

# ICANN | GAC

Governmental Advisory Committee

<b>Status</b>	Final
<b>Distribution</b>	Public
<b>Date</b>	21 November 2022

---

## Governmental Advisory Committee Comments on the Draft Registration Data Consensus Policy for gTLDs (EPDP Phase 1 Implementation)

---

### Table of Contents

<b>1. Summary of GAC Comment</b>	<b>1</b>
<b>2. Specific GAC Comments on Draft Registration Data Consensus Policy</b>	<b>3</b>
Section 2. Scope	3
Section 3. Definitions and Interpretation	3
Section 5. Data Protection Agreement	3
Section 6. Collection of Registration Data	4
Section 7. Transfer of Registration Data from Registrar to Registry Operator	5
Section 9. Publication of Domain Name Registration Data	5
Overlap of Section 9. Publication of Domain Name Registration Data & Section 10. Disclosure Requests	6
Section 10. Disclosure Requests	6
Section 12. Retention of Registration Data	7
<b>3. Specific GAC Comments on Implementation of EPDP Phase 1 Recommendation 27: Changes to existing policies and procedures</b>	<b>7</b>
Thick WHOIS Transition Policy for .COM, .NET and. JOBS	7

### **1. Summary of GAC Comment**

The GAC welcomes the implementation of the EPDP Team Phase 1 final recommendations and appreciates the efforts of the team members. The GAC highlights several public policy concerns with the proposed implementation including issues related to:

1. the definition and proposed timelines to respond to urgent requests;
2. the collection and publication of reseller data;
3. the collection/publication of registration information related to legal entities; and
4. the inclusion of qualifiers related to “commercial feasibility” in connection with redacted data.

The GAC also notes:

- There are several instances in which the proposed implementation would benefit from increased clarity or further explanation (for example, the obligation to enter into data protection agreements). Clear standards are particularly important both for proper implementation and enforcement of the consensus policies.
- It is also important to understand the reasoning behind certain conclusions, particularly with regard to those policies (such as the “thick Whois Policy”) that are deemed “superseded” by the Phase 1 implementation.
- Once these policies are implemented, the GAC encourages ICANN Compliance to assess whether Registrars are providing links to how to make a disclosure request so that those wanting to make a request are able to do so.

#### Other Big Picture Concerns: Lack of Clear Standards

The GAC appreciates the importance of designing a policy that is able to respond to pending and future legislative and regulatory developments. However, the GAC notes that some elements of the policy need to be reviewed with the objective of providing legal certainty and clarity around implementation and enforcement. In their current formulation, some aspects of the policy do not provide sufficient clarity or the conditions for a homogeneous application across the gTLDs. As commented in the relevant sections, this refers in particular to the obligation concerning data protection agreements and the identification (apparently on a case by case basis) of applicable legal bases. In particular, the discretion left to registrars to redact data based on commercial reasons or technical feasibility raises concerns.

#### Other Big Picture Concerns: Implementation of a Partial System Resulting in a Policy Gap

The GAC observes that the timelines for implementation of the Phase 1 recommendations were initially contemplated as occurring reasonably close in time to implementation of the subsequent Phase 2 and Phase 2A recommendations. That timing no longer appears likely and the GAC registers its concern that only part of the contemplated system for domain name registration data access and disclosure is scheduled for implementation. For instance, the proposed Draft Registration Data Consensus Policy does not take into account EPDP Phase 2 and in particular the approved EPDP Phase 2A Recommendations, which risks implementing a policy that will soon be overtaken by implementation of subsequent closely-related policies. Further, the EPDP Phase 2A recommendations require a functionality to distinguish registrants that are natural persons from those that are legal persons, even if the actual use of such functionality by the contracted parties remains voluntary. This functionality is not reflected in the proposed registration data policy. Rather, the Phase 1 implementation makes it optional to collect the data field pertaining to “registrant organisation”. Notably, the GAC has, on multiple occasions<sup>1</sup> stressed that legal entities’ registration data, which are not personal data (such as registrant organisation) are not covered by data protection rules and hence should be made public.

---

<sup>1</sup> See [GAC San Juan Communiqué](#) (15 March 2018) section V.1.a.iv p.8; [GAC Input on the Initial Report of the EPDP on gTLD Registration Data](#) (21 December 2019) section 5 p.7; [GAC Input on the Draft Final Report of the EPDP on gTLD Registration Data](#) (20 February 2019); [GAC/ALAC Joint Statement on EPDP](#) (13 March 2019); [GAC Minority Statement on EPDP Phase 2 Final Report](#) (24 August 2020), pp.7-8; [GAC ICANN70 Communiqué](#) (25 March 2021) section IV.5 p.7; [GAC Minority Statement on the Final Report of Phase 2A](#) (10 September 2021); and [GAC Response to Board Clarifying Questions on GAC ICANN70 Communiqué – WHOIS/Data Protection](#) (6 October 2021).

