and unanticipated uses for the data may emerge, especially in the realm of cybersecurity. As a result, the potential for the SSAD to improve over time, adjust to new obstacles, and respond to new legal guidance is crucial.

---

15 The GAC also notes that the proposed definition of consumer protection requests seems unduly restrictive and requests that the proposed parenthetical be interpreted as illustrative rather than comprehensive.

16 *See* SSAC Comment on the Initial Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process *(*SAC 111) at pp. 9-10.

17 Rec. 6.2 and Rec. 10.4 and 10.11.

18 Rec. 6.2.

19 Rec. 6.2

20 *See footnote 14 above*

On the topic of automation, the Final Recommendation on Automated Disclosure Decisions requires automation for any categories of requests for which automation is determined "to be technically and commercially feasible and legally permissible."[21] Although the EPDP team considered a range of use cases for automation, it was able to agree upon only two to include in the Final Report.[22] Some stakeholder groups, including the GAC, had anticipated an SSAD that included more automation and centralization because, as recognized by representatives from the Belgian Data Protection Authority, a centralized model "seems to be a better, 'common sense' option in terms of security and for data subjects."[23] Nevertheless, the GAC and some other stakeholder groups agreed to this "hybrid" rather than centralized model so long as the final recommendations included a mechanism that provided the flexibility for the SSAD to evolve and change without having to engage in a new PDP effort for each adjustment that was consistent with the Final Report.

Recommendation 18 creates a Standing Committee to be composed of representatives of all the stakeholder groups that participated in the EPDP to grapple with these decisions. However, the GAC believes that Recommendation 18, which provides for review of implementation of the policy recommendations, does not seem to meet the goal of providing for an efficient mechanism for the SSAD to evolve. In particular, there is insufficient clarity regarding whether new use cases for automation comprise new policy or implementation of existing policy. The GAC observes that if every new use case is deemed new policy requiring a new PDP, it is not clear at this stage that the SSAD would effectively evolve and in particular move towards more centralization. Under this scenario, the SSAD could remain fragmented with all the concerns that go along with such fragmentation. Hence, the GAC requests that the GNSO ensure that the EPDP recommendations provide enough certainty in this regard, allowing automation of further elements whenever the "technically and commercially feasible and legally permissible" test is met.

Other requirements for even proposing a change include not only consensus by the Standing Committee but also approval by the contracted parties. The recommendations would then need approval by the GNSO Council (which lacks representation from the Advisory Committees) before they could become adopted. This "evolution" process could become complex and lengthy and is not suited to dealing with implementation issues that require quick and decisive action.

Financial Sustainability

The Recommendations could create a system that is too expensive for the users for which it is intended, including SSAD users that investigate and combat cyber security threats. The Recommendations state that "Data subjects MUST NOT bear the costs for having data disclosed to third parties; Requestors of the SSAD data should primarily bear the costs of maintaining this system."[24] While the GAC recognizes the appeal of not charging registrants when others wish to access their data, the GAC also notes that registrants assume the costs of domain registration services as a whole when they register a domain name. As the SSAC recently noted:

> Such costs should include disclosures to third parties with rights to obtain redacted data in order to fulfill legitimate security, stability and resiliency (SSR) activities and potentially other legal activities (e.g., rights protections) that fall outside SSAC's scope of activities. The overall SSR of the DNS requires the ability to access such data to

[21] Rec. 9.3.

[22] *See* Rec. 9.41 and 9.42 (9.43 and 9.44 relate to the narrow categories of requests only for the city field or records that do not contain personal data).

[23] https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority

[24] Rec. 14.2.

