

## Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process

20 February 2019

### Status of This Document

---

This is the Final Recommendations Report of the GNSO Expedited Policy Development Process (EPDP) Team on the Temporary Specification for gTLD Registration Data for submission to the GNSO Council.

### Preamble

---

This Final Report documents the EPDP Team's: (i) deliberations and responses to the charter questions, (ii) input received on the EPDP's Initial Report and the EPDP Team's subsequent analysis (iii) policy recommendations and associated consensus levels, and (iv) implementation guidance, for GNSO Council consideration.

---

## Table of Contents

<b>1 EXECUTIVE SUMMARY</b>	<b>3</b>
<b>2 OVERVIEW OF RECOMMENDATIONS</b>	<b>5</b>
<b>3 EPDP TEAM APPROACH</b>	<b>29</b>
<b>4 PUBLIC COMMENT ON THE EPDP TEAM INITIAL REPORT</b>	<b>32</b>
<b>5 EPDP TEAM RESPONSES TO CHARTER QUESTIONS &amp; RECOMMENDATIONS</b>	<b>34</b>
<b>6 NEXT STEPS</b>	<b>78</b>
<b>GLOSSARY</b>	<b>79</b>
<b>ANNEX A - BACKGROUND</b>	<b>86</b>
<b>ANNEX B – EPDP TEAM MEMBERSHIP AND ATTENDANCE</b>	<b>87</b>
<b>ANNEX C - COMMUNITY INPUT</b>	<b>91</b>
<b>ANNEX D – DATA ELEMENTS WORKBOOKS</b>	<b>92</b>
<b>ANNEX E - CONSENSUS CALL PROCESS AND DESIGNATIONS</b>	<b>148</b>
<b>ANNEX F – MINORITY STATEMENT</b>	<b>151</b>
<b>ANNEX G – EPDP TEAM GROUP STATEMENTS</b>	<b>155</b>

# 1 Executive Summary

On 17 May 2018, the ICANN Board of Directors (ICANN Board) adopted the [Temporary Specification for generic top-level domain \(gTLD\) Registration Data](#)<sup>1</sup> (“Temporary Specification”). The Temporary Specification modifies existing requirements in the Registrar Accreditation and Registry Agreements to comply with the European Union’s General Data Protection Regulation (“GDPR”)<sup>2</sup>. In accordance with the ICANN Bylaws, Consensus policies and Temporary Policies specification in the RA and RAA, the Temporary Specification will expire on 25 May 2019.

On 19 July 2018, the GNSO Council [initiated](#) an Expedited Policy Development Process (EPDP) and [chartered](#) the EPDP on the Temporary Specification for gTLD Registration Data team. All GNSO Stakeholder Groups, Constituencies, and ICANN Advisory Committees, that indicated interest in participating, are represented on the EPDP Team, although the Charter limits the number of members per group.

The charter asks the EPDP to determine if the Temporary Specification for gTLD Registration Data should become an ICANN Consensus Policy as is, or with modifications. In addition, the result must comply with the GDPR and take into account other relevant privacy and data protection laws. Additionally, the EPDP Team’s charter requires discussion of a standardized access model to nonpublic registration data, after the EPDP Team completes policy recommendations and answers ‘gating questions.

On 21 November 2018, the EPDP Team published its [Initial Report for public comment](#). The Initial Report contained the EPDP Team’s preliminary recommendations and a set of questions for public comment. The EPDP Team also examined and made recommendations about: (i) the validity, legitimacy and legal basis of the purposes outlined in the Temporary Specification, (ii) the legitimacy, necessity and scope of (x) the registrar collection of registration data and (y) the transfer of data from registrars to registries, each as outlined in the Temporary Specification, and (iv) the publication of registration data by registrars and registries as outlined in the Temporary Specification.

The Initial Report also provided preliminary recommendations and questions for the public to consider: (i) the transfer of data from registrars and registries to escrow providers and ICANN, (ii) the transfer of data from registries to emergency back-end registry operators (“EBERO”), (iii) the definition and framework for reasonable access to registration data, (iv) respective roles and responsibilities under the GDPR, i.e., the

---

<sup>1</sup> Because the Temporary Specification is central to the EPDP Team’s work, readers unfamiliar with the Temporary Specification may wish to read it before reading this Initial Report to gain a better understanding of and context for this Final Report.

<sup>2</sup> The GDPR can be found at <https://eur-lex.europa.eu/eli/reg/2016/679/oj>; for information on the GDPR see, <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/>

responsible parties, (v) applicable updates to ICANN Consensus Policies, and (vi) future work by the GNSO to ensure relevant Consensus Policies are reassessed to become consistent with applicable law.

The EPDP Team documented each of the data processing steps, and the purpose and the legal basis for each. This foundational work was necessary to develop GDPR-compliant solutions and is available in the Report's Appendix.

After the publication of the Initial Report, the EPDP Team: (i) sought guidance on legal issues, (ii) carefully reviewed public comments received in response to the publication of the Initial Report, (iii) reviewed the work-in-progress with the community groups the Team members represent, (iv) deliberated for the production of this Final Report that will be reviewed by the GNSO Council and, if approved, forwarded to the ICANN Board of Directors for approval as an ICANN Consensus Policy. Consensus calls on the recommendations contained in this Final Report, as required by the GNSO Working Group Guidelines, were carried out by the EPDP Team Chair, as described here: <https://mm.icann.org/pipermail/gns0-epdp-team/2019-February/001436.html>.

## 2 Overview of Recommendations

The GNSO Council chartered this EPDP Team to determine if the Temporary Specification for gTLD Registration Data should become an ICANN Consensus Policy as is, or with Proposed Responses to the Charter Questions & Preliminary Recommendations.

After reviewing the public comments on the Initial Report and updating the recommendations, the EPDP Team presents its recommendations for GNSO Council consideration. **Unless indicated differently as is the case for recommendation #2 and #16, recommendations have achieved full consensus / consensus support of the EPDP Team** (see Annex E for further details).

### 2.1 Recommendations for Council consideration

#### **EPDP Team Recommendation #1.**

The EPDP Team recommends that the following ICANN Purposes for processing gTLD Registration Data form the basis of the new ICANN policy:

1. a. In accordance with the relevant registry agreements and registrar accreditation agreements, activate a registered name and allocate it to the Registered Name Holder.
1. b. Subject to the Registry and Registrar Terms, Conditions and Policies and ICANN Consensus Policies:
  - (i) Establish the rights of a Registered Name Holder in a Registered Name; and
  - (ii) Ensure that a Registered Name Holder may exercise its right in the use, maintenance and disposition of the Registered Name.;
2. Contributing to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission through enabling responses to lawful data disclosure requests.<sup>3</sup>
3. Enable communication with the Registered Name Holder on matters relating to the Registered Name;
4. Provide mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure of a Registrar or Registry Operator, or unavailability of a Registrar or Registry Operator, as described in the RAA and RA, respectively;
5. i) Handle contractual compliance monitoring requests and audit activities consistent with the terms of the Registry agreement and the Registrar accreditation agreements and any applicable data processing agreements, by processing specific data only as necessary;  
ii) Handle compliance complaints initiated by ICANN, or third parties consistent with the terms of the Registry agreement and the Registrar accreditation agreements.

<sup>3</sup> Purpose 2 should not preclude disclosure in the course of investigating intellectual property infringement.

6. Operationalize policies for the resolution of disputes regarding or relating to the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names), namely, the UDRP, URS, PDDRP, RRDRP, and the TDRP; and
7. Enabling validation to confirm that Registered Name Holder meets gTLD registration policy eligibility criteria voluntarily adopted by Registry Operator and that are described or referenced in the Registry Agreement for that gTLD.<sup>4</sup>

**EPDP Team Recommendation #2. (Divergence)**

The EPDP Team commits to considering in Phase 2 of its work whether additional purposes should be considered to facilitate ICANN's Office of the Chief Technology Officer (OCTO) to carry out its mission (see <https://www.icann.org/octo>). This consideration should be informed by legal guidance on if/how provisions in the GDPR concerning research apply to ICANN Org and the expression for the need of such pseudonymized data by ICANN.

**EPDP Team Recommendation #3.**

In accordance with the EPDP Team Charter and in line with Purpose #2, the EPDP Team undertakes to make a recommendation pertaining to a standardised model for lawful disclosure of non-public Registration Data (referred to in the Charter as 'Standardised Access') now that the gating questions in the charter have been answered. This will include addressing questions such as:

- Whether such a system should be adopted
- What are the legitimate purposes for third parties to access registration data?
- What are the eligibility criteria for access to non-public Registration data?
- Do those parties/groups consist of different types of third-party requestors?
- What data elements should each user/party have access to?

In this context, the EPDP team will consider amongst other issues, disclosure in the course of intellectual property infringement and DNS abuse cases.<sup>5</sup>

---

<sup>4</sup> The EPDP Team's approval of Purpose 7 does not prevent and should not be interpreted as preventing Registry Operators from voluntarily adopting gTLD registration policy eligibility criteria that are not described or referenced in their respective Registry Agreements.

<sup>5</sup> The EPDP recognizes that ICANN has a responsibility to foster the openness, interoperability, resilience, security and/or stability of the DNS in accordance with its stated mission (citation required). It may have a purpose to require actors in the ecosystem to respond to data disclosure requests that are related to the security, stability and resilience of the system. The proposed Purpose 2 in this report is a placeholder, pending further legal analysis of the controller/joint controller relationship, and consultation with the EDPB. The EPDP recommends that further work be done in phase 2 on these issues, including a review of a limited purpose related to the enforcement of contracted party accountability for disclosure of personal data to legitimate requests.

There is a need to confirm that disclosure for legitimate purposes is not incompatible with the purposes for which such data has been collected.

**EPDP Team Recommendation #4.**

The EPDP Team recommends that requirements related to the accuracy of registration data under the current ICANN contracts and consensus policies shall not be affected by this policy.<sup>6</sup>

**EPDP Team Recommendation #5.**

The EPDP Team recommends that the data elements listed below (as illustrated in the data elements workbooks in Annex D) are required to be collected by registrars. In the aggregate, this means that the following data elements are to be collected<sup>7</sup> where some data elements are automatically generated and, as indicated below, in some cases it is optional for the registered name holder to provide those data elements:

Data Elements (Collected & Generated*)	Collection Logic
Domain Name	Green
Registrar Whois Server*	Green
Registrar URL*	Green
Registrar Registration Expiration Date*	Yellow
Registrar*	Green
Registrar IANA ID*	Green
Registrar Abuse Contact Email*	Green
Registrar Abuse Contact Phone*	Green
Reseller*	Yellow
Domain Status(es)*	Green
Registrant Fields	Green
• Name	Green
• Organization	Yellow
• Street	Green
• City	Green
• State/province	Green
• Postal code	Green
• Country	Green
• Phone	Green

<sup>6</sup> The topic of accuracy as related to GDPR compliance is expected to be considered further as well as the WHOIS Accuracy Reporting System.

<sup>7</sup> For those data elements marked as “Optional”, these are either optional for the Registrar to offer or optional for the RNH to provide. In both cases, if data is provided, it must be processed.

• Phone ext	
• Fax	
• Fax ext	
• Email	
Tech Fields	1
• Name	
• Phone	
• Email	
Name Server(s)	
DNSSEC	
Name Server IP Address(es)	
• Additional data elements as identified by Registry Operator in its registration policy, such as (i) status as Registry Operator Affiliate or Trademark Licensee [.MICROSOFT]; (ii) membership in community [.ECO]; (iii) licensing, registration or appropriate permits (.PHARMACY, .LAW) place of domicile [.NYC]; (iv) business entity or activity [.BANK, .BOT]	

Required   
 Optional

For further details, see [complete data elements matrix](#).

For the purpose of the Technical contact, which is optional for the Registered Name Holder to complete (and if the Registrar provides this option), Registrars are to advise the Registered Name Holder at the time of registration that the Registered Name Holder is free to (1) designate the same person as the registrant (or its representative) as the technical contact; or (2) provide contact information which does not directly identify the technical contact person concerned.

**EPDP Team Recommendation #6.**

The EPDP Team recommends that, as soon as commercially reasonable, Registrar must provide the opportunity for the Registered Name Holder to provide its Consent to publish redacted contact information, as well as the email address, in the RDS for the sponsoring registrar.



**EPDP Team Recommendation #7.**

The EPDP Team recommends that the specifically-identified data elements under “[t]ransmission of registration data from Registrar to Registry”, as illustrated in the aggregate data elements workbooks, must be transferred from registrar to registry provided an appropriate legal basis exists and data processing agreement is in place. In the aggregate, these data elements are:

Transfer of Data Elements from Registrar to Registry:

Data Elements (Collected & Generated*)	Transfer Logic
Domain Name	Green
Registrar Whois Server*	
Registrar URL*	
Registrar Registration Expiration Date*	Yellow
Registrar*	Green
Registrar IANA ID*	
Registrar Abuse Contact Email*	
Registrar Abuse Contact Phone*	
Reseller*	Yellow
Domain Status(es)*	Green
Registrant Fields	Yellow
• Name	
• Organization	
• Street	
• City	
• State/province	
• Postal code	
• Country	
• Phone	
• Phone ext	
• Fax	
• Fax ext	
• Email	
Tech Fields	Yellow
• Name	
• Phone	
• Email	
Name Server(s)	

Name Server IP Address(es)	
<ul style="list-style-type: none"> <li>Additional data elements as identified by Registry Operator in its registration policy, such as (i) status as Registry Operator Affiliate or Trademark Licensee [.MICROSOFT]; (ii) membership in community [.ECO]; (iii) licensing, registration or appropriate permits (.PHARMACY, .LAW] place of domicile [.NYC]; (iv) business entity or activity [.BANK, .BOT]</li> </ul>	





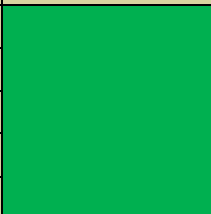
Required	
Optional	

For illustrative purposes, see [complete data elements matrix](#).

**EPDP Team Recommendation #8.**

1. The EPDP Team recommends that ICANN Org enters into legally-compliant data protection agreements with the data escrow providers.
2. The EPDP Team recommends updates to the contractual requirements for registries and registrars to transfer data that they process to the data escrow provider to ensure consistency with the data elements listed below (for illustrative purposes, see relevant workbooks in Annex D that analyze the purpose to provide mechanisms for safeguarding Registered Name Holders’ Registration Data).
3. The data elements to be transferred by Registries and Registrars to data escrow providers are:

For Registrars:

Data Elements (Collected & Generated*)	Collection Logic
Domain Name	
Registrar Registration Expiration Date*	
Registrar*	
Reseller*	
Registrant Fields	
<ul style="list-style-type: none"> <li>Name</li> </ul>	
<ul style="list-style-type: none"> <li>Street</li> </ul>	
<ul style="list-style-type: none"> <li>City</li> </ul>	
<ul style="list-style-type: none"> <li>State/province</li> </ul>	
<ul style="list-style-type: none"> <li>Postal code</li> </ul>	

• Country	Green
• Phone	
• Phone ext	Yellow
• Fax	
• Fax ext	
• Email	Green
Tech Fields	Light Green
• Name	Yellow
• Phone	
• Email	

For Registries:

Data Elements (Collected & Generated*)	Collection Logic
Domain Name	Green
Registry Domain ID*	
Registrar Whois Server*	
Registrar URL*	
Updated Date*	
Creation Date*	
Registry Expiry Date*	
Registrar Registration Expiration Date*	Yellow
Registrar*	Green
Registrar IANA ID*	
Registrar Abuse Contact Email*	
Registrar Abuse Contact Phone*	
Reseller*	Yellow
Domain Status(es)*	Green
Registry Registrant ID*	
Registrant Fields	Light Green
• Name	Yellow
• Organization	
• Street	
• City	
• State/province	
• Postal code	
• Country	
• Phone	
• Phone ext	

• Fax	
• Fax ext	
• Email	
Tech ID*	
Tech Fields	
• Name	
• Phone	
• Email	
Name Server(s)	
DNSSEC	
Name Server IP Address(es)	
• Additional data elements as identified by Registry Operator in its registration policy, such as (i) status as Registry Operator Affiliate or Trademark Licensee [.MICROSOFT]; (ii) membership in community [.ECO]; (iii) licensing, registration or appropriate permits (.PHARMACY, .LAW) place of domicile [.NYC]; (iv) business entity or activity [.BANK, .BOT]	

Required   
 Optional

**EPDP Team Recommendation #9.**

1. The EPDP Team recommends that updates, if needed, are made to the contractual requirements concerning the registration data elements for registries and registrars to transfer to ICANN Org the domain name registration data that they process when required/requested for purpose 5 (Contractual Compliance). (Note: Current language within the Contracts currently provides the appropriate scope for contractual compliance requests and subsequent transfer (e.g. Art 2.11 new gTLD Base Registry Agreement). (For illustrative purposes, please see Annex D - contractual compliance monitoring requests, audits, and complaints submitted by Registry Operators, Registrars, Registered Name Holders, and other Internet users). Registrars and Registries are required to transmit to ICANN org any RDS elements that are requested for Purpose 5. To clarify, the data elements listed in Annex D are the aggregate of data elements that ICANN Compliance may request. As noted in the Summary of ICANN Organization’s Contractual Compliance Team Data Processing Activities “If the Contractual Compliance Team is unable to validate the issue(s) outlined in a complaint because the publicly available WHOIS data is redacted/masked, it will request the redacted/masked registration data directly from the contracted party (or its representative). In these instances, the Contractual Compliance Team will only request the redacted/masked data elements that are

needed to validate the issue(s) outlined in the complaint”. Note, this recommendation does not exclude other information required by ICANN Contractual Compliance to enforce ICANN consensus policies and contracts.

**EPDP Team Recommendation #10.**

Requirements for processing personal data in public RDDS where processing is subject to GDPR: The EPDP Team recommends that redaction must be applied as follows to the data elements that are collected. Data elements neither redacted nor anonymized must appear via free public based query access<sup>8</sup>:

Data Elements (Collected & Generated*)	Redacted	Disclosure Logic		
Domain Name	No	Green		
Registry Domain ID*	Yes			
Registrar Whois Server*	No			
Registrar URL*	No			
Updated Date*	No			
Creation Date*	No			
Registry Expiry Date*	No			
Registrar Registration Expiration Date*	No		Yellow	
Registrar*	No		Green	
Registrar IANA ID*	No			
Registrar Abuse Contact Email*	No			
Registrar Abuse Contact Phone*	No			
Reseller*	No			Yellow
Domain Status(es)*	No			Green
Registry Registrant ID*	Yes			
Registrant Fields				
• Name	Yes	Green		
• Organization	Yes			
• Street	Yes			
• City	Yes <sup>9</sup>			
• State/province	No			
• Postal code	Yes			
• Country	No			

<sup>8</sup> As noted in the data elements workbooks, “a minimum public data set of registration data will be made available for query of gTLD second level domains in a freely accessible directory. Where a data element has been designated as non-public, it will be redacted”.

<sup>9</sup> See recommendation #11 for further details

• Phone	Yes	Green
• Email	Yes	
Tech ID*	Yes	
Tech Fields		
• Name	Yes	Green
• Phone	Yes	
• Email	Yes	
Name Server(s)	No	Yellow
DNSSEC	No	
Name Server IP Address(es)	No	
Last Update of Whois Database*	No	Green

Required  
Optional



The EPDP Team also confirms that, where GDPR is not applicable, Registry Operator and Registrar MAY apply the requirements outlined in this recommendation, as well as recommendation #12, #13, #14 and #15 (i) where it has a commercially reasonable purpose to do so, or (ii) where it is not technically feasible to limit application of these requirements.

**EPDP Team Recommendation #11.**

The EPDP Team recommends that redaction must be applied as follows to this data element:

Data Element	Redacted
Registrant Field	
• City	Yes

The EPDP Team expects to receive further legal advice on this topic which it will analyze in phase 2 of its work to determine whether or not this recommendation should be modified.

**EPDP Team Recommendation #12.**

The EPDP Team recommends that:

- The Organization field will be published if that publication is acknowledged or confirmed by the registrant via a process that can be determined by each registrar. If the registered name holder does not confirm the publication, the Organization field can be redacted or the field contents deleted at the option of the registrar.
- The implementation will have a phase-in period to allow registrars the time to deal with existing registrations and develop procedures.
- In the meantime, registrars will be permitted to redact the Organization Field.

- A registry Operator, where they believe it feasible to do so, may publish or redact the Org Field in the RDDS output.

**Implementation advice:** the implementation review team should consider the following implementation model discussed by the EPDP Team:

For existing registrations, the first step will be to confirm the correctness / accuracy of the existing Organization field data.

For the period between the adoption of EPDP policy recommendations and the conclusion of the implementation effort set for on, or before, 29 February 2020:

- 1) Registrars will redact the Organization field
- 2) Registrars will contact the registered name holders that have entered data in the Organization field and request review and confirmation that the data is correct.
  - a) If the registered name holder confirms or corrects the data will remain in the Organization field.
  - b) If the registrant declines, or does not respond to the query, the Registrar may redact the Organization field, or delete the field contents. If necessary, the registration will be re-assigned to the Registered Name Holder.
- 3) If Registrar chooses to publish the Registrant Organization field, it will notify these registered name holders that of the “date certain,” the Organization field will be treated as non-personal data and be published, for those Registered Names Holders who have confirmed the data and agreed to publication.