## 2. Specific GAC Comments on Draft Registration Data Consensus Policy

### Section 2. Scope

The GAC notes that Section 2.2 of the Draft Policy stipulates that *“Registrar Operator’s and Registrar’s Processing of Personal Data contained in Registration Data for purposes other than the purposes identified in the Data Protection Agreement required by Section 5 is beyond the scope of this Policy”*. The GAC recommends clarifying this language as it is unclear what “other purposes” includes. This is especially relevant given that Data Protection Agreements in Section 5 are made conditional on an assessment by contracted parties and the lack of a common model for data processing agreements makes it unclear what purposes could be covered therein.

### Section 3. Definitions and Interpretation

The GAC acknowledges the role of the GDPR in serving as a catalyst for this policy and notes that the precise wording of these definitions has no bearing on parties’ obligations to comply with applicable law. Nevertheless, the GAC recommends that in some circumstances greater specificity could be useful, including on “consent” (the GDPR requires the provision of consent for each purpose.) and “personal data,” which would benefit from greater clarity around the meaning of an identifiable natural person. Further, the GAC recommends the addition of text making clear that no costs will be borne by those willing to access “published” data. Finally, while the GAC is cognizant of maintaining a narrowly tailored set of circumstances warranting “urgent requests for lawful disclosure,” to ensure contracted parties are able to respond efficiently to these requests, the GAC recommends that this category of urgent requests include “imminent or ongoing serious cybersecurity incidents” (such as those deriving from large scale ransomware, malware or botnet campaigns, which may for example affect consumer protection and would require an immediate need for disclosure) regardless of whether the target is critical infrastructure.

### Section 5. Data Protection Agreement

Section 5 stipulates that *“Data Protection Agreement ICANN, gTLD Registry Operators, and accredited Registrars MUST enter into required data protection agreements with each other and with relevant third party providers contemplated under this Policy where applicable law requires.”*

The GAC recommends review of this provision to clarify the obligation for the cited parties to enter into a data protection agreement. First, if there are legal requirements, then the relevant laws establish the obligation regardless of these policies. Second, the policy implementation appears to be internally inconsistent because it both obliges the parties to enter into DPAs but then qualifies this obligation by indicating that it is subject to any ‘applicable law.’ This makes it unclear whether there is truly an obligation or not. Moreover, it is unclear how operators would assess which laws establish such a requirement. This risks making uniform implementation inside the same gTLD difficult. The GAC would support making the Data Processing Agreement unequivocally mandatory by deleting the reference “where applicable law requires.” The GAC notes the importance of clearly defined roles and responsibilities for the processing of the data in the Registrar Agreements. This is also supported by the current temporary specifications, which include the following provision: *“Registry Operator MUST include Processing provisions in its Registry-Registrar Agreement with Registrar concerning the handling of Personal Data in a manner that complies with applicable requirements of Article 28 of the GDPR”*.

## Section 6. Collection of Registration Data

6.3. The GAC finds this section unclear as it could imply that under certain circumstances the contact details of the technical contact may replace the contact details of the registrant. The present data policy should ensure that the contact details of both the registrant and the technical contact are collected.

*“6.4 Registrar MAY generate the Reseller data element value. “*

The GAC observes that the domain name industry has evolved considerably since ICANN’s inception, and today includes roles and entities which may not have existed in previous RDDS systems; similarly, new entities may be created tomorrow which have yet to be conceived of today. In recognition of this, the GAC supports the inclusion of corporate entities inherent to the registrar’s distribution channel (such as the RDAP Response Profile entity 2.5 enumerating the “reseller” role) as it is the purpose of the RDDS system to enumerate roles and responsibilities relevant to domain name registrations; such entities should be included in an RDAP response, when they exist. This would also prove as a benefit in highlighting the best point of contact to deal with notifications of abuse or compromise to the party with the ability to act the quickest or most appropriately. To that end, the GAC suggests the following text:

*6.4 Registrar SHOULD generate the Reseller data element value, for the Reseller with a direct relationship with the Registrant.*