> enable communications with the owners of compromised resources, as well as the determination of fraudulent and malicious activities that enable the suspension of registration services obtained by criminal actors.[25]

Additionally, the GAC notes that much of the expense of the SSAD relates to its pervasive use of manual (versus automated) processing, an approach with inherently limited scalability and intrinsically high cost. The financial sustainability of SSAD cannot be separated from its reliance on manual processing. Reducing manual processing to the extent possible will contribute to the financial sustainability of the SSAD.[26] Taken as a whole, the Recommendations relating to financing the SSAD could be difficult to implement and raise more questions than they answer, notably, 1) to what extent may ICANN help subsidize the system; 2) to what extent may registrars pass on the costs of the SSAD to their customers; 3) what role would requestors have in setting and approving fees for the system, etc. The GAC believes that "a formal assessment of user impacts and the security and stability impacts" is advisable.[27]

Issues not Addressed in EPDP Phase 2 Final Report

Data Accuracy

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, [and] (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 contingent upon the data's accuracy. Moreover, the accuracy of the registration data is an essential requirement of GDPR and 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 is concerned about the absence of any Recommendations on this vital topic in the Final Report.

As the GAC has previously emphasized:

> 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.*"[28]

---

[25] SAC 111.

[26] Another topic that would encourage less manual processing would be to explore what legally permissible mechanisms contracted parties could implement to permit data subjects to provide either freely given consent or objection to disclosure of their data at the time of domain name registration. This would facilitate maintenance of databases of protected versus non-protected information, opening non-protected databases to lower-cost automated processing.

[27] *See* SAC 111.

[28] GAC Comment on Addendum to Phase 2.

Consistent with the GDPR, it is essential that data accuracy and quality is ensured in relation "to the purpose for which they [the data] are processed."[29] Disclosure of inaccurate data would defeat the purpose of SSAD and would risk violating data protection rules. Accuracy is a core data protection principle in most data protection laws across the globe. In particular, the accuracy requirement is mandated by Article 5 of the GDPR.

The effectiveness of the current contract requirements in place to promote WHOIS accuracy seems to be uncertain. Recent review team reports raise questions about the effectiveness of the verification procedures, such as the RDS Review Team and the CCT Review Team reports, both of which the GAC endorsed.[30] Moreover, since 2014, WHOIS accuracy comprises the single largest complaint category among complaints reported to ICANN Compliance regarding Registrars.[31]

The GAC therefore calls on the GNSO Council to request the current EPDP with addressing this issue so that data accuracy is included as an integral component of the SSAD.

Natural/Legal

In the GAC ICANN68 Communiqué of 27 June 2020, the GAC had sought an update from the GNSO, as soon as possible, on its progress towards developing a specific plan to continue the policy development process to address the unresolved issue related to distinguishing between natural and legal entities. This issue is important because personal data protection regulations, including the GDPR, only apply to and protect the processing of personal data of natural persons.[32] Information concerning legal persons is not considered personal data under personal data protection regulations, including the GDPR, if it does not allow the identification of individuals. Therefore, the contracted parties could make such data publicly available without triggering data protection concerns. Nevertheless, as reflected in the Final Report, Registrars and Registry Operators continue to be *permitted* but not *obligated* to differentiate between registrations of legal and natural persons.[33] This practice does not "ensure the continued availability of WHOIS to the greatest extent possible"[34] and the Final Report's lack of recommended procedures applicable to this distinction fails to meet the express directive of the Phase 1 EPDP team and EPDP team Charter.[35]

---

[29] *See* GDPR Art. 5(1)(d). *See also* United Kingdom's Information Commission Office's Guide to the GDPR, Guidance For Organizations, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/

[30] *See, e.g.*, Registration Directory Services WHOIS 2 Review Final Report at pp. 49-61 (noting that WHOIS inaccuracy rates continue to be high and are likely under-reported)**;** Governmental Advisory Committee Comments on the Final Report of the RDS-WHOIS2 Review Team, dated 23 December 2019 at pp. 5-7; Competition, Consumer Trust and Consumer Choice Review Team Final Report at pp. 103-06. *See also* WHOIS Review Team Report (11 May 2012) at pp. 11-13 ("low level of accurate WHOIS data is unacceptable, and decreases consumer trust in WHOIS, in the industry which ICANN provides rules for and coordinates, and therefore in ICANN itself").