For new registrations, beginning with the “date certain”:

- 1) New registrations will present some disclosure, disclaimer or confirmation when data is entered in the Organization field. Registrars are free to develop their own process (e.g., opt-in, pop-up advisory or question, locked/grayed out field).
- 2) If the registered name holder confirms the data and agrees to publication:
  - a) The data in the Organization field will be published,
  - b) The Organization will be listed as the Registered Name Holder.
  - c) The name of the registered name holder (a natural person) will be listed as the point of contact at the Registrant Organization.

After the implementation phase-in period, the ORG FIELD will no longer be REDACTED by the registrar unless registered name holder has not agreed to publication.

Note, this is a Registrar obligation. For a Registry to publish is optional, until such time a way has been found that allows for the transfer of consent from Registrar to Registry.

**EPDP Team Recommendation #13.**

1) The EPDP Team recommends that the Registrar MUST provide an email address or a web form to facilitate email communication with the relevant contact, but MUST NOT identify the contact email address or the contact itself, unless as per Recommendation #6, the Registered Name Holder has provided consent for the publication of its email address.

2) The EPDP Team recommends Registrars MUST maintain Log Files, which shall not contain any Personal Information, and which shall contain confirmation that a relay of the communication between the requestor and the Registered Name Holder has occurred, not including the origin, recipient, or content of the message. Such records will be available to ICANN for compliance purposes, upon request. Nothing in this recommendation should be construed to prevent the registrar from taking reasonable and appropriate action to prevent the abuse of the registrar contact process.<sup>10</sup>

**EPDP Team Recommendation #14.**

In the case of a domain name registration where an "affiliated"<sup>11</sup> privacy/proxy service used (e.g. where data associated with a natural person is masked), Registrar (and Registry where applicable) MUST include in the public RDDS and return in response to any query full non-personal RDDS data of the privacy/proxy service, which MAY also include the existing privacy/proxy pseudonymized email.

**EPDP Team Recommendation #15.**

1. In order to inform its Phase 2 deliberations, the EPDP team recommends that ICANN Org, as a matter of urgency, undertakes a review of all of its active processes and procedures so as to identify and document the instances in which personal data is requested from a registrar beyond the period of the 'life of the registration'. Retention periods for specific data elements should then be identified, documented, and relied upon to establish the required relevant and specific minimum data retention expectations for registrars. The EPDP Team recommends community members be invited to contribute to this data gathering exercise by providing input on other legitimate purposes for which different retention periods may be applicable.
2. In the interim, the EPDP team has recognized that the Transfer Dispute Resolution Policy ("TDRP") has been identified as having the longest justified retention period

<sup>10</sup> Examples of abuse could include, but are not limited to, requestors purposely flooding the registrar's system with voluminous and invalid contact requests. This recommendation is not intended to prevent legitimate requests.

<sup>11</sup> As defined in the [Registrar Accreditation Agreement, Specification on Privacy and Proxy Registrations](#): "For any Proxy Service or Privacy Service offered by the Registrar or its Affiliates, including any of Registrar's or its Affiliates' P/P services distributed through Resellers, and used in connection with Registered Names Sponsored by the Registrar, the Registrar and its Affiliates".



of one year and has therefore recommended registrars be required to retain only those data elements deemed necessary for the purposes of the TDRP, for a period of fifteen months following the life of the registration plus three months to implement the deletion, i.e., 18 months<sup>12</sup>. This retention is grounded on the stated policy stipulation within the TDRP that claims under the policy may only be raised for a period of 12 months after the alleged breach (FN: see TDRP section 2.2) of the Transfer Policy (FN: see Section 1.15 of TDRP). This retention period does not restrict the ability of registries and registrars to retain data elements provided in Recommendations 4 -7 for other purposes specified in Recommendation 1 for shorter periods.<sup>13</sup>

3. The EPDP team recognizes that Contracted Parties may have needs or requirements for different retention periods in line with local law or other requirements. The EPDP team notes that nothing in this recommendation, or in separate ICANN-mandated policy, prohibits contracted parties from setting their own retention periods, which may be longer or shorter than what is specified in ICANN policy.
4. The EPDP team recommends that ICANN Org review its current data retention waiver procedure<sup>14</sup> to improve efficiency, request response times, and GDPR compliance, e.g., if a Registrar from a certain jurisdiction is successfully granted a data retention waiver, similarly-situated Registrars might apply the same waiver through a notice procedure and without having to produce a separate application.

**EPDP Team Recommendation #16. (Divergence)**

The EPDP Team recommends that Registrars and Registry Operators are permitted to differentiate between registrants on a geographic basis, but are not obligated to do so.

**EPDP Team Recommendation #17.**

- 1) The EPDP Team recommends that Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so.
- 2) The EPDP Team recommends that as soon as possible ICANN Org undertakes a study, for which the terms of reference are developed in consultation with the community, that considers:
  - The feasibility and costs including both implementation and potential liability costs of differentiating between legal and natural persons;

---

<sup>12</sup> Even though the TDRP provides for a 12 month period to file a complaint, the data is to be retained for an additional three months to ensure that TDRP complaints that are filed at the end of the 12 month period can be addressed.

<sup>13</sup> In Phase 2, the EPDP Team will work on identifying different retention periods for any other purposes, including the purposes identified in this Report.

<sup>14</sup> For avoidance of doubt, ICANN's data retention waiver procedure only applies to contracted parties who need to apply for shorter data retention periods. Contracted parties do not need to seek a waiver for longer retention periods for data retention under their own controllership.

- Examples of industries or other organizations that have successfully differentiated between legal and natural persons;
  - Privacy risks to registered name holders of differentiating between legal and natural persons; and
  - Other potential risks (if any) to registrars and registries of not differentiating.
- 3) The EPDP Team will determine and resolve the Legal vs. Natural issue in Phase 2.

**EPDP Team Recommendation #18.**

The EPDP Team recommends that the current requirements in Sections 4.1 and 4.2 of Appendix A to the Temporary Specification in relation to access to non-public registration data, upon expiration are replaced with the criteria below and finalized through the requirements set during the implementation stage, recognizing that work in Phase 2 on a system for Standardized Access to Non-Public Registration Data may further complement, revise, or supersede these requirements. In addition, the EPDP team recommends that when a system for Standardized Access to Non-Public Registration Data is developed, the need for a policy governing Reasonable Requests for Lawful Disclosure outside of that model will be required.

The EPDP Team recommends that the new policy will refer to “Reasonable Requests for Lawful Disclosure of Non-Public Registration Data” or “Reasonable Requests for Lawful Disclosure”, instead of ‘Reasonable Access’ and that Registrar and Registry Operator must process and respond to Reasonable Requests for Lawful Disclosure.

The basic criteria for Reasonable Requests Lawful Disclosure are as follows: First, a Reasonable Request for Lawful Disclosure must follow the format required by the Registrar or Registry Operator and provide the required information, which are to be finalized during the implementation phase (see below). Second, delivery of a properly-formed Reasonable Request for Lawful Disclosure to a Registrar or Registry Operator does NOT require automatic disclosure of information. Third, Registrars and Registry Operators will consider each request on its merits, including the asserted GDPR legal bases.

Registrars and Registry Operators must publish, in a publicly accessible section of their web-site, the mechanism and process for submitting Reasonable Requests for Lawful Disclosure. The mechanism and process should include information on the required format and content of requests, means of providing a response, and the anticipated timeline for responses.

The EPDP Team recommends that criteria for a Reasonable Request for Lawful Disclosure and the requirements for acknowledging receipt of a request and response to such request will be defined as part of the implementation of these policy recommendations but will include at a minimum:

- Minimum Information Required for Reasonable Requests for Lawful Disclosure:
  - Identification of and information about the requestor (including, the nature/type of business entity or individual, Power of Attorney statements, where applicable and relevant);
  - Information about the legal rights of the requestor and specific rationale and/or justification for the request, (e.g. What is the basis or reason for the request; Why is it necessary for the requestor to ask for this data?);
  - Affirmation that the request is being made in good faith;
  - A list of data elements requested by the requestor and why this data is limited to the need;
  - Agreement to process lawfully any data received in response to the request.
  
- Timeline & Criteria for Registrar and Registry Operator Responses - Registrars and Registries must reasonably consider and accommodate requests for lawful disclosure:
  - Response time for acknowledging receipt of a Reasonable Request for Lawful Disclosure. Without undue delay, but not more than two (2) business days from receipt, unless shown circumstances does not make this possible.
  - Requirements for what information responses should include. Responses where disclosure of data (in whole or in part) has been denied should include: rationale sufficient for the requestor to understand the reasons for the decision, including, for example, an analysis and explanation of how the balancing test was applied (if applicable).
  - Logs of Requests, Acknowledgements and Responses should be maintained in accordance with standard business recordation practices so that they are available to be produced as needed including, but not limited to, for audit purposes by ICANN Compliance;
  - Response time for a response to the requestor will occur without undue delay, but within maximum of 30 days unless there are exceptional circumstances. Such circumstances may include the overall number of requests received. The contracted parties will report the number of requests received to ICANN on a regular basis so that the reasonableness can be assessed.
  - A separate timeline of [less than X business days] will 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].

The EPDP Team recommends that the above be implemented and further work on defining these criteria commences as needed and as soon as possible.

**EPDP Team Recommendation #19.**

The EPDP Team recommends that ICANN Org negotiates and enters into required data protection agreements, as appropriate, with the Contracted Parties. In addition to the legally required components of such agreement, the agreement shall specify the responsibilities of the respective parties for the processing activities as described therein. Indemnification clauses should ensure that the risk for certain data processing is borne, to the extent appropriate, by the parties that are involved in the processing. Due consideration should be given to the analysis carried out by the EPDP Team in its Final Report.

**EPDP Team Recommendation #20.**

During Phase 1 of its work, the EPDP Team documented the data processing activities and responsible parties associated with gTLD registration data. The EPDP Team, accordingly, recommends the inclusion of the data processing activities and responsible parties, outlined below, to be confirmed and documented in the relevant data protection agreements, noting, however, this Recommendation may be affected by the finalization of the necessary agreements that would confirm and define the roles and responsibilities.

**ICANN PURPOSE<sup>15</sup>:**

As subject to Registry and Registrar terms, conditions and policies, and ICANN Consensus Policies:

- To establish the rights of a Registered Name Holder in a Registered Name; to ensure that a Registered Name Holder may exercise its rights in the use and disposition of the Registered Name; and
- To activate a registered name and allocate it to a Registered Name Holder.

<b>Processing Activity</b>	<b>Responsible Party<sup>16</sup>:</b>	<b>Lawful Basis<sup>17</sup>:</b>
<b>Collection</b>	ICANN Registrars Registries	6(1)(b) for Registrars 6(1)(f) for ICANN and Registries
<b>Transmission from Rr to Ry</b>	Registrars Registries	Certain data elements (domain name and nameservers) would be required to be disclosed. The

<sup>15</sup> The term ICANN Purpose is used to describe purposes for processing personal data that should be governed by ICANN Org via a Consensus Policy. Note there are additional purposes for processing personal data, which the contracted parties might pursue, but these are outside of what ICANN and its community should develop policy on or contractually enforce. It does not necessarily mean that such purpose is solely pursued by ICANN org.

<sup>16</sup> Note, the responsible party is not necessarily the party carrying out the processing activity. This applies to all references of ‘responsible party’ in these tables.

<sup>17</sup> In relation to the application of 6(1)b, please see input provided by external legal counsel in relation to charter questions k, l and m above.

<b>Disclosure</b>		lawful basis would be 6(1)b, should personal data be involved for Registrars and 6 (1)(f) of the GDPR for Registries.  For other data elements, Art. 6(1)(f) of the GDPR.
	Registrars Registries	Certain data elements (domain name and nameservers) would be required to be transferred from the Registrar to Registry. The lawful basis would be 6(1)b, should personal data be involved, for Registrars and 6 (1)(f) of the GDPR for Registries. 6(1)(f)
<b>Data Retention</b>	ICANN	6(1)(f)

**ICANN PURPOSE:**

Maintaining the security, stability and resiliency of the Domain Name System In accordance with ICANN’s mission through the enabling of lawful access for legitimate third-party interests to data elements collected for the other purposes identified herein.

<b>Processing Activity</b>	<b>Responsible Party:</b>	<b>Lawful Basis:</b>
<b>Collection</b>	ICANN Registrars Registries	6(1)(f)
<b>Transmission from Rr to Ry</b>	N/A	N/A
<b>Disclosure</b>	ICANN	6(1)(f)
<b>Data Retention</b>	ICANN	N/A

**ICANN PURPOSE:**  
 Enable communication with and/or notification to the Registered Name Holder and/or their delegated agents of technical and/or administrative issues with a Registered Name

<u>Processing Activity</u>	<u>Responsible Party:</u>	<u>Lawful Basis:</u>
Collection	Registrar Registries	6(1)(b) for Registrars 6(1)(f) for Registries
Transmission from Rr to Ry	ICANN Registries	6(1)(f)
Disclosure	TBD	
Data Retention	ICANN	N/A

**ICANN PURPOSE:**  
 Provide mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure, or other unavailability of a Registrar or Registry Operator

<u>Processing Activity</u>	<u>Responsible Party:</u>	<u>Lawful Basis</u>
Collection	ICANN	6(1)(f)
Transmission from Rr to Ry	ICANN	6(1)(f)
Disclosure	ICANN	6(1)(f)
Data Retention	ICANN	6(1)(f)

**ICANN PURPOSE:**  
 Handle contractual compliance monitoring requests, audits, and complaints submitted by Registry Operators, Registrars, Registered Name Holders, and other Internet users.

<u>Processing Activity</u>	<u>Responsible Party:</u>	<u>Lawful Basis:</u>
Collection	ICANN	6(1)(f)
Transmission from Rr to Ry	ICANN	6(1)(f)
Disclosure	N/A	
Data Retention	ICANN	6(1)(f)

**ICANN PURPOSE:**  
 Coordinate, operationalize and facilitate policies for resolution of disputes regarding or relating to the registration of domain names (as opposed to the use of such domain names), namely, the UDRP, URS, PDDRP, RRDRP and future-developed domain name registration-related dispute procedures for which it is established that the processing of personal data is necessary

<b>Processing Activity</b>	<b>Responsible Party:</b>	<b>Lawful Basis:</b>
<b>Collection</b>	ICANN Registrars	6(1)(b) for Registrars 6(1)(f) for Registries
<b>Transmission from Rr to Ry</b>	ICANN Registries Registrars	6(1)(b) for Registrars 6(1)(f) for Registries
<b>Transmission to dispute resolution providers</b>	ICANN Registries Registrars Dispute Resolution Provider – Processor or independent controller	6(1)(b) for Registrars 6(1)(f) for Registries and ICANN
<b>Disclosure</b>		
<b>Data Retention</b>		

**ICANN PURPOSE:**  
 Enabling validation to confirm that Registered Name Holder meets optional gTLD registration policy eligibility criteria voluntarily adopted by Registry Operator.

<b>Processing Activity</b>	<b>Responsible Party:</b>	<b>Lawful basis:</b>
<b>Collecting specific data for Registry Agreement-mandated eligibility requirements</b>	Registries	6(1)(b) for Registrars 6(1)(f) for Registries
<b>Collecting specific data for Registry Operator-adopted eligibility requirements</b>	Registries	6(1)(b) for Registrars 6(1)(f) for Registries

<b>Transmission from Rr to Ry RA-mandated eligibility requirements</b>	Registries	6(1)(b) for Registrars 6(1)(f) for Registries
<b>Transmission from Rr to Ry Registry-adopted eligibility requirements</b>	Registries	6(1)(b) for Registrars 6(1)(f) for Registries
<b>Disclosure</b>	Registries	N/A
<b>Data Retention</b>	Registries	6(1)(f)

**EPDP Team Recommendation #21.**

The EPDP Team also recommends that the GNSO Council instructs the review of all RPMs PDP WG to consider, as part of its deliberations, whether there is a need to update existing requirements to clarify that a complainant must only be required to insert the publicly-available RDDS data for the domain name(s) at issue in its initial complaint. The EPDP Team also recommends the GNSO Council to instruct the RPMs PDP WG to consider whether upon receiving updated RDDS data (if any), the complainant must be given the opportunity to file an amended complaint containing the updated respondent information.

**EPDP Team Recommendation #22.**

The EPDP Team recommends that ICANN Org must enter into appropriate data protection agreements with dispute resolution providers in which, amongst other items, the data retention period is specifically addressed.



**EPDP Team Recommendation #23.**

The EPDP Team recommends that, for the new policy on gTLD registration data, the following requirements MUST apply in relation to URS and UDRP until such time as these are superseded by recommendations from the RPMs PDP WG and/or policies from the EPDP regarding disclosure:

Uniform Rapid Suspension (supplemental requirements for the 17 October 2013 URS High Level Technical Requirements for Registries and Registrars and URS Rules effective 28 June 2013)

(1) Registry Operator Requirement: The Registry Operator (or appointed BERO) MUST provide the URS provider with the full Registration Data for each of the specified domain names, upon the URS provider notifying the Registry Operator (or appointed BERO) of the existence of a complaint, or participate in another mechanism to provide the full Registration Data to the Provider as specified by ICANN. If the gTLD operates as a "thin" registry, the Registry Operator MUST provide the available Registration Data to the URS Provider.

(2) Registrar Requirement: If the domain name(s) subject to the complaint reside on a "thin" registry, the Registrar MUST provide the full Registration Data to the URS Provider upon notification of a complaint.

(3) URS Rules: Complainant's complaint will not be deemed defective for failure to provide the name of the Respondent (Registered Name Holder) and all other relevant contact information required by Section 3 of the URS Rules if such contact information of the Respondent is not available in registration data publicly available in RDDS or not otherwise known to Complainant. In such an event, Complainant may file a complaint against an unidentified Respondent and the Provider shall provide the Complainant with the relevant contact details of the Registered Name Holder after being presented with a complaint against an unidentified Respondent.

Uniform Dispute Resolution Policy (supplemental requirements for the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules"))

(1) Registrar Requirement: The Registrar MUST provide the UDRP provider with the full Registration Data for each of the specified domain names, upon the UDRP provider notifying the Registrar of the existence of a complaint, or participate in another mechanism to provide the full Registration Data to the Provider as specified by ICANN.

(2) Complainant's complaint will not be deemed defective for failure to provide the name of the Respondent (Registered Name Holder) and all other relevant contact information required by Section 3 of the UDRP Rules if such contact information of the Respondent is not available in registration data publicly available in RDDS or not otherwise known to Complainant. In such an event, Complainant may file a complaint against an unidentified Respondent and the Provider shall provide the Complainant with the relevant contact details of the Registered Name Holder after being presented with a complaint against an unidentified Respondent.

**EPDP Team Recommendation #24.**

The EPDP Team recommends that for the new policy on gTLD registration data, the following requirements MUST apply in relation to the Transfer Policy until such time these are superseded by recommendations that may come out of the Transfer Policy review that is being undertaken by the GNSO Council:

Supplemental procedures for the [Transfer Policy](#) applicable to all ICANN-accredited Registrars

(a) Until such time when the RDAP service (or other secure methods for transferring data) is required by ICANN to be offered, if the Gaining Registrar is unable to gain access to then-current Registration Data for a domain name subject of a transfer, the related requirements in the Transfer Policy will be superseded by the below provisions:

(a1) The Gaining Registrar is not REQUIRED to obtain a Form of Authorization from the Transfer Contact.

(a2) The Registrant MUST independently re-enter Registration Data with the Gaining Registrar. In such instance, the Gaining Registrar is not REQUIRED to follow the Change of Registrant Process as provided in Section II.C. of the Transfer Policy.

(b) As used in the Transfer Policy:

(b1) The term "Whois data" SHALL have the same meaning as "Registration Data".

(b2) The term "Whois details" SHALL have the same meaning as "Registration Data".

(b3) The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".

(b4) The term "Whois" SHALL have the same meaning as "RDDS".

(c) Registrar and Registry Operator SHALL follow best practices in generating and updating the "AuthInfo" code to facilitate a secure transfer process.

(d) Registry Operator MUST verify that the "AuthInfo" code provided by the Gaining Registrar is valid in order to accept an inter-registrar transfer request.

**EPDP Team Recommendation #25.**

The EPDP Team recommends that the GNSO Council, as part of its review of the Transfer Policy, specifically requests the review of the implications, as well as adjustments, that may be needed to the Transfer Policy as a result of GDPR, with great urgency.

**EPDP Team Recommendation #26.**

The EPDP Team recommends that ICANN Org enters into required data protection agreements such as a Data Processing Agreement (GDPR Art. 28) or Joint Controller Agreement (Art. 26), as appropriate, with the non-Contracted Party entities involved in registration data processing such as data escrow providers and EBERO providers. These agreements are expected to set out the relationship obligations and instructions for data processing between the different parties.