Further, the GAC views the current definition of “Reseller” within the 2013 Registrar Accreditation Agreement (RAA)<sup>2</sup> as potentially inclusive of privacy and/or proxy services offered by entities within the registrar’s distribution channel. The GAC seeks clarification as to which entities SHOULD or SHOULD NOT be considered “Resellers” within the Consensus Policy; to the extent entities exist within the registrar distribution channels which were assumed by the authors of the Consensus Policy to *not* fall within the Reseller data element, the GAC would appreciate explicit clarification. In such cases, the GAC would benefit from further clarification as to which data elements SHOULD be used for each category of entities existing in registrar distribution channels. If data elements do not currently exist for such entities, the GAC would view it as constructive to create and incorporate within the Consensus Policy such elements.

6.5 – 6.6: *“If provided by the Registered Name Holder, Registrar MUST collect the following data element values”.*

The GAC acknowledges that this wording stems from Recommendation 12 of EPDP Phase 1, however the GAC reiterates that these data elements may change as a result of pending policy recommendations, particularly the approved Phase 2A recommendations. EPDP Phase 2A has required the functionality of distinguishing between legal and natural persons and the GAC believes that such distinction has not been taken into account in the present Draft Policy. In particular, data such as ‘the registrant organisation’, though not essential for registrants who are natural persons, should nevertheless be collected when the registrant is a legal person. This information can thus be optional for natural persons but should be mandatory for legal persons. As the GAC has stressed on multiple occasions, personal data protection regulations, including the GDPR, apply to the processing of personal data of natural persons and not legal persons. Therefore, the contracted parties should collect and make data of legal persons publicly available. Additional safeguards may be considered for the case where the email address of a legal person contains personal data, in which case a functional email address can be published instead.

---

<sup>2</sup>*“a person or entity that participates in Registrar’s distribution channel for domain name registrations (a) pursuant to an agreement, arrangement or understanding with Registrar or (b) with Registrar’s actual knowledge, provides some or all Registrar Services, including collecting registration data about Registered Name Holders, submitting that data to Registrar, or facilitating the entry of the registration agreement between the Registrar and the Registered Name Holder”*

## Section 7. Transfer of Registration Data from Registrar to Registry Operator

7.3. *“Registrar MUST transfer the following data elements to Registry Operator provided an appropriate legal basis exists and data processing agreement is in place.”*

As already stressed in previous sections, the lack of clarity regarding the obligation to have a Data Processing Agreement does not help implementation and enforcement of this policy. The GAC recommends that the data policy be clear as regards the obligation of data protection agreements and that it includes appropriate data protection safeguards, including for the cases of transfers.

7.4. The GAC reiterates the importance of distinguishing between legal and natural persons (see above).

## Section 9. Publication of Domain Name Registration Data

As suggested in the definition section, the GAC recommends clarifying that publicly available means accessible free of charge. The proposed change is as follows:

9.1.1 *“In responses to RDDS queries, Registrar and Registry Operator MUST Publish free of charge the following data elements.”*

The GAC refers to comments formulated above in relation to the collection of data as regards the distinction of legal and natural persons. With regards to the publication requirements and for legal persons it is recommended to publish the additional data fields:

- Name of registrant,
- Phone number of registrant,
- A generic/functional email of registrant

These data should be added in the list of section 9.1.1. Moreover, the data referred to under section 9.1.6 (and especially registrant name, phone number and email) should not be redacted in the event the registrant is a legal person.

9.2.1 We acknowledge that the wording on voluntary legal/natural differentiation stems from EPDP Phase 1 Recommendation 17. However, this provision (9.2.1) gives a lot of uncertainty as it allows each contracted party to decide whether they want to redact (all) information based on a unilateral assessment of the existence of valid commercial or technical reasons, making the policy volatile. There is a need for a more uniform application.

9.2.6. The need to distinguish between legal and natural registrations also impacts this provision.

*“9.1.7. In responses to RDDS queries, Registrar and Registry Operator MAY Publish the Reseller data element.”*

As described in the GAC feedback to Section 6 above, the GAC appreciates the step taken to clarify registrar distribution channels via inclusion of the Reseller data element, but views this element as a necessary component for understanding the roles and responsibilities (e.g., for appropriate routing of law enforcement / court orders) to the entities best positioned to respond to them. The GAC therefore suggests:

*9.1.7. In responses to RDDS queries, Registrar and Registry Operator SHOULD Publish the Reseller data element(s) for the Reseller with a direct relationship with the Registrant..*

## Overlap of Section 9. Publication of Domain Name Registration Data & Section 10. Disclosure Requests

*“10.1. Registrar and Registry Operator MUST publish on their homepage a direct link to a page where the mechanism and process for submitting Disclosure Requests is detailed. The mechanism and process MUST specify (a) the required format and content of requests, (b) the Registrar’s or Registry Operator’s means of providing a response to the requestor, and (c) the anticipated timeline for responses.”*

The GAC supports inclusion of information on registrar websites pertaining to the mechanism and process for submitting Disclosure Requests, *however*, the GAC notes that a) any requestor seeking unredacted information may not know to look there, and b) the requestor has already viewed the single best channel for sharing such mechanism and process information: the published registration data itself.