[31] *See* ICANN Contract Compliance Annual Reports, Report Details regarding Registrars, 2014-2019, https://features.icann.org/compliance/dashboard/report-list.

[32] 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).

[33] *See* Section 2.3 of the EPDP Phase 2 Final Report, Priority 1 and Priority 2 Topics.

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

[35] *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).

The effect of masking data that is legally permitted to remain available to the public is significant because of the large number of domains registered to legal entities. A 2013 ICANN-commissioned study indicated that **legal entities comprised the highest percentage category of domain name registrants**.[36] One method for the public to assess the legitimacy of a website and for law enforcement authorities 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.

Significantly, the EPDP team received legal guidance that suggested several steps to reduce the risk of liability.[37] The implication of this guidance is that there could be a variety of measures to ensure that registrants accurately designate themselves as legal entities. It is to be noted that certain ccTLDs (including EU-based ccTLDs) already make certain registrant data of legal entities publicly available, demonstrating that such distinction is both legally permissible and feasible.[38]

Distinguishing the treatment of the data from legal versus natural persons is also closely related to the matter of automated processing. As noted above, legal persons are not protected by the GDPR. Thus, distinguishing legal from natural persons during the registration process could include assigning legal persons into the category of persons whose data should be automatically processed.[39]

The GAC believes that resolving the legal versus natural issue is critical for the entire SSAD model to meet its purpose and, at the same time, be compliant with applicable data protection laws. The GAC therefore requests the GNSO Council to make every practicable effort to address this issue. In that regard, the GAC reiterates its request that the EPDP team focus upon the legal guidance provided to develop reasonable policies to permit the information of legal entities to remain public.

Anonymized Email Address

The use of anonymized emails may be a solution to protect the registrant's identity while serving some of the legitimate domain name registration data access seekers' purposes. The Final Report lists among the Priority 2 items the "feasibility of unique contacts to have a uniform anonymized email address."[40] The EPDP team received legal guidance that anonymization as well as pseudonymization is "a useful Privacy Enhancing Technique/privacy by design measure."[41] As recognised by the same legal guidance, the GAC would like to note that anonymized

---

[36] *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.

[37] *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 (advised methods included developing clear notification language so that registrants avoid mistakes; ensuring that registrants understand the consequences of registering as a legal entity; and verifying that the contact information does not contain personal data).

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

[39] As a safeguard, persons with heightened legal protections could be assigned to non-automated query groups. This could include legal persons protected by national law (such as banking secrecy laws), natural persons with specific legal protections such as court protective orders, a data subject's vulnerable status (e.g., children, asylum seekers, other protected classes), and entire national populations in jurisdictions affording an affirmative right to personal privacy by default.

[40] Phase 2 EPDP Final Report at p. 3.

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

information falls outside the scope of the GDPR.[42] While the GAC acknowledges the possibility that a link could be created between the anonymous information and the personal data, it agrees with the legal advice that anonymization is a useful privacy enhancing technique and, as such, it should be further examined.

In light of the above, the GAC considers that further feasibility analysis is needed to better understand the benefits and risks of this option, rather than dismissing it without further examination.

Controllership

The possible joint controllership between the contracted parties and ICANN org is mentioned in the Final Report. Yet the GAC would expect more clarity on the status and role of each of the data controllers and processors in the SSAD model. In particular, having concrete data processing agreements in place would demonstrate more clearly how responsibility would be distributed between the contracted parties and ICANN org for the different data processing operations. The GAC would call on the GNSO Council to ask the EPDP to further address this issue.

Conclusion

The GAC applauds the good faith efforts of the stakeholders, staff and EPDP Chairs participating in Phase 2 of the EPDP for their sustained dedication to engaging on these important public policy matters. There are many commendable aspects of the Final Report. However, the GAC is of the view that certain key recommendations and unaddressed topics require further work and that, consequently, the GNSO Council should request the EPDP to finalize work on them consistent with the points raised in this Minority Statement. The GAC looks forward to continued engagement with our colleagues on these important issues.

[42] *See* Recital 26 to the GDPR.