**EPDP Team Recommendation #27.**

The EPDP Team recommends that as part of the implementation of these policy recommendations, updates are made to the following existing policies / procedures, and any others that may have been omitted, to ensure consistency with these policy recommendations as, for example, a number of these refer to administrative and/or technical contact which will no longer be required data elements:

- [Registry Registration Data Directory Services Consistent Labeling and Display Policy](#)
- [Thick WHOIS Transition Policy for .COM, .NET, .JOBS](#)
- [Rules for Uniform Domain Name Dispute Resolution Policy](#)
- [WHOIS Data Reminder Policy](#)
- [Transfer Policy](#)
- [Uniform Rapid Suspension System \(URS\) Rules](#)
- [Transfer Dispute Resolution Policy](#)

**EPDP Team Recommendation #28.**

The EPDP Team recommends that the effective date of the gTLD Registration Data Policy shall be February 29, 2020. All gTLD Registry Operators and ICANN-accredited registrars will be required to comply with the gTLD Registration Data Policy as of that date. The EPDP Team recommends that until February 29, 2020, registries and registrars are required EITHER to comply with this gTLD Registration Data Policy OR continue to implement measures consistent with the Temporary Specification (as adopted by the ICANN Board on 17 May 2018, and expired on 25 May 2019). Registries and registrars who continue to implement measures compliant with the expired Temporary Specification will not be subject to Compliance penalty specifically related to those measures until February 29, 2020.

The EPDP Team furthermore recommends that, as a matter of urgency, the GNSO Council and ICANN Org, informally convene the Implementation Review Team to allow for the necessary planning to take place before ICANN Board consideration of this Final Report, following which the IRT would be formally convened.

**EPDP Team Recommendation #29.**

Recognizing that in the case of some existing registrations, there may be an Administrative Contact but no or incomplete Registered Name Holder contact information, the EPDP team recommends that prior to eliminating Administrative Contact fields, all Registrars must ensure that each registration contains Registered Name Holder contact information.

## 2.2 Conclusions and Next Steps

This Final Report will be submitted to the GNSO Council for its consideration and approval.

## 2.3 Other Relevant Sections of this Report

This Final Report also includes:

- Background of the issue, documenting how the Board adopted the Temporary Specification and the required procedures accompanying that adoption;
- Documentation of participation in the EPDP Team’s deliberations, attendance records, and links to Statements of Interest;
- An annex that includes the EPDP Team’s mandate as defined in the Charter adopted by the GNSO Council and;
- Information concerning community input obtained through formal SO/AC and SG/C channels as well as the publication of the Initial Report for public comment, including the input provided.

## 3 EPDP Team Approach

This Section provides a summary overview of the EPDP Team’s working methodology and approach.

### 3.1 Working Methodology

The EPDP Team began its deliberations on [1 August 2018](#). It worked primarily through conference calls scheduled two or more times per week, in addition to email exchanges on its mailing list. Additionally, the EPDP Team held three face-to-face meetings; one at the ICANN headquarters in Los Angeles in September 2018; one at the ICANN 63 Public Meeting in Barcelona in October 2018; and a third in Toronto in January 2019. The EPDP Team’s wiki [workspace documents its meetings](#), including its [mailing list](#), draft documents, background materials, and input received from ICANN’s SO/ACs including the GNSO’s Stakeholder Groups and Constituencies.

The EPDP Team also prepared a Work Plan, which was reviewed and updated on a regular basis, and a template to (i) tabulate Constituency and Stakeholder Group statements (see Annex B); and (ii) input from other ICANN SOs/ACs and individual EPDP Team members (see Annex B). This template was also used to record input from other ICANN Supporting Organizations and Advisory Committees, as well as individual EPDP Team members’ responses (either on their own behalf or as representatives of their respective groups) which can be found in Annex C.

The EPDP Team held a [community session](#) at the ICANN63 Public Meeting in Barcelona, to present its methodologies and preliminary findings to the broader ICANN community for discussion and feedback.

### 3.2 Initial Fact-Finding and Triage

The EPDP Team Charter required the team to review a list of topics and questions, as part of its work to develop policy recommendations relating to the Temporary Specification. These topics and questions were derived in large part from the prior work of the [EPDP Drafting Team](#), comprised of GNSO Councilors.

The EPDP Team’s first deliverable under its charter was a “triage” document of the Temporary Specification to identify items that had Full Consensus support of the EPDP Team, and should be adopted as is (without further discussion or modifications).

The Triage report disclosed few areas where the EPDP Team agreed with the Temporary Specification language. However, there were several areas of agreement with the underlying principles in several sections of the Temporary Specification. Where a constituency / stakeholder group / advisory committee did indicate support for a certain section of the

Temporary Specification, edits were often also suggested, meaning that essentially no section of the Temporary Specification will be adopted without modifications.

The Triage report and the surveys and discussions that formed the basis for the Triage report informed the EPDP Team's work on the Initial Report:

1. EPDP Team members' comments suggested sequencing of topics, which improved efficiency.
2. EPDP Team members' rationales in support of/opposition to each section narrowed the discussion to particular issues and suggested proposed modifications.
3. The EPDP Team compiled a library of each group's positions on a variety of topics, including outstanding issues to be discussed in the course of the Team's deliberations.

The Triage Report as well as input received can be found here:

<https://community.icann.org/x/jxBpBQ>.

### 3.3 Discussion Summary Indexes

The Triage Report resulted in the Support Team's development of the Discussion Summary Indexes to combine all input received into one standard document, allowing the EPDP Team to prepare for meeting deliberations with the same set of information. The Discussion Summary Indexes included: (i) the relevant Charter Questions mapped to the Temporary Specification; (ii) relevant input received in response to the triage surveys, (iii) early input and (iv) advice provided by the European Data Protection Board (EDPB). The Discussion Summary Indexes can be found here: <https://community.icann.org/x/ExxpBQ>.

### 3.4 Data Elements Workbooks

The EPDP Team realized the need to review each of the data elements collected, the purpose for its processing, and the legal basis for that data processing. This work resulted in the creation of the Data Elements Workbooks, which bring together purpose, data elements, processing activities, lawful basis for processing and responsible parties. For the Data Element Workbook for each purpose identified by the EPDP Team, see Annex D.

### 3.5 Small Teams

The EPDP Team worked in small teams to develop proposed consensus positions for the entire team to consider. The EPDP Team used small teams before the Initial Report to explore overarching Charter issues, develop proposed answers to Charter Questions, and formulate preliminary recommendations for review by the full EPDP Team. The small teams covered three topics:

1. Legal and natural persons:  
Should Contracted Parties be allowed or required to treat legal and natural persons differently, and what mechanism is needed to ensure reliable determination of status?  
Is there a legal basis for Contracted Parties to treat legal and natural persons differently?  
What are the risks associated with differentiation of registrant status as legal or natural persons across multiple jurisdictions? (See EDPB letter of 5 July 2018).
2. Geographic basis:  
Should Registry Operators and Registrars (“Contracted Parties”) be permitted or required to differentiate between registrants on a geographic basis?
3. Temporary Specification and Reasonable Access  
Should existing requirements in the Temporary Specification remain in place until a model for access is finalized?

The EPDP Team also utilized small teams to review and analyze the public comments received on its Initial Report.

This approach, including the resultant work products, form the basis for the EPDP Team’s responses to the Charter Questions and recommendations are in the next section of this Final Report.

### 3.6 Mediation Techniques

The EPDP Team worked in face-to-face meetings with certified mediators from the Consensus Building Institute ([www.cbi.org](http://www.cbi.org)), who were generally credited with positively impacting the timely development of consensus positions and keeping discussions on track.

### 3.7 Charter Questions

In addressing the Charter Questions, the EPDP Team considered (1) each group’s responses to the [triage surveys](#); (2) each group’s [Early Input](#) on specific charter questions; and (3) public comments on the Initial Report.

## 4 Public Comment on the EPDP Team Initial Report

### 4.1 Background

On 21 November 2018, the EPDP Team published its [Initial Report for public comment](#). The Initial Report outlined the core issues discussed, proposed responses to Charter Questions and accompanying preliminary recommendations.

The EPDP Team welcomed community feedback on any issue in the Initial Report; however, the EPDP Team particularly sought input on the following questions. In responding to the below questions, the Initial Report encouraged commenters to (1) consider GDPR compliance in all responses, (2) identify specific changes, and (3) provide a rationale for any requested change:

- Are the proposed purposes outlined in the Initial Report sufficiently specific and, if not, how do you propose to modify them? Should any purposes be added?
- Are the recommended data elements as listed in the Initial Report as required for registrar collection necessary for the purposes identified? If not, why not? Are any data elements missing that are necessary to achieve the purposes identified?
- Are there other data elements than those listed in the Initial Report that are required to be transferred between registrars and registries / escrow providers that are necessary to achieve the purposes identified?
- Are there other data elements than those listed in the Initial Report that are required to be transferred between registrars and registries / ICANN Compliance that are necessary to achieve the purposes identified? Are there identified data elements that are not required to be transferred between registrars and registries / ICANN Compliance and are not necessary to achieve the purposes identified?
- Should the EPDP Team consider any changes in the redaction of data elements, compared to what is recommended in the Initial Report?
- Should the EPDP Team consider any changes to the recommended data retention periods compared to those recommended in the Initial Report? Do you believe the justification for retaining data beyond the term of the domain name registration is sufficient? Why or why not?
- What other factors should the EPDP team consider about whether Contracted Parties should be permitted or required to differentiate between registrants on a geographic basis? Between natural and legal persons? Are there any other risks associated with differentiation of registrant status (as natural or legal person) or geographic location? If so, please identify those factors and/or risks and how they would affect possible recommendations. Should the community explore whether procedures would be feasible to accurately distinguish on a global scale whether registrants/contracted parties fall within jurisdiction of the GDPR or other data protection laws? Can the community point to existing examples of where such a



differentiation is already made and could it apply at a global scale for purposes of registration data?

- Should the EPDP Team consider any changes to its recommendations in relation to "reasonable access" as outlined in the Initial Report?
- Are there any changes that the EPDP Team should consider in relation to the URS and UDRP that have not already been identified in the Initial Report?
- Are there any changes that the EPDP Team should consider in relation to the Transfer Policy that have not already been identified Initial Report?

## 4.2 Input received

Due to the expedited nature of this EPDP, the public comment forum ran for 30 days. The EPDP Team used a Google form to facilitate review of public comments. Nine GNSO Stakeholder Groups, Constituencies and ICANN Advisory Committees, submitted comments in addition to thirty-three contributions from individuals or organizations. The input provided is at:

<https://docs.google.com/spreadsheets/d/1GUf86Ngo97g74wLyDmeBv8IGcUtjLJWjsEdxBXcYDD4/edit#gid=694919619>.

## 4.3 Review of public comments

To facilitate its review of the public comments, the EPDP Team developed a set of [public comment review tools](#) (PCRTs). Through the work of small teams, plenary sessions, and face-to-face time, the EPDP Team completed its review and assessment of the input provided and agreed on changes to be made to the recommendations and/or report.

## 5 EPDP Team Responses to Charter Questions & Recommendations

After reviewing the public comments on the Initial Report and updating the recommendations, the EPDP Team presents its recommendations for GNSO Council consideration. This Final Report states the level of consensus within the EPDP Team achieved for the different recommendations. **Unless indicated differently as is the case for recommendation #2 and #16, recommendations have achieved full consensus / consensus support of the EPDP Team** (see Annex E for further details).

From the EPDP Team Charter:

“The EPDP Team is being chartered to determine if the Temporary Specification for gTLD Registration Data should become an ICANN Consensus Policy, as is or with modifications, while complying with the GDPR and other relevant privacy and data protection law. As part of this determination, the EPDP Team is, at a minimum, expected to consider the following elements of the Temporary Specification and answer the following charter questions. The EPDP Team shall consider what subsidiary recommendations it might make for future work by the GNSO which might be necessary to ensure relevant Consensus Policies, including those related to registration data, are reassessed to become consistent with applicable law”.

### Part 1: Purposes for Processing Registration Data

Charter Question

- a) Purposes outlined in Sec. 4.4.1-4.4.13 of the Temporary Specification:
- a1) Are the purposes enumerated in the Temporary Specification valid and legitimate?
  - a2) Do those purposes have a corresponding legal basis?
  - a3) Should any of the purposes be eliminated or adjusted?
  - a4) Should any purposes be added?

EPDP Team considerations and deliberations in addressing the charter questions:

- The EPDP Team reviewed the feedback that the European Data Protection Board provided in relation to lawful purposes for processing personal data and took specific note of the following:

“Nevertheless, the EDPB considers it essential that a clear distinction be maintained between the different processing activities that take place in the context of WHOIS and the respective purposes pursued by the various stakeholders involved. There are processing activities determined by ICANN, for which ICANN, as well as the registrars and registries, require their own legal basis and purpose, and then there are processing activities determined

by third parties, which require their own legal basis and purpose. The EDPB therefore reiterates that ICANN should take care not to conflate its own purposes with the interests of third parties, nor with the lawful grounds of processing which may be applicable in a particular case.”<sup>18</sup>

As well as,

“As expressed also in earlier correspondence with ICANN (including [this letter](#) of December 2017 and [this letter](#) of April 2018), WP29 expects ICANN to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data.”<sup>19</sup>

- The Discussion Summary Index for section 4.4 captures this input, and is at <https://community.icann.org/x/ExxpBQ>.
- The EPDP Team deliberated on the purposes listed in the Temporary Specification as a starting point, but reformulated the text and further specified the relevant lawful basis (if any) and the party/parties involved in the processing.
- “ICANN Purpose” is used to describe purposes for processing personal data that should be governed by ICANN Org via a Consensus Policy.
- Contracted parties might pursue additional purposes for processing personal data, but these are outside of what ICANN and its community should develop policy or contractually enforce. This does not necessarily mean that such purpose is solely pursued by ICANN Org, apart from purpose 2.

#### **EPDP Team Recommendation #1.**

The EPDP Team recommends that the following ICANN Purposes for processing gTLD Registration Data form the basis of the new ICANN policy:

1. a. In accordance with the relevant registry agreements and registrar accreditation agreements, activate a registered name and allocate it to the Registered Name Holder.
1. b. Subject to the Registry and Registrar Terms, Conditions and Policies and ICANN Consensus Policies:
  - (i) Establish the rights of a Registered Name Holder in a Registered Name; and
  - (ii) Ensure that a Registered Name Holder may exercise its right in the use, maintenance and disposition of the Registered Name.;

<sup>18</sup> See <https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf>

<sup>19</sup> See [https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois\\_en](https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_en)

2. Contributing to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission through enabling responses to lawful data disclosure requests.<sup>20</sup>
3. Enable communication with the Registered Name Holder on matters relating to the Registered Name;
4. Provide mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure of a Registrar or Registry Operator, or unavailability of a Registrar or Registry Operator, as described in the RAA and RA, respectively;
5.
  - i) Handle contractual compliance monitoring requests and audit activities consistent with the terms of the Registry agreement and the Registrar accreditation agreements and any applicable data processing agreements, by processing specific data only as necessary;
  - ii) Handle compliance complaints initiated by ICANN, or third parties consistent with the terms of the Registry agreement and the Registrar accreditation agreements.
6. Operationalize policies for the resolution of disputes regarding or relating to the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names), namely, the UDRP, URS, PDDRP, RRDRP, and the TDRP; and
7. Enabling validation to confirm that Registered Name Holder meets gTLD registration policy eligibility criteria voluntarily adopted by Registry Operator and that are described or referenced in the Registry Agreement for that gTLD.<sup>21</sup>

Note that for each of these purposes, the EPDP Team has also identified: (i) the related processing activities; (ii) the corresponding lawful basis for each processing activity; and (iii) the responsible parties involved in each processing activity. For more information regarding the above, please refer to the Data Elements Workbooks which can be found in Annex D.

Note that Purpose 2 is a placeholder pending further work on the issue of access in Phase 2 of this EPDP and is expected to be revisited once this Phase 2 work has been completed.

Note that updates have been made to the data elements workbooks for purpose 5 to clarify that the WHOIS Accuracy Reporting System (ARS) is considered covered as part of that purpose.

- The EPDP Team considered an additional purpose for processing registration data to address the needs and benefits provided by DNS security and stability research by ICANN Org through investigation, research and publication of reports on threats to the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS.

---

<sup>20</sup> Purpose 2 should not preclude disclosure in the course of investigating intellectual property infringement.

<sup>21</sup> The EPDP Team's approval of Purpose 7 does not prevent and should not be interpreted as preventing Registry Operators from voluntarily adopting gTLD registration policy eligibility criteria that are not described or referenced in their respective Registry Agreements.

In doing so, the EPDP Team considered:

- input provided by ICANN Org on the current use of data by ICANN’s Office of the Chief Technology Officer (OCTO) (see <https://community.icann.org/x/ahppBQ>), and
- relevant GDPR provisions that allow the use of personal data to carry out research, provided that other GDPR requirements are met.

In its input, OCTO stated it “does not require personal data in domain name registration data for its work. For example, OCTO’s Domain Abuse Activity Reporting (DAAR) project <<https://www.icann.org/octo-ssr/daar>> uses only the registrar and nameserver information.”

The discussion led to the preliminary conclusion that it was clear that OCTO does not at this time require the use of personal data in its work.

However, questions remained as to whether OCTO may require the use of pseudonymized data in the future in order to carry out its work. If this is the case, clarification may be required as to:

- how GDPR provisions would apply to ICANN Org given its multiple roles as data controller and processor and also the fact that ICANN Org currently does not collect the data; and
- whether ICANN Org could qualify for processing pseudonymized data for research purposes under some existing purpose for processing data listed above in this report.

Therefore, the EPDP Team recognized that additional consideration can be given to this topic once the questions above regarding the need for pseudonymized data and legal interpretation are answered. As a result, the EPDP Team is putting forward the following recommendation, recognizing that legal guidance received in the interim could make it no longer relevant.

**EPDP Team Recommendation #2.** (Divergence)

The EPDP Team commits to considering in Phase 2 of its work whether additional purposes should be considered to facilitate ICANN’s Office of the Chief Technology Officer (OCTO) to carry out its mission (see <https://www.icann.org/octo>). This consideration should be informed by legal guidance on if/how provisions in the GDPR concerning research apply to ICANN Org and the expression for the need of such pseudonymized data by ICANN.

**EPDP Team Recommendation #3.**

In accordance with the EPDP Team Charter and in line with Purpose #2, the EPDP Team undertakes to make a recommendation pertaining to a standardised model for lawful disclosure of non-public Registration Data (referred to in the Charter as 'Standardised Access') now that the gating questions in the charter have been answered. This will include addressing questions such as:

- Whether such a system should be adopted
- What are the legitimate purposes for third parties to access registration data?
- What are the eligibility criteria for access to non-public Registration data?
- Do those parties/groups consist of different types of third-party requestors?
- What data elements should each user/party have access to?

In this context, the EPDP team will consider amongst other issues, disclosure in the course of intellectual property infringement and DNS abuse cases.<sup>22</sup>

There is a need to confirm that disclosure for legitimate purposes is not incompatible with the purposes for which such data has been collected.

- The EPDP Team requested external counsel guidance on the topic of accuracy in the context of GDPR, and received the following summary answer:

“In sum, because compliance with the Accuracy Principle is based on a reasonableness standard, ICANN and the relevant parties will be better placed to evaluate whether these procedures are sufficient. From our vantage point, as the procedures do require affirmative steps that will help confirm accuracy, unless there is reason to believe these are *insufficient*, we see no clear requirement to review them.”<sup>23</sup>

**EPDP Team Recommendation #4.**

The EPDP Team recommends that requirements related to the accuracy of registration data under the current ICANN contracts and consensus policies shall not be affected by this policy.<sup>24</sup>

---

<sup>22</sup> The EPDP recognizes that ICANN has a responsibility to foster the openness, interoperability, resilience, security and/or stability of the DNS in accordance with its stated mission (citation required). It may have a purpose to require actors in the ecosystem to respond to data disclosure requests that are related to the security, stability and resilience of the system. The proposed Purpose 2 in this report is a placeholder, pending further legal analysis of the controller/joint controller relationship, and consultation with the EDPB. The EPDP recommends that further work be done in phase 2 on these issues, including a review of a limited purpose related to the enforcement of contracted party accountability for disclosure of personal data to legitimate requests.

<sup>23</sup> For further details, please see: <https://mm.icann.org/pipermail/gnso-epdp-legal/2019-February/000047.html>.

<sup>24</sup> The topic of accuracy as related to GDPR compliance is expected to be considered further as well as the WHOIS Accuracy Reporting System.

---

## Part 2: Required Data Processing Activities

### Charter Question

#### b) Collection of registration data by registrar:

- b1) What data should registrars be required to collect for each of the following contacts: Registrant, Tech, Admin, Billing?
- b2) What data is collected because it is necessary to deliver the service of fulfilling a domain registration, versus other legitimate purpose as outlined in part (A) above?
- b3) How shall legitimacy of collecting data be defined (at least for personal data collected from European registrants and others in jurisdictions with data protection law)?
- b4) Under the purposes identified in Section A, is there legal justification for collection of these data elements, or a legal reason why registrars should not continue to collect all data elements for each contact?

#### EPDP Team considerations and deliberations in addressing the charter questions:

- The EPDP Team considered both the input provided by each group in response to the triage surveys as well as the input provided by each group in response to the request for early input in relation to these questions.
- In addition, the EPDP Team reviewed the feedback from the European Data Protection Board related to the collection of registration data and took specific note of the following:

“The EDPB considers that registrants should in principle not be required to provide personal data directly identifying individual employees (or third parties) fulfilling the administrative or technical functions on behalf of the registrant. Instead, registrants should be provided with the option of providing contact details for persons other than themselves if they wish to delegate these functions and facilitate direct communication with the persons concerned. It should therefore be made clear, as part of the registration process, that the registrant is free to (1) designate the same person as the registrant (or its representative) as the administrative or technical contact; or (2) provide contact information which does not directly identify the administrative or technical contact person concerned (e.g. admin@company.com). For the avoidance of doubt, the EDPB recommends explicitly clarifying this within future updates of the Temporary Specification<sup>25</sup>”.