The GAC therefore suggests the publication of such “mechanism and process” information within the Registration Data as follows:

*“9.1.1 In responses to RDDS queries, Registrar and Registry operator MUST Publish the following data elements:”*

...

9.1.1.12 A direct link to a page where the mechanism and process for submitting Disclosure Requests is detailed.

## Section 10. Disclosure Requests

Paragraph 10.6 regarding Urgent Requests for Disclosure misapplies the approved Phase 1 policy recommendations by failing to implement expedited timeframes consistent with the nature of responding to emergency requests for disclosure. For context, EPDP Recommendation 18 stated that:

*A separate timeline of [less than X business days] will [be] considered for the response to ‘Urgent’ Reasonable Disclosure Requests, those Requests for which evidence is supplied to show an immediate need for disclosure [time frame to be finalized and criteria set for Urgent requests during implementation]. [Emphasis added].*

Notably, the Phase 1 Recommendations highlighted that these urgent requests relate to “an immediate need for disclosure.” The implementation team defined urgent requests (Definition 3.8) in a manner consistent with such an immediate need:

*“Urgent Requests for Lawful Disclosure” are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure, or child exploitation in cases where disclosure of the data is necessary in combatting or addressing this threat. Critical infrastructure means the physical and cybersystems that are vital in that their incapacity or destruction would have a debilitating impact on economic security or public safety.*

As stressed in the section pertaining to definition, the GAC recommends to include in the scope of urgent requests other circumstances generating an immediate need for disclosure and which would otherwise be included in the regular requests (maximum response time of 30 days), in particular significant cybersecurity threats or incidents (such as those deriving from large scale ransomware, malware or botnet campaigns) regardless of whether the target is critical infrastructure.

Furthermore, in relation to the timeline, the GAC notes that despite the immediate need for such information, the implementation team construed the Phase 1 recommendations to permit a two business-day response period followed by one business-day extension under certain circumstances. Put simply, three business days (which could stretch to seven calendar days depending on weekends and intervening holidays) is not a reasonable time period for responding to urgent requests. This is especially true because “urgent” requests apply only to emergency situations involving imminent threats to life and critical infrastructure among other things.

The implementation team misinterpreted the Phase 1 recommendations by applying the same two business-day acknowledgment period for general requests to urgent requests. This flawed interpretation had the effect of prolonging the timeframe to respond to an urgent request. However, the foundational logic of dealing with “urgent” requests separately was to streamline the entire process because these requests deal with time-sensitive matters that involve threats to life, safety, or vital infrastructure. Hence, it would be neither reasonable nor logical to view the 2-day acknowledgement provision as overriding or extending the separate timeline for responding to urgent requests. More specifically, the acknowledgement time for general requests should not delay the contemplated expedited timeline for urgent requests. The GAC believes that this interpretation conflicts with the clear Phase 1 directive to develop “a separate timeline” for the response to urgent requests. The GAC recommends that the implementation team must revisit this issue to ensure that responses to urgent requests are in fact expedited in a manner consistent with an emergency response.

## **Section 12. Retention of Registration Data**

*“Registrar MUST retain those data elements necessary for the purposes of the Transfer Dispute Resolution Policy for a period of no less than fifteen (15) months following end of Registrar’s sponsorship of the registration or an inter-registrant (change of registrant) transfer of the registration.”*

The GAC recommends reviewing this provision, which only sets a minimum (mandatory) retention period, whereas the requirement under the GDPR is to limit retention to the period necessary to fulfill the purpose of processing.

### **3. Specific GAC Comments on Implementation of EPDP Phase 1 Recommendation 27: Changes to existing policies and procedures**

#### **Thick WHOIS Transition Policy for .COM, .NET and. JOBS**

It is important to understand the reasoning behind the conclusion that this policy (among others) is deemed “superseded” by the Phase 1 implementation.