- The EPDP Team also took note of a related footnote which states, “[if contact details for persons other than the RNH are provided] it should be ensured that the individual concerned is informed”. The EPDP Team discussed whether this note implies that it is

---

<sup>25</sup> See <https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf>

sufficient for the Registered Name Holder (RNH) to inform the individual it has designated as the technical contact, or whether the registrar may have the additional legal obligations to obtain consent. The EPDP Team requested external legal counsel guidance on this topic and received the following summary answer:

“In cases where the RNH and the technical contact are not the same person, relying on the RNH to provide notice on the registrar's behalf will not meet GDPR's notice requirements if the RNH fails to provide the notice. While this may provide grounds for a contractual claim against the RNH, it is unlikely to provide a viable defence under the GDPR. Moreover, this arrangement will make it difficult for registrars to demonstrate that notice has been provided. If notice is not effectively provided, this could affect the legitimate interests analysis, since technical contacts may not "reasonably expect" the manner in which their data will be processed. If relying on consent, such an arrangement would make it difficult to document that consent has been provided”<sup>26</sup>.

- Noting some of the possible legal and technical challenges involved in collecting data from a third party, some (RySG, RrSG, NCSG) expressed the view that registrars should have the option, but should not be contractually required, to offer the RNH the ability to provide additional contact fields, e.g., technical function. Others (BC, IPC, ALAC, GAC and SSAC) expressed the view that registrars should be required to offer the RNH this ability, as making this optional could ultimately lead to risks to DNS stability, security and resiliency. The stakeholders supporting this view noted this functionality is considered important and desirable for some RNHs. The Team could not come to agreement on this issue and as such no recommendation is included in this Final Report in relation to whether optional also means, optional or required for the registrar to offer.
- All of the aforementioned input has been captured in the Discussion Summary Index for Appendix A which can be found here: <https://community.icann.org/x/ExxpBQ>.
- As a starting point, the EPDP examined data elements required to be collected today. The data elements workbooks in Annex D outline in detail which data elements are required to be collected for which purpose, and which data elements are optional for a Registered Name Holder to provide. Similarly, the data elements workbooks identify the applicable lawful basis. Processing activities identified as lawful under art. 6.1(b) are considered necessary for the performance of a contract (e.g., deliver the service of fulfilling a domain name registration).

---

<sup>26</sup> For further details, please see <https://mm.icann.org/pipermail/gnso-epdp-legal/2019-January/000034.html>.



**EPDP Team Recommendation #5.**

The EPDP Team recommends that the data elements listed below (as illustrated in the data elements workbooks in Annex D) are required to be collected by registrars. In the aggregate, this means that the following data elements are to be collected<sup>27</sup> where some data elements are automatically generated and, as indicated below, in some cases it is optional for the registered name holder to provide those data elements:

Data Elements (Collected & Generated*)	Collection Logic
Domain Name	Green
Registrar Whois Server*	
Registrar URL*	
Registrar Registration Expiration Date*	Yellow
Registrar*	Green
Registrar IANA ID*	
Registrar Abuse Contact Email*	
Registrar Abuse Contact Phone*	
Reseller*	Yellow
Domain Status(es)*	Green
Registrant Fields	1
• Name	Green
• Organization	
• Street	
• City	
• State/province	
• Postal code	
• Country	
• Phone	
• Phone ext	
• Fax	
• Fax ext	Yellow
• Email	
Tech Fields	1
• Name	Yellow
• Phone	
• Email	
Name Server(s)	Yellow

<sup>27</sup> For those data elements marked as “Optional”, these are either optional for the Registrar to offer or optional for the RNH to provide. In both cases, if data is provided, it must be processed

DNSSEC	
Name Server IP Address(es)	
<ul style="list-style-type: none"> <li>Additional data elements as identified by Registry Operator in its registration policy, such as (i) status as Registry Operator Affiliate or Trademark Licensee [.MICROSOFT]; (ii) membership in community [.ECO]; (iii) licensing, registration or appropriate permits (.PHARMACY, .LAW] place of domicile [.NYC]; (iv) business entity or activity [.BANK, .BOT]</li> </ul>	

Required   
 Optional 

For further details, see [complete data elements matrix](#).

For the purpose of the Technical contact, which is optional for the Registered Name Holder to complete (and if the Registrar provides this option), Registrars are to advise the Registered Name Holder at the time of registration that the Registered Name Holder is free to (1) designate the same person as the registrant (or its representative) as the technical contact; or (2) provide contact information which does not directly identify the technical contact person concerned.

**Note:**

In its most recent deliberations, the EPDP Team:

- decided that it would be optional for the registered name holder to provide: technical contact name, email, and phone number
- did not reach agreement on whether it would be optional or required for the registrar to offer the ability to the Registered Name Holder to provide these data elements,

The following groups expressed support for requiring registrars to provide the option for the RNH to provide tech contact data: IPC, BC, ALAC, SSAC, and GAC. The following groups expressed support for leaving it optional for registrars to provide the option for the RNH to provide tech contact data: RrSG, RySG and NCSG).

Please see the data element workbooks in Annex D for further detail in relation to the meaning of optional in the context of the different data elements.

**EPDP Team Recommendation #6.**  
 The EPDP Team recommends that, as soon as commercially reasonable, Registrar must provide the opportunity for the Registered Name Holder to provide its Consent to publish redacted contact information, as well as the email address, in the RDS for the sponsoring registrar.

### Charter Question

- c) Transfer of data from registrar to registry:
- c1) What data should registrars be required to transfer to the registry?
  - c2) What data is required to fulfill the purpose of a registry registering and resolving a domain name?
  - c3) What data is transferred to the registry because it is necessary to deliver the service of fulfilling a domain registration versus other legitimate purposes as outlined in part (a) above?
  - c4) Is there a legal reason why registrars should not be required to transfer data to the registries, in accordance with previous consensus policy on this point?
  - c5) Should registries have the option to require contact data or not?
  - c6) Is there a valid purpose for the registrant contact data to be transferred to the registry, or should it continue to reside at the registrar?

### EPDP Team considerations and deliberations in addressing the charter questions:

- For each of the Purposes for Processing Registration Data (above), the EPDP Team has identified where and which data is required to be transferred from the registrar to registry for the “Purposes” identified in response to charter question (a) as well as the identified corresponding lawful basis. As an illustration, please see the data elements workbooks in Annex D of this report for further details. Those processing activities identified as having a lawful basis under GDPR Art 6.1(b) were considered by the EPDP Team to be necessary for the performance of a contract, i.e., to deliver the service of fulfilling a domain registration.
- As part of this analysis, the EPDP Team has identified a set of data elements that are required to be transferred from the registrar to the registry in order to fulfill the Purposes for Processing Registration Data. This set of data elements constitutes an “aggregate minimum data set.” This is an aggregate minimum data set of all identified Purposes that registrars will be required to transfer to registries. This aggregate minimum data set also includes those data elements that MAY NOT be transferred from the registrar to the registry, where such a registry does not require such a transfer (with due regard to that registry’s terms, conditions, and policies).

### **EPDP Team Recommendation #7.**

The EPDP Team recommends that the specifically-identified data elements under “[t]ransmission of registration data from Registrar to Registry”, as illustrated in the aggregate data elements workbooks, must be transferred from registrar to registry provided an appropriate legal basis exists and data processing agreement is in place. In the aggregate, these data elements are:

Transfer of Data Elements from Registrar to Registry:

Data Elements (Collected & Generated*)	Transfer Logic
Domain Name	Green
Registrar Whois Server*	
Registrar URL*	
Registrar Registration Expiration Date*	Yellow
Registrar*	Green
Registrar IANA ID*	
Registrar Abuse Contact Email*	
Registrar Abuse Contact Phone*	
Reseller*	Yellow
Domain Status(es)*	Green
Registrant Fields	1
<ul style="list-style-type: none"> <li>• Name</li> </ul>	Yellow
<ul style="list-style-type: none"> <li>• Organization</li> </ul>	
<ul style="list-style-type: none"> <li>• Street</li> </ul>	
<ul style="list-style-type: none"> <li>• City</li> </ul>	
<ul style="list-style-type: none"> <li>• State/province</li> </ul>	
<ul style="list-style-type: none"> <li>• Postal code</li> </ul>	
<ul style="list-style-type: none"> <li>• Country</li> </ul>	
<ul style="list-style-type: none"> <li>• Phone</li> </ul>	
<ul style="list-style-type: none"> <li>• Phone ext</li> </ul>	
<ul style="list-style-type: none"> <li>• Fax</li> </ul>	
<ul style="list-style-type: none"> <li>• Fax ext</li> </ul>	
<ul style="list-style-type: none"> <li>• Email</li> </ul>	
Tech Fields	
<ul style="list-style-type: none"> <li>• Name</li> </ul>	Yellow
<ul style="list-style-type: none"> <li>• Phone</li> </ul>	
<ul style="list-style-type: none"> <li>• Email</li> </ul>	
Name Server(s)	
Name Server IP Address(es)	
<ul style="list-style-type: none"> <li>• Additional data elements as identified by Registry Operator in its registration policy, such as (i) status as Registry Operator Affiliate or Trademark Licensee [.MICROSOFT]; (ii) membership in community [.ECO]; (iii) licensing, registration or appropriate permits (.PHARMACY, .LAW) place of domicile [.NYC]; (iv) business entity or activity [.BANK, .BOT]</li> </ul>	Yellow

Required	
Optional	

For illustrative purposes, see [complete data elements matrix](#).

Charter Question

- d) Transfer of data from registrar/registry to data escrow provider:
  - d1) Should there be any changes made to the policy requiring registries and registrars to transfer the data that they process to the data escrow provider?
  - d2) Should there be any changes made to the procedures for transfer of data from a data escrow provider to ICANN Org?

EPDP Team considerations and deliberations in addressing the charter questions

- The EPDP Team considered both the input provided by each group in response to the triage surveys as well as the input provided by each group in response to the request for early input in relation to these questions.
- The EPDP Team considered Charter Question d1 and d2 in the context of the purpose to provide mechanisms for safeguarding Registered Name Holders' Registration Data and agreed that only data elements collected for other purposes identified herein and/or transferred from registrar to registry should be considered for escrow as those elements have been identified as necessary to meet the purpose.

**EPDP Team Recommendation #8.**

1. The EPDP Team recommends that ICANN Org enters into legally-compliant data protection agreements with the data escrow providers.
2. The EPDP Team recommends updates to the contractual requirements for registries and registrars to transfer data that they process to the data escrow provider to ensure consistency with the data elements listed below (for illustrative purposes, see relevant workbooks in Annex D that analyze the purpose to provide mechanisms for safeguarding Registered Name Holders' Registration Data).
3. The data elements to be transferred by Registries and Registrars to data escrow providers are:

For Registrars:

Data Elements (Collected & Generated*)	Collection Logic
Domain Name	
Registrar Registration Expiration Date*	
Registrar*	
Reseller*	

Registrant Fields	
• Name	
• Street	
• City	
• State/province	
• Postal code	
• Country	
• Phone	
• Phone ext	
• Fax	
• Fax ext	
• Email	
Tech Fields	
• Name	
• Phone	
• Email	

For Registries:

Data Elements (Collected & Generated*)	Collection Logic
Domain Name	
Registry Domain ID*	
Registrar Whois Server*	
Registrar URL*	
Updated Date*	
Creation Date*	
Registry Expiry Date*	
Registrar Registration Expiration Date*	
Registrar*	
Registrar IANA ID*	
Registrar Abuse Contact Email*	
Registrar Abuse Contact Phone*	
Reseller*	
Domain Status(es)*	
Registry Registrant ID*	
Registrant Fields	
• Name	
• Organization	
• Street	

• City	
• State/province	
• Postal code	
• Country	
• Phone	
• Phone ext	
• Fax	
• Fax ext	
• Email	
Tech ID*	
Tech Fields	1
• Name	
• Phone	
• Email	
Name Server(s)	
DNSSEC	
Name Server IP Address(es)	
• Additional data elements as identified by Registry Operator in its registration policy, such as (i) status as Registry Operator Affiliate or Trademark Licensee [.MICROSOFT]; (ii) membership in community [.ECO]; (iii) licensing, registration or appropriate permits (.PHARMACY, .LAW) place of domicile [.NYC]; (iv) business entity or activity [.BANK, .BOT]	

Required   
 Optional

Charter Question

- e) Transfer of data from registrar/registry to ICANN:
  - e1) Should there be any changes made to the policy requiring registries and registrars to transfer the domain name registration data that they process to ICANN Compliance, when required/requested?

EPDP Team considerations and deliberations in addressing the charter questions

- The EPDP Team discussed current requirements as well as future needs in relation to contractual compliance and consulted with the ICANN Compliance Team.

**EPDP Team Recommendation #9.**

1. The EPDP Team recommends that updates, if needed, are made to the contractual requirements concerning the registration data elements for registries and registrars to transfer to ICANN Org the domain name registration data that they process when required/requested for purpose 5 (Contractual Compliance). (Note: Current language within the Contracts currently provides the appropriate scope for contractual compliance requests and subsequent transfer (e.g. Art 2.11 new gTLD Base Registry Agreement) (For illustrative purposes, please see Annex D - contractual compliance monitoring requests, audits, and complaints submitted by Registry Operators, Registrars, Registered Name Holders, and other Internet users). Registrars and Registries are required to transmit to ICANN org any RDS elements that are requested for Purpose 5. To clarify, the data elements listed in Annex D are the aggregate of data elements that ICANN Compliance may request. As noted in the Summary of ICANN Organization’s Contractual Compliance Team Data Processing Activities “If the Contractual Compliance Team is unable to validate the issue(s) outlined in a complaint because the publicly available WHOIS data is redacted/masked, it will request the redacted/masked registration data directly from the contracted party (or its representative). In these instances, the Contractual Compliance Team will only request the redacted/masked data elements that are needed to validate the issue(s) outlined in the complaint”. Note, this recommendation does not exclude other information required by ICANN Contractual Compliance to enforce ICANN consensus policies and contracts.

## Charter Question

- f) Publication of data by registrar/registry:
  - f1) Should there be any changes made to registrant data that is required to be redacted? If so, what data should be published in a freely accessible directory?
  - f2) Should standardized requirements on registrant contact mechanism be developed?
  - f3) Under what circumstances should third parties be permitted to contact the registrant, and how should contact be facilitated in those circumstances?

## EPDP Team considerations and deliberations in addressing the charter questions

- The EPDP Team discussed which data elements are to be published in a freely accessible directory and which data elements are to be redacted. As a starting point, the EPDP Team considered the existing data-redaction list in the Temporary Specification (see Appendix A of the Temporary Specification). Although many agreed with the treatment (redaction vs. publication) of data-elements under the Temporary Specification, there was some disagreement as to whether the following elements should be treated differently, to either be redacted (as some believe they could contain personally identifiable information) or, in the alternative published, as described in greater detail below:
  - Organization,



- City, and
- Email Address.
- However, following review of the public comments received and further deliberation, the EPDP Team agreed to the following:

**EPDP Team Recommendation #10.**

Requirements for processing personal data in public RDDS where processing is subject to GDPR: The EPDP Team recommends that redaction must be applied as follows to the data elements that are collected. Data elements neither redacted nor anonymized must appear via free public based query access<sup>28</sup>:

Data Elements (Collected & Generated*)	Redacted	Disclosure Logic		
Domain Name	No	Green		
Registry Domain ID*	Yes			
Registrar Whois Server*	No			
Registrar URL*	No			
Updated Date*	No			
Creation Date*	No			
Registry Expiry Date*	No			
Registrar Registration Expiration Date*	No		Yellow	
Registrar*	No		Green	
Registrar IANA ID*	No			
Registrar Abuse Contact Email*	No			
Registrar Abuse Contact Phone*	No			
Reseller*	No			Yellow
Domain Status(es)*	No			Green
Registry Registrant ID*	Yes			
Registrant Fields	1		1	
• Name	Yes	Green		
• Organization	Yes			
• Street	Yes			
• City	Yes <sup>29</sup>			
• State/province	No			
• Postal code	Yes			
• Country	No			

<sup>28</sup> As noted in the data elements workbooks, “a minimum public data set of registration data will be made available for query of gTLD second level domains in a freely accessible directory. Where a data element has been designated as non-public, it will be redacted”.

<sup>29</sup> See recommendation #11 for further details

• Phone	Yes	Green
• Email	Yes	
Tech ID*	Yes	
Tech Fields		
• Name	Yes	Green
• Phone	Yes	
• Email	Yes	
Name Server(s)	No	Yellow
DNSSEC	No	
Name Server IP Address(es)	No	
Last Update of Whois Database*	No	

Required

Optional



The EPDP Team also confirms that, where GDPR is not applicable, Registry Operator and Registrar MAY apply the requirements outlined in this recommendation, as well as recommendation #12, #13, #14 and #15 (i) where it has a commercially reasonable purpose to do so, or (ii) where it is not technically feasible to limit application of these requirements.

- The EPDP Team requested external legal counsel guidance in relation to the topic of city field, is this considered personal data and must it be redacted or is there a lawful basis for publishing this information, and received the following summary answer:

“The legal analysis is clear – this is personal data; *in principle* publication could be justified on the basis of rights-holders legitimate interests, unless the interests of individuals override this.

How this is applied to the facts – establishing whether there is sufficient interest for rights holders and balancing this with the interests of registered name holders - is not clear cut.”<sup>30</sup>

<sup>30</sup> For further details, please see <https://mm.icann.org/pipermail/gnso-epdp-legal/2019-February/000053.html>.

**EPDP Team Recommendation #11.**

The EPDP Team recommends that redaction must be applied as follows to this data element:

Data Element	Redacted
Registrant Field	
<ul style="list-style-type: none"> <li>City</li> </ul>	Yes

The EPDP Team expects to receive further legal advice on this topic which it will analyze in phase 2 of its work to determine whether or not this recommendation should be modified.

**EPDP Team Recommendation #12.**

The EPDP Team recommends that:

- The Organization field will be published if that publication is acknowledged or confirmed by the registrant via a process that can be determined by each registrar. If the registered name holder does not confirm the publication, the Organization field can be redacted or the field contents deleted at the option of the registrar.
- The implementation will have a phase-in period to allow registrars the time to deal with existing registrations and develop procedures.
- In the meantime, registrars will be permitted to redact the Organization Field.
- A registry Operator, where they believe it feasible to do so, may publish or redact the Org Field in the RDDS output.

**Implementation advice:** the implementation review team should consider the following implementation model discussed by the EPDP Team:

For existing registrations, the first step will be to confirm the correctness / accuracy of the existing Organization field data.

For the period between the adoption of EPDP policy recommendations and the conclusion of the implementation effort set for on, or before, 29 February 2020:

- 1) Registrars will redact the Organization field
- 2) Registrars will contact the registered name holders that have entered data in the Organization field and request review and confirmation that the data is correct.
  - a) If the registered name holder confirms or corrects the data will remain in the Organization field.
  - b) If the registrant declines, or does not respond to the query, the Registrar may redact the Organization field, or delete the field contents. If necessary, the registration will be re-assigned to the Registered Name Holder.
- 3) If Registrar chooses to publish the Registrant Organization field, it will notify these registered name holders that of the “date certain,” the Organization field will be treated as non-personal data and be published, for those Registered Names Holders who have confirmed the data and agreed to publication.

For new registrations, beginning with the “date certain”:

- 1) New registrations will present some disclosure, disclaimer or confirmation when data is entered in the Organization field. Registrars are free to develop their own process (e.g., opt-in, pop-up advisory or question, locked/grayed out field).
- 2) If the registered name holder confirms the data and agrees to publication:
  - a) The data in the Organization field will be published,
  - b) The Organization will be listed as the Registered Name Holder.
  - c) The name of the registered name holder (a natural person) will be listed as the point of contact at the Registrant Organization.

After the implementation phase-in period, the ORG FIELD will no longer be REDACTED by the registrar, unless registered name holder has not agreed to publication.

Note, this is a Registrar obligation. For a Registry to publish is optional, until such time a way has been found that allows for the transfer of consent from Registrar to Registry.

**EPDP Team Recommendation #13.**

1) The EPDP Team recommends that the Registrar MUST provide an email address or a web form to facilitate email communication with the relevant contact, but MUST NOT identify the contact email address or the contact itself, unless as per Recommendation #6, the Registered Name Holder has provided consent for the publication of its email address.

2) The EPDP Team recommends Registrars MUST maintain Log Files, which shall not contain any Personal Information, and which shall contain confirmation that a relay of the communication between the requestor and the Registered Name Holder has occurred, not including the origin, recipient, or content of the message. Such records will be available to ICANN for compliance purposes, upon request. Nothing in this recommendation should be construed to prevent the registrar from taking reasonable and appropriate action to prevent the abuse of the registrar contact process.<sup>31</sup>

Note: in relation to 1), this matches the requirements in Section 2.5.1 of Appendix A to the Temporary Specification.

Note: The EPDP notes operational difficulties having to do with contacting registered name holders through webforms (where there is no confirmation that the message sent was received) and pseudonymized email addresses. Therefore, the registrar cannot be reasonably expected to confirm, or attempt to confirm by any means, the receipt of any such relayed communication. The EPDP notes that the GNSO Council may choose to consider

---

<sup>31</sup> Examples of abuse could include, but are not limited to, requestors purposely flooding the registrar’s system with voluminous and invalid contact requests. This recommendation is not intended to prevent legitimate requests.

further work on a potential method for safely and reliably contacting registrants in cases where their email cannot be displayed.

Note: Recommendation 3 of the EPDP Team’s Final Report specifically provides that the EPDP Team’s work shall not affect the accuracy of registration data under the current ICANN contracts and consensus policies. Accordingly, registrars are still required to reverify a registered name holder’s email address if the registrar receives information suggesting that the contact information is incorrect. This would include a bounced email notification or non-delivery notification message in response to a registrar-initiated communication. This requirement can be found in paragraph 4 of the Whois Accuracy Program Specification in the Registrar Accreditation Agreement.

**EPDP Team Recommendation #14.**

In the case of a domain name registration where an "affiliated"<sup>32</sup> privacy/proxy service used (e.g. where data associated with a natural person is masked), Registrar (and Registry where applicable) MUST include in the public RDDS and return in response to any query full non-personal RDDS data of the privacy/proxy service, which MAY also include the existing privacy/proxy pseudonymized email.

Note, PPSAI is an approved policy that is currently going through implementation. It will be important to understand the interplay between the display of information of affiliated vs. accredited privacy / proxy providers. Based on feedback received on this topic from the PPSAI IRT, the EPDP Team may consider this further in phase 2.

Charter Question

g) Data retention:

- g1) Should adjustments be made to the data retention requirement (life of the registration + 2 years)?
- g2) If not, are changes to the waiver process necessary?
- g3) In light of the EDPB letter of 5 July 2018, what is the justification for retaining registration data beyond the term of the domain name registration?

EPDP Team considerations and deliberations in addressing the charter questions

- In addition, the EPDP Team reviewed the feedback that the European Data Protection Board provided in relation to data retention and took specific note of the following:

“personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (article 5(2) GDPR). This is a matter which has

---

<sup>32</sup> As defined in the [Registrar Accreditation Agreement, Specification on Privacy and Proxy Registrations](#): “For any Proxy Service or Privacy Service offered by the Registrar or its Affiliates, including any of Registrar's or its Affiliates' P/P services distributed through Resellers, and used in connection with Registered Names Sponsored by the Registrar, the Registrar and its Affiliates”.

already been addressed repeatedly by both the WP29 and the EDPS.<sup>19</sup> It is for ICANN to determine the appropriate retention period, and it must be able to demonstrate why it is necessary to keep personal data for that period. So far ICANN is yet to demonstrate why each of the personal data elements processed in the context of WHO IS must in fact be retained for a period of 2 years beyond the life of the domain name registration. The EDPB therefore reiterates the request ICANN to re-evaluate the proposed retention period of two years and to explicitly justify and document why it is necessary to retain personal data for this period in light of the purposes pursued”<sup>33</sup>.

- For each of the purposes, the EPDP Team has identified in the data elements workbooks in Annex D the desired data retention period, including a rationale for why data needs to be retained for that period.

**EPDP Team Recommendation #15.**

1. In order to inform its Phase 2 deliberations, the EPDP team recommends that ICANN Org, as a matter of urgency, undertakes a review of all of its active processes and procedures so as to identify and document the instances in which personal data is requested from a registrar beyond the period of the 'life of the registration'. Retention periods for specific data elements should then be identified, documented, and relied upon to establish the required relevant and specific minimum data retention expectations for registrars. The EPDP Team recommends community members be invited to contribute to this data gathering exercise by providing input on other legitimate purposes for which different retention periods may be applicable.
2. In the interim, the EPDP team has recognized that the Transfer Dispute Resolution Policy (“TDRP”) has been identified as having the longest justified retention period of one year and has therefore recommended registrars be required to retain only those data elements deemed necessary for the purposes of the TDRP, for a period of fifteen months following the life of the registration plus three months to implement the deletion, i.e., 18 months<sup>34</sup>. This retention is grounded on the stated policy stipulation within the TDRP that claims under the policy may only be raised for a period of 12 months after the alleged breach (FN: see TDRP section 2.2) of the Transfer Policy (FN: see Section 1.15 of TDRP). This retention period does not restrict the ability of registries and registrars to retain data elements provided in Recommendations 4 -7 for other purposes specified in Recommendation 1 for shorter periods.<sup>35</sup>

<sup>33</sup> See <https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf>

<sup>34</sup> Even though the TDRP provides for a 12 month period to file a complaint, the data is to be retained for an additional three months to ensure that TDRP complaints that are filed at the end of the 12 month period can be addressed.

<sup>35</sup> In Phase 2, the EPDP Team will work on identifying different retention periods for any other purposes, including the purposes identified in this Report.

3. The EPDP team recognizes that Contracted Parties may have needs or requirements for different retention periods in line with local law or other requirements. The EPDP team notes that nothing in this recommendation, or in separate ICANN-mandated policy, prohibits contracted parties from setting their own retention periods, which may be longer or shorter than what is specified in ICANN policy.
4. The EPDP team recommends that ICANN Org review its current data retention waiver procedure<sup>36</sup> to improve efficiency, request response times, and GDPR compliance, e.g., if a Registrar from a certain jurisdiction is successfully granted a data retention waiver, similarly-situated Registrars might apply the same waiver through a notice procedure and without having to produce a separate application.

#### Charter Question

##### h) Applicability of Data Processing Requirements

- h1) Should Registry Operators and Registrars (“Contracted Parties”) be permitted or required to differentiate between registrants on a geographic basis?
- h2) Is there a legal basis for Contracted Parties to differentiate between registrants on a geographic basis?
- h3) Should Contracted Parties be allowed or required to treat legal and natural persons differently, and what mechanism is needed to ensure reliable determination of status?
- h4) Is there a legal basis for Contracted Parties to treat legal and natural persons differently?
- h5) What are the risks associated with differentiation of registrant status as legal or natural persons across multiple jurisdictions? (See EDPB letter of 5 July 2018).

#### EPDP Team considerations and deliberations in addressing the charter questions

- In relation to charter question h1, the EPDP Team agrees that contracted parties should be (and are) *permitted* to differentiate between registrants on a geographic basis; however, the EPDP Team members have divergent views on whether differentiation on a geographic basis should be required.
- The EPDP Team considered the public comment and developed the following thoughts in its deliberations in addressing the charter questions:
  - The EPDP Team discussed this extensively (as documented in the Initial Report) as well as in the context of the review on the public comments received on the Initial Report. In relation to part of charter question h1, the EPDP Team agrees that contracted parties should be (and are) permitted to differentiate between registrants on a geographic basis;
  - However, the EPDP Team members have divergent views on whether differentiation on a geographic basis should be required.

---

<sup>36</sup> For avoidance of doubt, ICANN’s data retention waiver procedure only applies to contracted parties who need to apply for shorter data retention periods. Contracted parties do not need to seek a waiver for longer retention periods for data retention under their own controllership.

- Recognizing that ICANN is a Data Controller in many scenarios and that ICANN may be considered “established” in Europe (within the meaning of the GDPR), the EPDP Team discussed whether those factors would have an effect upon the discussion and determining GDPR-compliant outcomes. It became clear that legal guidance in relation to the applicability of GDPR in the context of ICANN having an ‘establishment’ in Europe could further inform requirements.
- The EPDP Team also discussed the possibility of developing a set of rules for guiding the making of geographical distinctions in an GDPR-compliant manner (akin to the EWG hypothesized “rules engine”). The Team agreed that creating this set of rules was a complex task (just as it would be for individual registrars) and agreed such development could not occur within the remit of this Phase I EPDP. Such a development would also be dependent on the response to the aforementioned legal guidance.
- The EPDP Team discussed Charter Question h3, namely, should Contracted Parties be allowed or required to treat legal and natural persons differently, and what mechanism is needed to ensure reliable determination of status? In determining the answer to this question, the EPDP Team sought the guidance of external legal counsel, inquiring specifically, “If a registrar permits a registrant, at the time of domain name registration, to self-identify as a natural or legal person, does a registrant’s incorrect self-identification that results in the public display of personal data create liability under GDPR? If so, please advise, for each possible participant in the domain name registration process listed below, if that participant incurs liability.” External legal counsel provided the following summary answer:

“We conclude that the relevant parties could be subject to liability if a registrant wrongly self-identifies as a legal person (and not a natural person) and the registrant's data is disclosed in reliance on this self-identification. To reduce the risks, we propose several solutions, such as focus group testing of the registration process to minimise the risk of errors and technical tools (if feasible) to verify the information provided. We also recommend providing clear notice to data subjects of the consequences for them of the designation as either a legal or a natural person as well as a way for data subjects to easily correct a mistaken classification. One way to do this effectively would be to send a follow-up email after registration to the listed contacts – this could also help with the notice issue addressed in question 1<sup>37</sup>.”

- Factoring in the different positions on these questions as outlined in the Initial Report and considering the input received to the questions outlined in the Initial Report, the

---

<sup>37</sup> For further details, see <https://mm.icann.org/pipermail/gnso-epdp-legal/2019-January/000034.html>



EPDP Team is putting forward the following recommendations in response to the charter questions.

**EPDP Team Recommendation #16. (Divergence)**

The EPDP Team recommends that Registrars and Registry Operators are permitted to differentiate between registrants on a geographic basis, but are not obligated to do so.

**EPDP Team Recommendation #17.**

- 1) The EPDP Team recommends that Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so.
- 2) The EPDP Team recommends that as soon as possible ICANN Org undertakes a study, for which the terms of reference are developed in consultation with the community, that considers:
  - The feasibility and costs including both implementation and potential liability costs of differentiating between legal and natural persons;
  - Examples of industries or other organizations that have successfully differentiated between legal and natural persons;
  - Privacy risks to registered name holders of differentiating between legal and natural persons; and
  - Other potential risks (if any) to registrars and registries of not differentiating.
- 3) The EPDP Team will determine and resolve the Legal vs. Natural issue in Phase 2.

- i) Transfer of data from registry to Emergency Back End Registry Operator (“EBERO”)
  - i1) Consider that in most EBERO transition scenarios, no data is actually transferred from a registry to an EBERO. Should this data processing activity be eliminated or adjusted?

EPDP Team considerations and deliberations in addressing the charter questions

- While most EBERO transition scenarios may not involve the transfer of registration data, the EPDP Team documented this processing activity in order to comprehensively account for all relevant processing activities. In reviewing processing activities associated with EBERO, the EPDP Team noted that the EBERO process invokes the registry escrow process. Specifically, Section 2.3 and Specification 2 of the Registry Agreement refer to the Escrow Format Specification, which specifically mentions “such as domains, contacts, name servers, etc[.]” The EPDP Team concluded that no other registration data is processed under other components of the EBERO process. Thus, a separate workbook specifically for EBERO was not created because the Registry Escrow purpose (see Workbook E-Ry) documents the transfer of data within the processing activities section of the workbook.

## Charter Question

## j). Temporary Specification and Reasonable Access

- j1) Should existing requirements in the Temporary Specification remain in place until a model for access is finalized?
1. If so:
    1. Under Section 4 of Appendix A of the Temporary Specification, what is meant by “reasonable access” to Non-Public data?
    2. What criteria must Contracted Parties be obligated to consider in deciding whether to disclose non-public Registration data to an outside party requestor (i.e. whether or not the legitimate interest of the outside party seeking disclosure are overridden by the interests or fundamental rights or freedoms of the registrant)?
  2. If not:
    1. What framework(s) for disclosure could be used 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, and (iii) provide access to registration data based on legitimate interests not outweighed by the fundamental rights of relevant data subjects?
- j2) Can the obligation to provide “reasonable access” be further clarified and/or better defined through the implementation of a community-wide model for access or similar framework which takes into account at least the following elements:
1. What outside parties / classes of outside parties, and types of uses of non-public Registration Data by such parties, fall within legitimate purposes and legal basis for such use?
  2. Should such outside parties / classes of outside parties be vetted by ICANN in some manner and if so, how?
  3. If the parties should not be vetted by ICANN, who should vet such parties?
  4. In addition to vetting the parties, either by ICANN or by some other body or bodies, what other safeguards should be considered to ensure disclosure of Non-Public Personal Data is not abused?
- The intent of the recommendation hereunder is to provide clarity around the process and expectations of reasonable lawful disclosure in terms of making requests. The recommendation attempts to ensure that expectations are set for how to submit requests and in what fashion those requests will be handled once received. The Recommendation does NOT assume that disclosure will be made and, further, it is not contemplated how and on what basis a decision for disclosing (or not) will be made. Those issues are expected to be dealt with in Phase 2 of the EPDP Team’s work.

**EPDP Team Recommendation #18.**

The EPDP Team recommends that the current requirements in Sections 4.1 and 4.2 of Appendix A to the Temporary Specification in relation to access to non-public registration data, upon expiration are replaced with the criteria below and finalized through the requirements set during the implementation stage, recognizing that work in Phase 2 on a system for Standardized Access to Non-Public Registration Data may further complement, revise, or supersede these requirements. In addition, the EPDP team recommends that when a system for Standardized Access to Non-Public Registration Data is developed, the need for a policy governing Reasonable Requests for Lawful Disclosure outside of that model will be required.

The EPDP Team recommends that the new policy will refer to “Reasonable Requests for Lawful Disclosure of Non-Public Registration Data” or “Reasonable Requests for Lawful Disclosure”, instead of ‘Reasonable Access’ and that Registrar and Registry Operator must process and respond to Reasonable Requests for Lawful Disclosure.

The basic criteria for Reasonable Requests Lawful Disclosure are as follows: First, a Reasonable Request for Lawful Disclosure must follow the format required by the Registrar or Registry Operator and provide the required information, which are to be finalized during the implementation phase (see below). Second, delivery of a properly-formed Reasonable Request for Lawful Disclosure to a Registrar or Registry Operator does NOT require automatic disclosure of information. Third, Registrars and Registry Operators will consider each request on its merits, including the asserted GDPR legal bases.

Registrars and Registry Operators must publish, in a publicly accessible section of their website, the mechanism and process for submitting Reasonable Requests for Lawful Disclosure. The mechanism and process should include information on the required format and content of requests, means of providing a response, and the anticipated timeline for responses.

The EPDP Team recommends that criteria for a Reasonable Request for Lawful Disclosure and the requirements for acknowledging receipt of a request and response to such request will be defined as part of the implementation of these policy recommendations but will include at a minimum:

- Minimum Information Required for Reasonable Requests for Lawful Disclosure:
- Identification of and information about the requestor (including, the nature/type of business entity or individual, Power of Attorney statements, where applicable and relevant);
- Information about the legal rights of the requestor and specific rationale and/or justification for the request, (e.g. What is the basis or reason for the request; Why is it necessary for the requestor to ask for this data?);
- Affirmation that the request is being made in good faith;

- A list of data elements requested by the requestor and why this data is limited to the need;
- Agreement to process lawfully any data received in response to the request.
- Timeline & Criteria for Registrar and Registry Operator Responses - Registrars and Registries must reasonably consider and accommodate requests for lawful disclosure:
  - Response time for acknowledging receipt of a Reasonable Request for Lawful Disclosure. Without undue delay, but not more than two (2) business days from receipt, unless shown circumstances does not make this possible.
  - Requirements for what information responses should include. Responses where disclosure of data (in whole or in part) has been denied should include: rationale sufficient for the requestor to understand the reasons for the decision, including, for example, an analysis and explanation of how the balancing test was applied (if applicable).
  - Logs of Requests, Acknowledgements and Responses should be maintained in accordance with standard business recordation practices so that they are available to be produced as needed including, but not limited to, for audit purposes by ICANN Compliance;
  - Response time for a response to the requestor will occur without undue delay, but within maximum of 30 days unless there are exceptional circumstances. Such circumstances may include the overall number of requests received. The contracted parties will report the number of requests received to ICANN on a regular basis so that the reasonableness can be assessed.
  - A separate timeline of [less than X business days] will 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].

The EPDP Team recommends that the above be implemented and further work on defining these criteria commences as needed and as soon as possible.

### Part 3: Data Processing Terms

- k) ICANN's responsibilities in processing data
  - k1) For which data processing activities undertaken by registrars and registries as required by the Temporary Specification does ICANN determine the purpose and means of processing?
  - k2) In addition to any specific duties ICANN may have as data controller, what other obligations should be noted by this EPDP Team, including any duties to registrants that are unique and specific to ICANN's role as the administrator of policies and contracts governing gTLD domain names?

- l) Registrar's responsibilities in processing data
- l1) For which data processing activities required by the Temporary Specification does the registrar determine the purpose and means of processing?
  - l2) Identify a data controller and data processor for each type of data.
  - l3) Which registrant data processing activities required by the Temporary Specification do registrars undertake solely at ICANN's direction?
  - l4) What are the registrar's responsibilities to the data subject with respect to data processing activities that are under ICANN's control?
- m) Registry's responsibilities in processing data
- m1) For which data processing activities required by the Temporary Specification does the registry determine the purpose and means of processing?
  - m2) Which data processing activities required by the Temporary Specification does the registry undertake solely at ICANN's direction?
  - m3) Are there processing activities that registries may optionally pursue?
  - m4) What are the registry's responsibilities to the data subject based on the above?

#### EPDP Team considerations and deliberations in addressing the charter questions

- Through its work on the data elements workbooks, the EPDP Team has identified for illustrative purposes the following for each of the purposes: (1) responsible party/parties, and (2) which party/parties is/are involved in the relevant processing steps, see Annex D.
- Some members of the EPDP Team considered whether the identification of Data Controllers & Processors or other recommendations in this report could have an impact on "No Third-Party Beneficiary" clauses in existing ICANN Contracted Party agreements and whether it should be made clear that this may not be the intention.
- The EPDP Team took note of the GDPR requirements and notes that in instances where the EPDP Team has classified ICANN as a Controller, ICANN would be expected to comply with the law. However, the EPDP Team is not recommending additional requirements for ICANN at this time.
- Similarly, the EPDP Team took note of the GDPR requirements and notes that in instances where the EPDP Team has classified Registries and Registrars as Controllers, or Processors, the Registry and/or Registrar would be expected to comply with the law. However, the EPDP Team is not recommending additional requirements for contracted parties at this time.
- The EPDP Team asked two questions about the application of Article 6(1)b to external legal counsel:
  - a) Does the reference 'to which the data subject is party' limit the use of this lawful basis only to those entities that have a direct contractual relationship with the Registered Name Holder?
  - b) Does "necessary for the performance of a contract" relate solely to the registration and activation of a domain, or, alternatively, could related activities such as fighting DNS abuse also be considered necessary for the performance of a contract?

External legal counsel provided the following summary answers:

“a) it is not clear if the contractual necessity condition can only apply where there is a contract between data controller and data subject, or whether the contract could be between another person and the data subject. (For example, so that ICANN or a registry could argue that their processing is necessary for the contract between the registrar and the RNH/data subject). In countries where we have checked, there are no cases on point. Some data protection authorities interpret the provision narrowly. However, there is also guidance arguing for a more liberal approach. We think a more liberal approach is correct – but this is untested.

b) What is 'necessary' is interpreted strictly. We do not think that the EPDP could successfully argue that preventing DNS abuses is 'necessary' for the contract with the RNH. There is guidance from the Article 29 Working Party on this which has examples somewhat similar to ICANN's situation”.<sup>38</sup>

### **Processors, Controllers, Co-Controllers and Joint Controllers**

Controller is the person or entity, that alone or jointly with others, determines the purpose and means of processing. Processing, in turn is “*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*”.

Pursuant to Art. 4 no. (7) GDPR “controller” means the natural or legal person, public authority, agency or other body which, **alone or jointly with others**, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

In situations where two or more controllers “jointly” determine the purposes and means of processing, Art. 26 GDPR specifies additional requirements that apply (“Joint Controller”).

In contrast to controllers, processors do not have the right to make decisions with regard to the purposes and means of processing, but act for the contractor (controller) with a duty to comply with the controller(s)' instructions.

---

<sup>38</sup> For further details, please see <https://mm.icann.org/pipermail/gnso-epdp-legal/2019-January/000035.html>.

Processors can be afforded some discretion in deciding on the means of processing, whereas a determination of the purposes of processing is usually a function reserved to controllers.<sup>39</sup>

The purpose of processing is an “expected result that is intended or guides planned actions”. The means of processing is the “type and manner in which a result or objective is achieved”<sup>40</sup>.

Processors are distinguished from [joint] controllers based on the following criteria:

- A person or entity that has no legal or factual influence on the decision concerning the purposes for and manner in which personal data is processed cannot be a controller.
- A person or entity that alone or jointly with others decides on the purposes of processing is always a controller.
- The controller may also delegate the decision(s) concerning the means of processing to the processor, but the controller cannot delegate the “essential elements which are traditionally and inherently reserved to the determination of the controller, such as ‘which data shall be processed?’, ‘for how long shall they be processed?’ ‘who shall have access to them?’, and so on.”.
- Processors are independent legal persons who are different from the controller and who process data on behalf of the controller(s) without deciding on the purposes of processing.<sup>41</sup>

Where two or more different organizations jointly determine the purposes or the essential elements of the means of the processing they will be joint controllers and must enter into an agreement as required by Art. 26 of the GDPR. The participation of the parties to the joint determination may take different forms and does not need to be equally shared. Jointly must interpreted “as meaning ‘together with’ or ‘not alone’ in different forms and combinations” and “the assessment of joint control should mirror the assessment of ‘single’ control”. Therefore, it cannot be assumed that ICANN and the contracted parties are co-controllers for the processing of data, rather than joint controllers. A co-controllership would require two or more parties which are completely independent of one another, co-operatively working together in the processing of data but for different purposes.

ICANN and the EPDP Charter Questions and How the Above Principles are Applied Herein

---

<sup>39</sup> *Klabundein Ehmann/Selmayr*, „Datenschutz-Grundverordnung“ Art.4 marg. no. 29

<sup>40</sup> Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 16, available at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\\_de.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf)

<sup>41</sup> Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 18, 39, 40, available at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\\_de.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf)

As discussed below, the processing of registration data is covered by the overarching purpose of the registration of a domain name by all three parties in this process.

#### Purpose of Art. 26 GDPR

The regulation is to primarily protect of the rights and freedoms of data subjects.<sup>42</sup> This document is intended to address the clear allocation of responsibilities in relation to ensure the rights of data subjects. In more complex role allocations, e.g. in the area of domain registration with several distribution levels, the data subject's right of access and other rights are to be guaranteed across levels.<sup>43</sup>

"The definition of the term "processing" listed in Article 2 lit. b of the guideline does not exclude the option that diverse actors participate in diverse operations or sets of operations in connection with personal data. These operations can be executed simultaneously or in diverse stages. In such a complex environment it is even more important that roles and responsibilities are allocated to ensure that the complexity of joint control does not result in an impractical division of responsibility that would affect the effectiveness of data protection law."<sup>44</sup>

Recital 79 GDPR furthermore clarifies that the regulation is to simplify monitoring by the supervisory authorities.

The factual control of the data processing, as well as control over external effects vis-à-vis the data subject, is determinative when reviewing responsibility.

Furthermore, processing should not be artificially divided into smaller processing steps, but can be uniformly considered as a set of operations. In this respect, data collection, passing on to the registry, review and implementation and ongoing management of the registration can be considered as one set of "domain registration" operations, because it pursues the overall purpose of registering the domain for a new registrant. This also applies if diverse agencies pursue different purposes within the processing chain, when engaged in the detail of smaller processing steps on a micro level. On a macro level, the same purpose is pursued overall with all small steps in the chain, so that a uniform set of operations specifically applies here (Art.29 Group WP 169, p. 25).

Differentiation is required when considering the operation of collecting and processing the data collected by the registrar from its customers in order to create an invoice, to maintain a customer account, and to manage the contractual relationship with its customers. This data fulfils another purpose that is not codetermined by the registry and ICANN.

Further analysis should be carried out to determine, for the table below, which processing activities are determined jointly and which are not.

---

<sup>42</sup> Bertmannin Ehmann/Selmayr "Datenschutz-Grundverordnung" Art. 26, marg. no. 1

<sup>43</sup> Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 27, available at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\\_de.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf)

<sup>44</sup> Art. 29 Data Protection Working Party, Statement 1/2010 of 16 February 2010, p. 22, available at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169\\_de.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf)



This also corresponds to the legislative intent to have clear and simple regulations concerning responsibility in case of multiple participants and complex processing structures, and to prevent a splitting of responsibilities to protect the data subjects as far as possible.

Pursuant to Article 1 Section 1.1 of the ICANN bylaws, ICANN has responsibility:

*“to ensure the stable and secure operation of the Internet's unique identifier systems as described in this Section 1.1(a) (the "**Mission**"). Specifically, ICANN:*

*(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System ("**DNS**") and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("**gTLDs**"). In this role, ICANN's scope is to coordinate the development and implementation of policies:*

- For which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS including, with respect to gTLD registrars and registries, policies in the areas described in Annex G-1 and Annex G-2;”*

As already stated, ICANN fulfils this responsibility among other things by contractually specifying for the various participants the data which must mandatorily be collected and retained. With these legitimate provisions, ICANN specifies a purpose for the processing operation overall and thus becomes joint controller in addition to registry and registrar. It should be noted that ICANN's responsibility is unaffected by the fact that certain requirements have been decided upon by multiple stakeholders or have determined and put into effect through a community effort. Such joint discussion or drafting of certain policies or requirements does not place ICANN in a role as the entity ultimately requiring the contracted parties to act in accordance with the policies issued by ICANN.

#### Joint and several liability

Irrespective of joint control, if two or more controllers are involved in the “same” processing then there will be joint and several liability unless a party can provide it is not responsible for the event giving rise to the damage (Art. 82). The factual responsibility may be adjusted only *inter parties*. Therefore, having clear allocations between the parties is even more important *inter parties*.

#### Fines

However, such joint and multiple liability may not apply to fines under Art. 83 (4) lit. a) GDPR. In this respect, registry and registrar are liable pursuant to their role allocation for breaches in their area or against duties under the GDPR, which were incumbent upon them within the scope of the contractual basis.

### Joint Controller Agreement

Joint controllers must furthermore specify, in a transparent form, who fulfills which duties vis-à-vis the data subjects, as well as who the contact point for data subject's rights is (Art. 26 (1) p. 2 GDPR).

However, the data subject is authorized to address any of the participating responsible agencies to assert its rights, regardless of the specification concerning competence (Art. 26 (3) GDPR).

The agreement is to regulate the specific controllers that are to fulfill the duties prescribed by GDPR. Pursuant to Recital 79 GDPR, the following must be specifically regulated in a transparent form:

- how the relations and functions of the controllers among each other are designed,
- how roles are distributed between controllers to fulfill data subject rights of registrants,

Article 26 permits the parties to allocate responsibility for providing notice to the party best able to fulfill the obligation. However, Art. 26 GDPR suggests that multiple controllers fulfill information obligations centrally. Details shall be agreed upon between the parties.

Therefore, in relation to the above, as described, the EPDP, has set forth within the Initial Report, the Responsibility of each named party in relation to the specified Purposes, listed and based on the legal basis recommendations, for the respective Purpose and in relation to its duties performed for the data subject.

In relation to Preliminary Recommendation #13 below, the EPDP Team understands that relationship between ICANN Org, Registries and Registrars requires work at a greater level of granularity than in this report. During the further work of the EPDP and negotiations that will subsequently take place between the Registries, Registrars and ICANN in relation to memorializing the relationship between the parties for various processing activities the parties shall conduct a detailed review of the individual processing activities and the actions to be taken by the respective parties to determine if there is joint control and the scope of any joint control; and b) (irrespective of joint control) to allocate responsibility. If there is joint control, then any agreement shall meet the requirements of Art. 26 sec 2 of the GDPR (including a document being made to data subjects), which specifies:

"The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject."

A clear demarcation the processing activities covered by the agreement versus those carried out by either party outside the scope of the agreement shall be documented.

The agreement shall recognize that parties are currently using third parties' services or otherwise work with third parties, such as

- Data Escrow Agents
- EBEROs
- Registry Service Providers
- Registrar as a Service Providers
- Resellers
- Dispute Resolution Providers
- the TMCH.

This may or may not include processing of personal data by those third parties. Where personal data is processed by third parties, the respective agreement will need to ensure that the data processing is carried out in a way compliant with GDPR. However, conditional to GDPR compliance, nothing in the agreement shall prevent the respective parties from engaging third parties and entering into the required agreements without further authorizations from the other parties.

**EPDP Team Recommendation #19.**

The EPDP Team recommends that ICANN Org negotiates and enters into required data protection agreements, as appropriate, with the Contracted Parties. In addition to the legally required components of such agreement, the agreement shall specify the responsibilities of the respective parties for the processing activities as described therein. Indemnification clauses should ensure that the risk for certain data processing is borne, to the extent appropriate, by the parties that are involved in the processing. Due consideration should be given to the analysis carried out by the EPDP Team in its Final Report.

**EPDP Team Recommendation #20.**

During Phase 1 of its work, the EPDP Team documented the data processing activities and responsible parties associated with gTLD registration data. The EPDP Team, accordingly, recommends the inclusion of the data processing activities and responsible parties, outlined below, to be confirmed and documented in the relevant data protection agreements, noting, however, this Recommendation may be affected by the finalization of the necessary agreements that would confirm and define the roles and responsibilities.

**ICANN PURPOSE<sup>45</sup>:**

As subject to Registry and Registrar terms, conditions and policies, and ICANN Consensus Policies:

<sup>45</sup> The term ICANN Purpose is used to describe purposes for processing personal data that should be governed by ICANN Org via a Consensus Policy. Note there are additional purposes for processing personal data, which the contracted parties might pursue, but these are outside of what ICANN and its community should develop policy on or contractually enforce. It does not necessarily mean that such purpose is solely pursued by ICANN org.

- To establish the rights of a Registered Name Holder in a Registered Name; to ensure that a Registered Name Holder may exercise its rights in the use and disposition of the Registered Name; and
- To activate a registered name and allocate it to a Registered Name Holder.

<b>Processing Activity</b>	<b>Responsible Party<sup>46</sup>:</b>	<b>Lawful Basis<sup>47</sup>:</b>
<b>Collection</b>	ICANN Registrars Registries	6(1)(b) for Registrars 6(1)(f) for ICANN and Registries
<b>Transmission from Rr to Ry</b>	Registrars Registries	Certain data elements (domain name and nameservers) would be required to be disclosed. The lawful basis would be 6(1)b, should personal data be involved for Registrars and 6 (1)(f) of the GDPR for Registries.  For other data elements, Art. 6(1)(f) of the GDPR.
<b>Disclosure</b>	Registrars Registries	Certain data elements (domain name and nameservers) would be required to be transferred from the Registrar to Registry. The lawful basis would be 6(1)b, should personal data be involved, for Registrars and 6 (1)(f) of the GDPR for Registries. 6(1)(f)
<b>Data Retention</b>	ICANN	6(1)(f)

**ICANN PURPOSE:**

Maintaining the security, stability and resiliency of the Domain Name System In accordance with ICANN’s mission through the enabling of lawful access for legitimate third-party interests to data elements collected for the other purposes identified herein.

<sup>46</sup> Note, the responsible party is not necessarily the party carrying out the processing activity. This applies to all references of ‘responsible party’ in these tables.

<sup>47</sup> In relation to the application of 6(1)b, please see input provided by external legal counsel in relation to charter questions k, l and m above.

<u>Processing Activity</u>	<u>Responsible Party:</u>	<u>Lawful Basis:</u>
Collection	ICANN Registrars Registries	6(1)(f)
Transmission from Rr to Ry	N/A	N/A
Disclosure	ICANN	6(1)(f)
Data Retention	ICANN	N/A

**ICANN PURPOSE:**

Enable communication with and/or notification to the Registered Name Holder and/or their delegated agents of technical and/or administrative issues with a Registered Name

<u>Processing Activity</u>	<u>Responsible Party:</u>	<u>Lawful Basis:</u>
Collection	Registrar Registries	6(1)(b) for Registrars 6(1)(f) for Registries
Transmission from Rr to Ry	ICANN Registries	6(1)(f)
Disclosure	TBD	
Data Retention	ICANN	N/A

**ICANN PURPOSE:**

Provide mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure, or other unavailability of a Registrar or Registry Operator

<u>Processing Activity</u>	<u>Responsible Party:</u>	<u>Lawful Basis</u>
Collection	ICANN	6(1)(f)
Transmission from Rr to Ry	ICANN	6(1)(f)
Disclosure	ICANN	6(1)(f)
Data Retention	ICANN	6(1)(f)

**ICANN PURPOSE:**  
 Handle contractual compliance monitoring requests, audits, and complaints submitted by Registry Operators, Registrars, Registered Name Holders, and other Internet users.

<u>Processing Activity</u>	<u>Responsible Party:</u>	<u>Lawful Basis:</u>
Collection	ICANN	6(1)(f)
Transmission from Rr to Ry	ICANN	6(1)(f)
Disclosure	N/A	
Data Retention	ICANN	6(1)(f)

**ICANN PURPOSE:**  
 Coordinate, operationalize and facilitate policies for resolution of disputes regarding or relating to the registration of domain names (as opposed to the use of such domain names), namely, the UDRP, URS, PDDRP, RRDRP and future-developed domain name registration-related dispute procedures for which it is established that the processing of personal data is necessary

<u>Processing Activity</u>	<u>Responsible Party:</u>	<u>Lawful Basis:</u>
Collection	ICANN Registrars	6(1)(b) for Registrars 6(1)(f) for Registries
Transmission from Rr to Ry	ICANN Registries Registrars	6(1)(b) for Registrars 6(1)(f) for Registries
Transmission to dispute resolution providers	ICANN Registries Registrars Dispute Resolution Provider – Processor or independent controller	6(1)(b) for Registrars 6(1)(f) for Registries and ICANN
Disclosure		
Data Retention		

<b>ICANN PURPOSE:</b> Enabling validation to confirm that Registered Name Holder meets optional gTLD registration policy eligibility criteria voluntarily adopted by Registry Operator.		
<b>Processing Activity</b>	<b>Responsible Party:</b>	<b>Lawful basis:</b>
Collecting specific data for Registry Agreement-mandated eligibility requirements	Registries	6(1)(b) for Registrars 6(1)(f) for Registries
Collecting specific data for Registry Operator-adopted eligibility requirements	Registries	6(1)(b) for Registrars 6(1)(f) for Registries
Transmission from Rr to Ry RA-mandated eligibility requirements	Registries	6(1)(b) for Registrars 6(1)(f) for Registries
Transmission from Rr to Ry Registry-adopted eligibility requirements	Registries	6(1)(b) for Registrars 6(1)(f) for Registries
Disclosure	Registries	N/A
Data Retention	Registries	6(1)(f)

**Part 4: Updates to Other Consensus Policies**

Charter Question

n) URS

n1) Should Temporary Specification language be confirmed, or are additional adjustments needed?

## o) UDRP

o1) Should Temporary Specification language be confirmed, or are additional adjustments needed?

EPDP Team considerations and deliberations in addressing the charter questions

- The EPDP Team noted that as of the Team’s deliberations, although some members have reported no significant issues in relation to the functioning and operation of the URS and UDRP following the adoption of the Temporary Specification, others reported difficulties as access to domain name registration pre-filing is often unavailable in the absence of an agreed upon standard for “reasonable access”.
- The EPDP Team also took note of the fact that an existing GNSO PDP WG, namely the Review of All Rights Protection Mechanisms in All gTLDs (RPMs) PDP WG, is currently tasked with reviewing the URS and UDRP and is expected to factor in any changes resulting from GDPR requirements.
- The EPDP Team requests that when the EPDP Team commences its deliberations on a standardized access framework, a representative of the RPMs PDP WG shall provide an update on the current status of deliberations so that the EPDP Team may determine if/how the WG’s recommendations may affect consideration of the URS and UDRP in the context of the standardized access framework deliberations.

**EPDP Team Recommendation #21.**

The EPDP Team also recommends that the GNSO Council instructs the review of all RPMs PDP WG to consider, as part of its deliberations, whether there is a need to update existing requirements to clarify that a complainant must only be required to insert the publicly-available RDDS data for the domain name(s) at issue in its initial complaint. The EPDP Team also recommends the GNSO Council to instruct the RPMs PDP WG to consider whether upon receiving updated RDDS data (if any), the complainant must be given the opportunity to file an amended complaint containing the updated respondent information.

**EPDP Team Recommendation #22.**

The EPDP Team recommends that ICANN Org must enter into appropriate data protection agreements with dispute resolution providers in which, amongst other items, the data retention period is specifically addressed.

**EPDP Team Recommendation #23.**

The EPDP Team recommends that, for the new policy on gTLD registration data, the following requirements MUST apply in relation to URS and UDRP until such time as these are superseded by recommendations from the RPMs PDP WG and/or policies from the EPDP regarding disclosure:



Uniform Rapid Suspension (supplemental requirements for the 17 October 2013 URS High Level Technical Requirements for Registries and Registrars and URS Rules effective 28 June 2013)

(1) Registry Operator Requirement: The Registry Operator (or appointed BERO) MUST provide the URS provider with the full Registration Data for each of the specified domain names, upon the URS provider notifying the Registry Operator (or appointed BERO) of the existence of a complaint, or participate in another mechanism to provide the full Registration Data to the Provider as specified by ICANN. If the gTLD operates as a "thin" registry, the Registry Operator MUST provide the available Registration Data to the URS Provider.

(2) Registrar Requirement: If the domain name(s) subject to the complaint reside on a "thin" registry, the Registrar MUST provide the full Registration Data to the URS Provider upon notification of a complaint.

(3) URS Rules: Complainant's complaint will not be deemed defective for failure to provide the name of the Respondent (Registered Name Holder) and all other relevant contact information required by Section 3 of the URS Rules if such contact information of the Respondent is not available in registration data publicly available in RDDS or not otherwise known to Complainant. In such an event, Complainant may file a complaint against an unidentified Respondent and the Provider shall provide the Complainant with the relevant contact details of the Registered Name Holder after being presented with a complaint against an unidentified Respondent.

Uniform Dispute Resolution Policy (supplemental requirements for the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules"))

(1) Registrar Requirement: The Registrar MUST provide the UDRP provider with the full Registration Data for each of the specified domain names, upon the UDRP provider notifying the Registrar of the existence of a complaint, or participate in another mechanism to provide the full Registration Data to the Provider as specified by ICANN.

2) Complainant's complaint will not be deemed defective for failure to provide the name of the Respondent (Registered Name Holder) and all other relevant contact information required by Section 3 of the UDRP Rules if such contact information of the Respondent is not available in registration data publicly available in RDDS or not otherwise known to Complainant. In such an event, Complainant may file a complaint against an unidentified Respondent and the Provider shall provide the Complainant with the relevant contact details of the Registered Name Holder after being presented with a complaint against an unidentified Respondent.

#### Charter Question

##### p) Transfer Policy

p1) Should Temporary Specification language be confirmed or modified until a dedicated PDP can revisit the current transfer policy?

p2) If so, which language should be confirmed, the one based on RDAP or the one based in current WHOIS?

EPDP Team considerations and deliberations in addressing the charter questions

- The EPDP Team noted that as of the Team's deliberations, no significant issues have been reported in relation to the functioning and operation of the Transfer Policy, although some indicated that based on anecdotal evidence, the number of hijacking incidents may have gone down as the result of the registrant email address no longer being published, while others pointed to increased security risks as a result of those changes.
- The EPDP Team also took note of the fact that a review of the Transfer Policy has commenced which, in addition to including an overall review of the Transfer Policy, also includes additional information as to how the GDPR and the Temporary Specification requirements have affected inter-registrar transfers.

**EPDP Team Recommendation #24.**

The EPDP Team recommends that for the new policy on gTLD registration data, the following requirements MUST apply in relation to the Transfer Policy until such time these are superseded by recommendations that may come out of the Transfer Policy review that is being undertaken by the GNSO Council:

Supplemental procedures for the [Transfer Policy](#) applicable to all ICANN-accredited Registrars

(a) Until such time when the RDAP service (or other secure methods for transferring data) is required by ICANN to be offered, if the Gaining Registrar is unable to gain access to then-current Registration Data for a domain name subject of a transfer, the related requirements in the Transfer Policy will be superseded by the below provisions:

(a1) The Gaining Registrar is not REQUIRED to obtain a Form of Authorization from the Transfer Contact.

(a2) The Registrant MUST independently re-enter Registration Data with the Gaining Registrar. In such instance, the Gaining Registrar is not REQUIRED to follow the Change of Registrant Process as provided in Section II.C. of the Transfer Policy.

(b) As used in the Transfer Policy:

(b1) The term "Whois data" SHALL have the same meaning as "Registration Data".

(b2) The term "Whois details" SHALL have the same meaning as "Registration Data".

(b3) The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".

(b4) The term "Whois" SHALL have the same meaning as "RDDS".

(c) Registrar and Registry Operator SHALL follow best practices in generating and updating the "AuthInfo" code to facilitate a secure transfer process.

(d) Registry Operator MUST verify that the "AuthInfo" code provided by the Gaining Registrar is valid in order to accept an inter-registrar transfer request.

**EPDP Team Recommendation #25.**

The EPDP Team recommends that the GNSO Council, as part of its review of the Transfer Policy, specifically requests the review of the implications, as well as adjustments, that may be needed to the Transfer Policy as a result of GDPR, with great urgency.

## Charter Question

## q) Sunsetting WHOIS Contractual Requirements

q1) After migration to RDAP, when can requirements in the Contracts to use WHOIS protocol be eliminated?

q2) If EPDP Team's decision includes a replacement directory access protocol, such as RDAP, when can requirements in the Contracts to use WHOIS protocol be eliminated?

At the time of publication of this Final Report, the EPDP Team elected to prioritize its policy recommendations with respect to the Temporary Specification. The EPDP Team believes addressing eventual migration to RDAP and sunseting of WHOIS requirements is premature at this time, i.e., before the policy recommendations are implemented and work on RDAP has been finalized.

While the exact date of the possible elimination of WHOIS requirements will be determined in the policy implementation phase, the EPDP Team notes any current WHOIS requirements negated or made redundant by eventual policy recommendations will no longer be required.

**Other recommendations****EPDP Team Recommendation #26.**

The EPDP Team recommends that ICANN Org enters into required data protection agreements such as a Data Processing Agreement (GDPR Art. 28) or Joint Controller Agreement (Art. 26), as appropriate, with the non-Contracted Party entities involved in registration data processing such as data escrow providers and EBERO providers. These agreements are expected to set out the relationship obligations and instructions for data processing between the different parties.

**EPDP Team Recommendation #27.**

The EPDP Team recommends that as part of the implementation of these policy recommendations, updates are made to the following existing policies / procedures, and any others that may have been omitted, to ensure consistency with these policy recommendations as, for example, a number of these refer to administrative and/or technical contact which will no longer be required data elements:

- [Registry Registration Data Directory Services Consistent Labeling and Display Policy](#)
- [Thick WHOIS Transition Policy for .COM, .NET, .JOBS](#)
- [Rules for Uniform Domain Name Dispute Resolution Policy](#)

- [WHOIS Data Reminder Policy](#)
- [Transfer Policy](#)
- [Uniform Rapid Suspension System \(URS\) Rules](#)
- [Transfer Dispute Resolution Policy](#)

### Implementation

Although the objective is to keep the timeframe for implementation to a minimum, additional time will be necessary to implement these policy recommendations. As such, the EPDP Team has considered how to avoid a gap between the adoption of these policy recommendations by the ICANN Board and the subsequent implementation, noting the impending expiration of the Temporary Specification requirements. As such:

#### **EPDP Team Recommendation #28.**

The EPDP Team recommends that the effective date of the gTLD Registration Data Policy shall be February 29, 2020. All gTLD Registry Operators and ICANN-accredited registrars will be required to comply with the gTLD Registration Data Policy as of that date. The EPDP Team recommends that until February 29, 2020, registries and registrars are required EITHER to comply with this gTLD Registration Data Policy OR continue to implement measures consistent with the Temporary Specification (as adopted by the ICANN Board on 17 May 2018, and expired on 25 May 2019). Registries and registrars who continue to implement measures compliant with the expired Temporary Specification will not be subject to Compliance penalty specifically related to those measures until February 29, 2020.

The EPDP Team furthermore recommends that, as a matter of urgency, the GNSO Council and ICANN Org, informally convene the Implementation Review Team to allow for the necessary planning to take place before ICANN Board consideration of this Final Report, following which the IRT would be formally convened.

#### **EPDP Team Recommendation #29.**

Recognizing that in the case of some existing registrations, there may be an Administrative Contact but no or incomplete Registered Name Holder contact information, the EPDP team recommends that prior to eliminating Administrative Contact fields, all Registrars must ensure that each registration contains Registered Name Holder contact information.

Note: in relation to Recommendation #29, this must happen prior to February 29, 2020.

Furthermore, the EPDP Team expects that as part of the implementation process due consideration is given to how appropriate notice is provided to the Registered Name Holder of the changes that will occur as a result of these policy recommendations to allow the Registered Name Holder to adjust as necessary. If deemed appropriate, this could follow an approach similar to the one described for the Organization Field transition process.

### Implementation Guidance

In relation to the definitional work that will take place during the implementation phase, “Registration Data” will mean the data elements identified in Annex D, collected from a natural and legal person in connection with a domain name registration.

The EPDP Team expects that the same due diligence is undertaken in the implementation phase in relation to understanding and assuring compliance with GDPR and due consideration is given to the definition of personal data (see e.g. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/>).

### **EPDP Team’s Policy Change Impact Analysis**

Per the EPDP Team’s Charter, the goal of this effort is to determine if the Temporary Specification for gTLD Registration Data should become an ICANN Consensus Policy, as is or with modifications, while complying with the GDPR and other relevant privacy and data protection law. As part of this determination, the EPDP Team has considered the elements of the Temporary Specification as outlined in the charter and answered the charter questions. The EPDP Team has considered what subsidiary recommendations it might make for future work by the GNSO which might be necessary to ensure relevant Consensus Policies, including those related to registration data, are reassessed to become consistent with applicable law (see relevant recommendations).

The EPDP Team recommends that as part of the implementation process further consideration will be given to a set of metrics to help inform the evaluation to measure success of these policy recommendations.

## 6 Next Steps

### 6.1 Next Steps

This Final Report will be submitted to the GNSO Council for its consideration and approval.

## Glossary

### 1. Advisory Committee

An Advisory Committee is a formal advisory body made up of representatives from the Internet community to advise ICANN on a particular issue or policy area. Several are mandated by the ICANN Bylaws and others may be created as needed. Advisory committees have no legal authority to act for ICANN, but report their findings and make recommendations to the ICANN Board.

### 2. ALAC - At-Large Advisory Committee

ICANN's At-Large Advisory Committee (ALAC) is responsible for considering and providing advice on the activities of the ICANN, as they relate to the interests of individual Internet users (the "At-Large" community). ICANN, as a private sector, non-profit corporation with technical management responsibilities for the Internet's domain name and address system, will rely on the ALAC and its supporting infrastructure to involve and represent in ICANN a broad set of individual user interests.

### 3. Business Constituency

The Business Constituency represents commercial users of the Internet. The Business Constituency is one of the Constituencies within the Commercial Stakeholder Group (CSG) referred to in Article 11.5 of the ICANN bylaws. The BC is one of the stakeholder groups and constituencies of the Generic Names Supporting Organization (GNSO) charged with the responsibility of advising the ICANN Board on policy issues relating to the management of the domain name system.

### 4. ccNSO - The Country-Code Names Supporting Organization

The ccNSO the Supporting Organization responsible for developing and recommending to ICANN's Board global policies relating to country code top-level domains. It provides a forum for country code top-level domain managers to meet and discuss issues of concern from a global perspective. The ccNSO selects one person to serve on the board.

### 5. ccTLD - Country Code Top Level Domain

ccTLDs are two-letter domains, such as .UK (United Kingdom), .DE (Germany) and .JP (Japan) (for example), are called country code top level domains (ccTLDs) and correspond to a country, territory, or other geographic location. The rules and policies for registering domain names in the ccTLDs vary significantly and ccTLD registries limit use of the ccTLD to citizens of the corresponding country.

For more information regarding ccTLDs, including a complete database of designated ccTLDs and managers, please refer to <http://www.iana.org/cctld/cctld.htm>.

## **6. Contracted Parties House**

The Contracted Parties House (CPH) is one of two houses in the GNSO. The CPH includes the two stakeholder groups, the Registry Stakeholder Group and the Registrar Stakeholder Group.

## **7. Domain Name Registration Data**

Domain name registration data, also referred to as registration data, refers to the information that registrants provide when registering a domain name and that registrars or registries collect. Some of this information is made available to the public. For interactions between ICANN Accredited Generic Top-Level Domain (gTLD) registrars and registrants, the data elements are specified in the current RAA. For country code Top Level Domains (ccTLDs), the operators of these TLDs set their own or follow their government's policy regarding the request and display of registration information.

## **8. Domain Name**

As part of the Domain Name System, domain names identify Internet Protocol resources, such as an Internet website.

## **9. DNS - Domain Name System**

DNS refers to the Internet domain-name system. The Domain Name System (DNS) helps users to find their way around the Internet. Every computer on the Internet has a unique address - just like a telephone number - which is a rather complicated string of numbers. It is called its "IP address" (IP stands for "Internet Protocol"). IP Addresses are hard to remember. The DNS makes using the Internet easier by allowing a familiar string of letters (the "domain name") to be used instead of the arcane IP address. So instead of typing 207.151.159.3, you can type [www.internic.net](http://www.internic.net). It is a "mnemonic" device that makes addresses easier to remember.

## **10. EPDP – Expedited Policy Development Process**

A set of formal steps, as defined in the ICANN bylaws, to guide the initiation, internal and external review, timing and approval of policies needed to coordinate the global Internet's system of unique identifiers. An EPDP may be initiated by the GNSO Council only in the following specific circumstances: (1) to address a narrowly defined policy issue that was identified and scoped after either the adoption of a GNSO policy recommendation by the ICANN Board or the implementation of such an adopted recommendation; or (2) to provide new or additional policy recommendations on a specific policy issue that had been substantially scoped previously, such that extensive, pertinent background information already exists, e.g. (a) in an Issue Report for a possible PDP that was not initiated; (b) as part of a previous PDP that was not completed; or (c) through other projects such as a GNSO Guidance Process.

## **11. GAC - Governmental Advisory Committee**

The GAC is an advisory committee comprising appointed representatives of national governments, multi-national governmental organizations and treaty organizations, and



distinct economies. Its function is to advise the ICANN Board on matters of concern to governments. The GAC will operate as a forum for the discussion of government interests and concerns, including consumer interests. As an advisory committee, the GAC has no legal authority to act for ICANN, but will report its findings and recommendations to the ICANN Board.

## **12. General Data Protection Regulation (GDPR)**

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.

## **13. GNSO - Generic Names Supporting Organization**

The supporting organization responsible for developing and recommending to the ICANN Board substantive policies relating to generic top-level domains. Its members include representatives from gTLD registries, gTLD registrars, intellectual property interests, Internet service providers, businesses and non-commercial interests.

## **14. Generic Top Level Domain (gTLD)**

"gTLD" or "gTLDs" refers to the top-level domain(s) of the DNS delegated by ICANN pursuant to a registry agreement that is in full force and effect, other than any country code TLD (ccTLD) or internationalized domain name (IDN) country code TLD.

## **15. gTLD Registries Stakeholder Group (RySG)**

The gTLD Registries Stakeholder Group (RySG) is a recognized entity within the Generic Names Supporting Organization (GNSO) formed according to Article X, Section 5 (September 2009) of the Internet Corporation for Assigned Names and Numbers (ICANN) Bylaws.

The primary role of the RySG is to represent the interests of gTLD registry operators (or sponsors in the case of sponsored gTLDs) ("Registries") (i) that are currently under contract with ICANN to provide gTLD registry services in support of one or more gTLDs; (ii) who agree to be bound by consensus policies in that contract; and (iii) who voluntarily choose to be members of the RySG. The RySG may include Interest Groups as defined by Article IV. The RySG represents the views of the RySG to the GNSO Council and the ICANN Board of Directors with particular emphasis on ICANN consensus policies that relate to interoperability, technical reliability and stable operation of the Internet or domain name system.

## **16. ICANN - The Internet Corporation for Assigned Names and Numbers**

The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. Originally, the Internet Assigned Numbers Authority (IANA) and other entities

performed these services under U.S. Government contract. ICANN now performs the IANA function. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes.

### **17. Intellectual Property Constituency (IPC)**

The Intellectual Property Constituency (IPC) represents the views and interests of the intellectual property community worldwide at ICANN, with a particular emphasis on trademark, copyright, and related intellectual property rights and their effect and interaction with Domain Name Systems (DNS). The IPC is one of the constituency groups of the Generic Names Supporting Organization (GNSO) charged with the responsibility of advising the ICANN Board on policy issues relating to the management of the domain name system.

### **18. Internet Service Provider and Connectivity Provider Constituency (ISPCP)**

The ISPs and Connectivity Providers Constituency is a constituency within the GNSO. The Constituency's goal is to fulfill roles and responsibilities that are created by relevant ICANN and GNSO bylaws, rules or policies as ICANN proceeds to conclude its organization activities. The ISPCP ensures that the views of Internet Service Providers and Connectivity Providers contribute toward fulfilling the aims and goals of ICANN.

### **19. Name Server**

A Name Server is a DNS component that stores information about one zone (or more) of the DNS name space.

### **20. Non Commercial Stakeholder Group (NCSG)**

The Non Commercial Stakeholder Group (NCSG) is a Stakeholder Group within the GNSO. The purpose of the Non Commercial Stakeholder Group (NCSG) is to represent, through its elected representatives and its Constituencies, the interests and concerns of noncommercial registrants and noncommercial Internet users of generic Top-level Domains (gTLDs). It provides a voice and representation in ICANN processes to: non-profit organizations that serve noncommercial interests; nonprofit services such as education, philanthropies, consumer protection, community organizing, promotion of the arts, public interest policy advocacy, children's welfare, religion, scientific research, and human rights; public interest software concerns; families or individuals who register domain names for noncommercial personal use; and Internet users who are primarily concerned with the noncommercial, public interest aspects of domain name policy.

### **21. Non-Contracted Parties House**

The Non-Contracted Parties House (NCPH) is one of the two major structures making up the GNSO. The GNSO is a bicameral structure, with one house made up of those that are directly contracting with ICANN, and the other for those that are not. The NCPH includes members who are internet service providers, businesses, connectivity providers and intellectual

property constituencies. The NCPH is composed of the Commercial and Non-Commercial Stakeholders Groups.

## **22. Post Delegation Dispute Resolution Procedures (PDDRs)**

Post-Delegation Dispute Resolution Procedures have been developed to provide those harmed by a new gTLD Registry Operator's conduct an alternative avenue to complain about that conduct. All such dispute resolution procedures are handled by providers external to ICANN and require that complainants take specific steps to address their issues before filing a formal complaint. An Expert Panel will determine whether a Registry Operator is at fault and recommend remedies to ICANN.

## **23. Registered Name**

"Registered Name" refers to a domain name within the domain of a gTLD, whether consisting of two (2) or more (e.g., john.smith.name) levels, about which a gTLD Registry Operator (or an Affiliate or subcontractor thereof engaged in providing Registry Services) maintains data in a Registry Database, arranges for such maintenance, or derives revenue from such maintenance. A name in a Registry Database may be a Registered Name even though it does not appear in a zone file (e.g., a registered but inactive name).

## **24. Registrar**

The word "registrar," when appearing without an initial capital letter, refers to a person or entity that contracts with Registered Name Holders and with a Registry Operator and collects registration data about the Registered Name Holders and submits registration information for entry in the Registry Database.

## **25. Registrar Accreditation Agreement**

The Registrar Accreditation Agreement (RAA) is the contract that governs the relationship between ICANN and its accredited registrars. The RAA sets out the obligations of both parties.

## **26. Registrars Stakeholder Group (RrSG)**

The Registrars Stakeholder Group is one of several Stakeholder Groups within the ICANN community and is the representative body of registrars. It is a diverse and active group that works to ensure the interests of registrars and their customers are effectively advanced. We invite you to learn more about accredited domain name registrars and the important roles they fill in the domain name system.

## **27. Registry Agreement**

The Registry Agreement (RA) is the contract that governs the relationship between ICANN and each Registry Operator. The RA sets out the obligations of both parties.

**28. Registry Operator**

A "Registry Operator" is the person or entity then responsible, in accordance with an agreement between ICANN (or its assignee) and that person or entity (those persons or entities) or, if that agreement is terminated or expires, in accordance with an agreement between the US Government and that person or entity (those persons or entities), for providing Registry Services for a specific gTLD.

**29. Registry-Registrar Agreement**

The Registry-Registrar Agreement is a contract between a Registrar and a Registry operator that sets out the obligations both parties.

**30. Registration Data Directory Service (RDDS)**

Domain Name Registration Data Directory Service or RDDS refers to the service(s) offered by registries and registrars to provide access to Domain Name Registration Data.

**31. Registration Restrictions Dispute Resolution Procedure (RRDRP)**

The Registration Restrictions Dispute Resolution Procedure (RRDRP) is intended to address circumstances in which a community-based New gTLD Registry Operator deviates from the registration restrictions outlined in its Registry Agreement.

**32. SO - Supporting Organizations**

The SOs are the three specialized advisory bodies that advise the ICANN Board of Directors on issues relating to domain names (GNSO and CCNSO) and, IP addresses (ASO).

**33. SSAC - Security and Stability Advisory Committee**

An advisory committee to the ICANN Board comprised of technical experts from industry and academia as well as operators of Internet root servers, registrars and TLD registries.

**34. TLD - Top-level Domain**

TLDs are the names at the top of the DNS naming hierarchy. They appear in domain names as the string of letters following the last (rightmost) ".", such as "net" in <http://www.example.net>. The administrator for a TLD controls what second-level names are recognized in that TLD. The administrators of the "root domain" or "root zone" control what TLDs are recognized by the DNS. Commonly used TLDs include .COM, .NET, .EDU, .JP, .DE, etc.

**35. Uniform Dispute Resolution Policy (UDRP)**

The Uniform Dispute Resolution Policy (UDRP) is a rights protection mechanism that specifies the procedures and rules that are applied by registrars in connection with disputes that arise over the registration and use of gTLD domain names. The UDRP provides a mandatory administrative procedure primarily to resolve claims of abusive, bad faith domain name registration. It applies only to disputes between registrants and third parties, not disputes between a registrar and its customer.

**36. Uniform Rapid Suspension (URS)**

The Uniform Rapid Suspension System is a rights protection mechanism that complements the existing Uniform Domain-Name Dispute Resolution Policy (UDRP) by offering a lower-cost, faster path to relief for rights holders experiencing the most clear-cut cases of infringement.

**37. WHOIS**

WHOIS protocol is an Internet protocol that is used to query databases to obtain information about the registration of a domain name (or IP address). The WHOIS protocol was originally specified in RFC 954, published in 1985. The current specification is documented in RFC 3912. ICANN's gTLD agreements require registries and registrars to offer an interactive web page and a port 43 WHOIS service providing free public access to data on registered names. Such data is commonly referred to as "WHOIS data," and includes elements such as the domain registration creation and expiration dates, nameservers, and contact information for the registrant and designated administrative and technical contacts.

WHOIS services are typically used to identify domain holders for business purposes and to identify parties who are able to correct technical problems associated with the registered domain.

## Annex A - Background

### Process Background

On 19 July 2018, the GNSO Council [initiated](#) an Expedited Policy Development Process (EPDP) and [chartered](#) the EPDP on the Temporary Specification for gTLD Registration Data Team. Unlike other GNSO PDP efforts, which are open for anyone to join, the GNSO Council chose to limit the membership composition of this EPDP, primarily in recognition of the need to complete the work in a relatively short timeframe and to resource the effort responsibly. GNSO Stakeholder Groups, the Governmental Advisory Committee (GAC), the Country Code Supporting Organization (ccNSO), the At-Large Advisory Committee (ALAC), the Root Server System Advisory Committee (RSSAC) and the Security and Stability Advisory Committee (SSAC) were each been invited to appoint up to a set number of members and alternates, as outlined in the [charter](#). In addition, the ICANN Board and ICANN Org have been invited to assign a limited number of liaisons to this effort. A call for volunteers to the aforementioned groups was issued in July, and the EPDP Team held its first meeting on [1 August 2018](#).

### Issue Background

On 17 May 2018, the ICANN Board of Directors (ICANN Board) adopted the [Temporary Specification for generic top-level domain \(gTLD\) Registration Data](#) (“Temporary Specification”) pursuant to the procedures for the establishment of temporary policies in ICANN’s agreements with Registry Operators and Registrars (“Contracts”). The Temporary Specification provides modifications to existing requirements in the Registrar Accreditation and Registry Agreements in order to comply with the European Union’s General Data Protection Regulation (“GDPR”). Following adoption of a temporary specification, the procedure for Temporary Policies as outlined in the Registrar Accreditation and Registry Agreements, provides the Board “shall immediately implement the Consensus Policy development process set forth in ICANN’s Bylaws”. Additionally, the procedure provides this Consensus Policy development process on the Temporary Specification must be carried out within a one-year period as the Temporary Specification can only remain in force for up to one year, from the effective date of 25 May 2018, i.e., the Temporary Specification will expire on 25 May 2019.

On 19 July 2018, the GNSO Council [initiated](#) an Expedited Policy Development Process (EPDP) and [chartered](#) the EPDP on the Temporary Specification for gTLD Registration Data Team. The EPDP Team held its first meeting on [1 August 2018](#).

## Annex B – EPDP Team Membership and Attendance

### EPDP Team Membership and Attendance

The members of the EPDP Team are:

	Members / Liaisons	Affiliation	SOI	% of Meetings Attended <sup>48</sup>
1	<a href="#">Alan Woods</a>	RySG	<a href="#">SOI</a>	91.5
2	<a href="#">Kristina Rosette<sup>49</sup></a>	RySG	<a href="#">SOI</a>	91.1
2	<a href="#">Beth Bacon<sup>50</sup></a>	RySG	<a href="#">SOI</a>	15.2
3	<a href="#">Marc Anderson</a>	RySG	<a href="#">SOI</a>	100
4	<a href="#">James M. Bladel</a>	RrSG	<a href="#">SOI</a>	76.8
5	<a href="#">Matt Serlin</a>	RrSG	<a href="#">SOI</a>	86.4
6	<a href="#">Emily Taylor</a>	RrSG	<a href="#">SOI</a>	82.1
7	<a href="#">Alex Deacon</a>	<a href="#">IPC</a>	<a href="#">SOI</a>	91.5
8	<a href="#">Diane Plaut</a>	<a href="#">IPC</a>	<a href="#">SOI</a>	89.8
9	<a href="#">Margie Milam</a>	BC	<a href="#">SOI</a>	93.2
10	<a href="#">Mark Svancarek</a>	BC	<a href="#">SOI</a>	93.2
11	<a href="#">Esteban Lescano<sup>51</sup></a>	ISPCP	<a href="#">SOI</a>	32.7
11	Fiona Assonga <sup>52</sup>	ISPCP	<a href="#">SOI</a>	13.6
12	<a href="#">Thomas Rickert</a>	ISPCP	<a href="#">SOI</a>	91.5
13	<a href="#">Stephanie Perrin</a>	<a href="#">NCSG</a>	<a href="#">SOI</a>	96.6

<sup>48</sup> This does not include attendance to F2F meetings which is recorded separately. See <https://community.icann.org/x/rQarBQ>, <https://community.icann.org/x/0QO8BQ>, <https://community.icann.org/x/1A08BQ>, <https://community.icann.org/x/2gO8BQ>, <https://community.icann.org/x/3wO8BQ> and [https://community.icann.org/x/sAn\\_BQ](https://community.icann.org/x/sAn_BQ).

<sup>49</sup> changed to observer on 08, February 2019

<sup>50</sup> changed to member on 08, February for Kristina Rosette until 31, March 2019

<sup>51</sup> Resigned 6 February 2019

<sup>52</sup> Became member on 06, February 2019 - no longer alternate due to Esteban Loscano' leaving

	<b>Members / Liaisons</b>	<b>Affiliation</b>	<b>SOI</b>	<b>% of Meetings Attended<sup>48</sup></b>
14	<a href="#">Ayden Férdeline</a>	<a href="#">NCSG</a>	<a href="#">SOI</a>	72.9
15	<a href="#">Milton Mueller</a>	<a href="#">NCSG</a>	<a href="#">SOI</a>	74.6
16	<a href="#">Julf Helsingius</a>	<a href="#">NCSG</a>	<a href="#">SOI</a>	89.8
17	<a href="#">Amr Elsadr</a>	<a href="#">NCSG</a>	<a href="#">SOI</a>	84.7
18	<a href="#">Farzaneh Badiei</a>	<a href="#">NCSG</a>	<a href="#">SOI</a>	86.4
19	<a href="#">Georgios Tselentis</a>	GAC	<a href="#">SOI</a>	74.6
20	Kavouss Arasteh	GAC	<a href="#">SOI</a>	76.3
21	<a href="#">Ashley Heineman</a>	GAC	<a href="#">SOI</a>	69.5
22	<a href="#">Alan Greenberg</a>	<a href="#">ALAC</a>	<a href="#">SOI</a>	91.5
23	<a href="#">Hadia Elminiawi</a>	<a href="#">ALAC</a>	<a href="#">SOI</a>	100
24	Benedict Addis	SSAC	<a href="#">SOI</a>	79.7
25	<a href="#">Ben Butler</a>	SSAC	<a href="#">SOI</a>	94.9
26	<a href="#">Chris Disspain</a>	ICANN Board Liaison	<a href="#">SOI</a>	97.4
27	<a href="#">Leon Felipe Sanchez</a>	ICANN Board Liaison	<a href="#">SOI</a>	76.3
28	<a href="#">Rafik Dammak</a>	GNSO Council Liaison	<a href="#">SOI</a>	100
29	<a href="#">Trang Nguyen</a>	ICANN Org Liaison (GDD)	<a href="#">SOI</a>	Not tracked
30	Dan Halloran	ICANN Org Liaison (Legal)	n/a	Not tracked
31	<a href="#">Kurt Pritz</a>	EPDP Team Chair	<a href="#">SOI</a>	100

The alternates of the EPDP Team are:



	<b>Alternates</b>	<b>Affiliation</b>	<b>SOI</b>	<b>% of Meetings Attended</b>
1	<a href="#">Matthew Crossman</a> <sup>53</sup>	RySG		0.0
2	<a href="#">Arnaud Wittersheim</a>	RySG	<a href="#">SOI</a>	1.7
3	<a href="#">Sebastien Ducos</a>	RySG	<a href="#">SOI</a>	1.7
4	Jeff Yeh <sup>54</sup>	RrSG	<a href="#">SOI</a>	3.8
4	Volker Greimann <sup>55</sup>	RrSG	<a href="#">SOI</a>	6.1
5	Lindsay Hamilton-Reid <sup>56</sup>	RrSG	<a href="#">SOI</a>	42.1
5	Sarah Wylid <sup>57</sup>	RrSG	<a href="#">SOI</a>	66.7
6	Theo Geurts	RrSG	<a href="#">SOI</a>	23.7
7	<a href="#">Brian King</a>	IPC	<a href="#">SOI</a>	16.9
8	Steve DelBianco	BC	<a href="#">SOI</a>	6.8
9	Suman Lal Pradhan <sup>58</sup>	ISPCP	<a href="#">SOI</a>	0
10	<a href="#">Tatiana Tropina</a>	NCSG	<a href="#">SOI</a>	20.3
11	<a href="#">David Cake</a>	NCSG	<a href="#">SOI</a>	5.1
12	<a href="#">Collin Kurre</a>	NCSG	<a href="#">SOI</a>	27.1
13	<a href="#">Chris Lewis-Evans</a>	GAC	<a href="#">SOI</a>	35.6
14	<a href="#">Rahul Gosain</a>	GAC	<a href="#">SOI</a>	13.6
15	<a href="#">Laureen Kapin</a>	GAC	<a href="#">SOI</a>	20.3
16	<a href="#">Holly Raiche</a>	ALAC	<a href="#">SOI</a>	1.7

<sup>53</sup> Joined as alternate on 11, February 2019

<sup>54</sup> changed to observer 08, October 2018

<sup>55</sup> Joined as alternate on 08, October 2018

<sup>56</sup> Resigned as alternate on 18, December 2018

<sup>57</sup> Joined as alternate on 18, December 2018

<sup>58</sup> Joined as alternate on 06, February 2019 replacing Fiona Assonga as the alternate

17	Seun Ojedeji	ALAC	<a href="#">SOI</a>	3.4
18	Greg Aaron	SSAC	<a href="#">SOI</a>	8.5
19	Rod Rasmussen	SSAC	<a href="#">SOI</a>	8.5

<b>EPDP Staff Support Team</b>
Berry Cobb
Caitlin Tubergen
Marika Konings
Andrea Glandon
Terri Agnew

The detailed attendance records can be found at <https://community.icann.org/x/4opHBQ>.

The EPDP Team email archives can be found at <https://mm.icann.org/pipermail/gnso-epdp-team/>.

\* The following are the ICANN SO/ACs and GNSO Stakeholder Groups and Constituencies for which EPDP TEAM members provided affiliations:

RrSG – Registrar Stakeholder Group

RySG – Registry Stakeholder Group

BC – Business Constituency

NCSG – Non-Commercial Stakeholder Group

IPC – Intellectual Property Constituency

ISPCP – Internet Service and Connection Providers Constituency

GAC – Governmental Advisory Committee

ALAC – At-Large Advisory Committee

SSAC – Security and Stability Advisory Committee

## Annex C - Community Input

### Request for Input

According to the GNSO's PDP Manual, an EPDP Team should formally solicit statements from each GNSO Stakeholder Group and Constituency at an early stage of its deliberations. An EPDP Team is also encouraged to seek the opinion of other ICANN Supporting Organizations and Advisory Committees who may have expertise, experience or an interest in the issue. As a result, the EPDP Team reached out to all ICANN Supporting Organizations and Advisory Committees as well as GNSO Stakeholder Groups and Constituencies with a request for input at the start of its deliberations. In response, statements were received from:

- The GNSO Business Constituency (BC)
- The GNSO Intellectual Property Constituency (IPC)
- The GNSO Non-Commercial Stakeholder Group (NCSG)
- The Registries Stakeholder Group (RySG)
- The At-Large Advisory Committee (ALAC)
- The Governmental Advisory Committee (GAC)
- The Security and Stability Advisory Committee (SSAC)

The full statements can be found here: <https://community.icann.org/x/Ag9pBQ>.

### Review of Input Received

All of the statements received were added to the [Discussion Summary Index](#) for the corresponding section in the Temporary Specification (where applicable) and reviewed by the EPDP Team as part of its deliberations on that particular topic.

## Annex D – Data Elements Workbooks

### Table of Contents:

#	Purpose	Link
1A	In accordance with the relevant registry agreements and registrar accreditation agreements, activate a registered name and allocate it to the Registered Name Holder.	<a href="#">LINK</a>
1B	Subject to the Registry and Registrar Terms, Conditions and Policies and ICANN Consensus Policies: <ol style="list-style-type: none"> <li>i. Establish the rights of a Registered Name Holder in a Registered Name; and</li> <li>ii. Ensure that a Registered Name Holder may exercise its right in the use, maintenance and disposition of the Registered Name.</li> </ol>	<a href="#">LINK</a>
2	Contributing to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN’s mission through enabling responses to lawful data disclosure requests.	<a href="#">LINK</a>
3	Enable communication with the Registered Name Holder on matters relating to the Registered Name.	<a href="#">LINK</a>
4A	Provide mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure of a Registrar or Registry Operator, or unavailability of a Registrar or Registry Operator, as described in the RAA and RA, respectively.	<a href="#">LINK</a>
4B	Provide mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure of a Registrar or Registry Operator, or unavailability of a Registrar or Registry Operator, as described in the RAA and RA, respectively.	<a href="#">LINK</a>
5	<ol style="list-style-type: none"> <li>i. Handle contractual compliance monitoring requests and audit activities consistent with the terms of the Registry agreement and the Registrar accreditation agreements and any applicable data processing agreements, by processing specific data only as necessary;</li> <li>ii. Handle compliance complaints initiated by ICANN, or third parties consistent with the terms of the Registry agreement and the Registrar accreditation agreements.</li> </ol>	<a href="#">LINK</a>
6	Operationalize policies for the resolution of disputes regarding or relating to the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names), namely, the UDRP, URS, PDDRP, RRDRP, and the TDRP	<a href="#">LINK</a>
7	Enabling validation to confirm that Registered Name Holder meets gTLD registration policy eligibility criteria voluntarily adopted by Registry Operator and that are described or referenced in the Registry Agreement for that gTLD.	<a href="#">LINK</a>

In a previous version of this document, the term “ICANN Purpose” was used in the title of the Purpose Statement for each workbook to describe purposes for processing registration data, including personal data, that should be governed by ICANN via a Consensus Policy. “ICANN” has since been removed, but the principle still applies. Note there are additional purposes for processing personal data, which the contracted parties may pursue, such as billing customers, but these are outside of what ICANN and its community should develop policy on or contractually enforce. It does not necessarily mean that such purpose is solely pursued by ICANN Org.

### **Primary Processing Activity Definitions:**

#### *Preamble*

*Definitions have been supplied with the primary types of Processing Activities of Collection, Transmission, Disclosure, and Retention. It is hoped that these definitions will provide clarity to documenting the Processing Activities and avoid confusion of their use in policy versus what may actually occur technically.*

#### **Collection**

*The processing action whereby the Controller or Processor gains (or gains access to) the data.*

#### **Transmission/Transfer**

*The processing action whereby data is disclosed by a Controller or Processor to another party when that other party is involved in the processing of those data.*

#### **Disclosure<sup>59</sup>**

*The processing action whereby the Controller accepts responsibility for release of personal information to third parties upon request.*

#### **Publication**

*The processing action whereby data is disclosed to third parties, by being made publicly available for a public interest purpose.*

#### **Retention**

*When the primary purpose of data processing has been achieved, and/or the data is no longer required for that purpose, such data may be retained by a Controller (or Processor), where the Controller (or Processor) has established additional specific and stated purposes, and where such retention is:*

- A. Not incompatible with the primary/original purpose for the processing of the data; or*
- B. Reasonably necessary to demonstrate the fulfilment of the original purpose. (e.g. the retention of data to demonstrate completion, by the Controller/Processor, of a contractual obligation in contemplation of defending against claims of breach of contract etc.); and*
- C. Processing of retained data is limited to only those purpose(s) for which such data are retained.*

---

<sup>59</sup> Not ALL data are necessarily required to be disclosed. The data elements represented in the workbooks are an aggregate of which data may be disclosed, but specific elements are yet to be determined depending on the situation.

**Other Definitions:**

- **Optional:** - In the Initial Report, those data elements marked as “(optional, (O))”, were used in a generic sense and ultimately caused confusion in how they traversed the processing activities.
  - Refined legend: O-RNH, O-Rr, O-CP
    - Optional for Registrant to fill in, but if supplied it must be processed
    - Optional for Registrar to provide, but if supplied it must be processed
    - Optional for contracted party subject to terms and conditions
- **Generated:** The data elements tables contain a list of in-scope fields of registration data as derived from existing policy, technical specifications, or contract specifications. Fields marked with an “\*” are fields that are either collected from the data subject, or automatically “generated” by the registrar or registry.

**Lawful Basis:**

The workbooks each contain a section that documents the processing activities as well as a space to document the lawful basis. The EPDP has received legal advice regarding the application of Art. 6(1)(b), necessary for performance of a contract, as a lawful basis. To date, outside legal counsel has noted, "A registrar could rely on Article 6(1)(b) as the lawful basis for processing other than simply registering and activating a domain if it can show that such processing is for one of the fundamental objectives of the contract. It would be difficult to argue that that processing to prevent DNS abuse is "necessary for the performance of a contract to which the data subject is party". Based on this application, we have tentatively marked the processing activities of registrar collection and transfer under as lawful under 6(1)(b), while we have marked all other processing under the other purposes as 6(1)(f), noting this is a placeholder pending further legal analysis. Any designations suggested in the workbooks below is based on the EPDP Team’s best current thinking but that in the end the determination is a result of law not opinion.

**Data Flow Diagrams and Data Elements Tables:**

- The diagrams are simple representations arrangements (colored data flow lines) between ICANN, Contracted Parties, Service Providers, and the Data Subject (Registrant). They are not an accurate depiction of the exact agreements that may already exist or future ones. Further, the data flows (black lined data flow) are also not representative of what how the data may actually flow technically. More detailed analysis and documentation will be required to accurately reflect the data flow.
- The data elements tables are also limited in how they properly reflect how data traverses the processing activities identified for each purpose. They act more as a policy tool to manage an inventory of data elements used in existing publicly accessible Whois directory today. Further, the roles played are also more complex than what is represented here. For example, the processing activity of a transfer means that one party performs the “transfer”, while the receiving party is “collecting” the data.

# 1A

**PURPOSE:**

In accordance with the relevant Registry Agreements and Registrar Accreditation Agreements, activate a registered name and allocate it to the Registered Name Holder.

**Purpose Rationale:**

**1) If the purpose is based on an ICANN contract, cite the relevant section of the ICANN contracts that corresponds to the above purpose, if any.**

- RAA - <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>

Yes, this purpose is lawful based on ICANN’s mission to coordinate the allocation and assignment of names in the root zone of the Domain Name System. Specifically, Section 3.2 of the RAA “Submission of Registered Name Holder Data to Registry” refers to what data elements must be placed in the Registry Database as a part of the domain registration (<https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>) & <https://www.icann.org/resources/pages/registries/registries-agreements-en>).

**2) Is the purpose in violation with ICANN's bylaws?**

No, it is not in violation of ICANN’s Bylaws. Specifically, Article 1, Section 1.1 Mission (a)(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System ("DNS") and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("gTLDs"). In this role, ICANN's scope is to coordinate the development and implementation of policies <https://www.icann.org/resources/pages/governance/bylaws-en/#article1>.

Further, Articles G-1 and G-2 stipulate, “issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet, registrar services, registry services, or the DNS;” and “Examples of the above include, without limitation: principles for allocation of registered names in a TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);”

**3) Are there any “picket fence” considerations related to this purpose?**

This purpose is related to WHOIS, which is within the Picket Fence. Specifically, Specification 1 of the Registry Agreement (Section 3.1(b) (iv) and (v) of legacy RA) and Specification 4 of the Registrar Accreditation Agreement both refer to categories of issues and principles of allocation of registered names in a TLD.

**Lawfulness of Processing Test:**

Processing Activity:	Responsible Party: <small>(Charter Questions 3k, 3l, 3m)</small>	Lawful Basis: (Is the processing necessary to achieve the purpose?)
<b>1A-PA1:</b> Collection of registration data to allocate and activate	ICANN Registrars Registries	6(1)(b) for Registrars

<p>the domain name string to Registered Name Holder</p> <p>(Charter Question 2b)</p>	<p>RNH</p>	<p>This is a 6(1)(b) purpose for Registrars because it is necessary to collect registrant data to allocate a string to a registrant. Without collecting minimal registrant data, the contracted party has no way of tracing the string back to registrant and is not able to deliver its side of the contract.</p> <p>6(1)(f) for Registries and ICANN</p> <p>This is a 6(1)(f) purpose for Registries receiving such data from Registrars to allocate the domain name at the Registry level, this collection is based on 6(1)(f) purpose.</p> <p>(NOTE: that registries collection of the data occurs only when the data is disclosed to them by the registrar as per 1A-PA2)</p>
<p><b>1A-PA2:</b> Transmission of registration data from Registrar to Registry</p> <p>(Charter Questions 2c, 2d, 2e, 2i)</p>	<p>ICANN Registrars Registries</p>	<p>Certain data elements (Domain Name and NameServers) would be required to be transferred from the Registrar to Registry. The lawful basis would be 6(1)(b) (vis á vis the processing of the Registrar), should personal data be involved.</p> <p>(NOTE: the Registry’s receipt of this data is the collection, as per 1A-PA1)</p>
<p><b>1A-PA3:</b> Publication of registration data to the DNS</p> <p>(Charter Questions 2f (gating questions), 2j)</p>	<p>ICANN Registrars Registries</p>	<p>Activation of the domain name registration in the DNS requires the publication of certain data elements, namely Domain Name and NameServers. The lawful basis would be 6(1)(f), should personal data be involved.</p> <p>Due to the minimal discretion in the requirements of 1A this is a direction from ICANN on what and how to achieve the result. Registries and Registrars retain minimal discretion and thus are acting as processors in 1A.</p>
<p><b>1A-PA4:</b> Retention of registration data by Registrar, Registry</p> <p>(Charter Questions 2g)</p> <p>Note, this PA is not represented on the data elements table, because data processed above represents what data elements will be retained</p>	<p>ICANN Registrars Registries</p>	<p>6(1)(f) for Registrars</p> <p>This is a 6(1)(f) purpose because although there is likely a legitimate interest in providing mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a dispute over ownership or an improper transfer, it is not necessary from a technical perspective to retain the data in order to allocate a string to a registered name holder, and therefore is not necessary to perform the registration contract.</p> <p>The EPDP Team agreed to a period of one year following the life of the registration a registration as the retention period in</p>

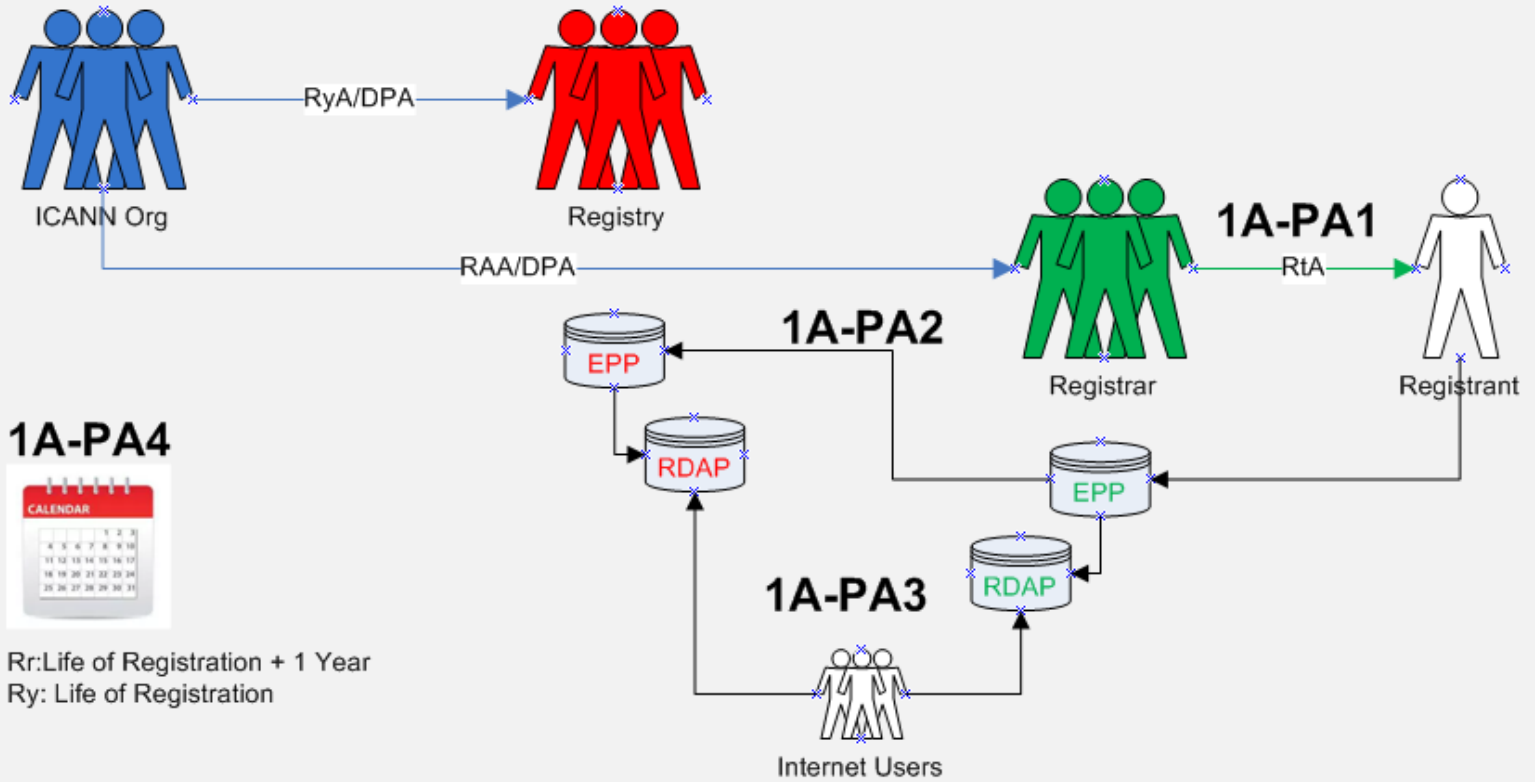


order to conform with the Transfer Dispute Resolution Policy requirements. Refer to the details around retention in Recommendation #11

6(1)(f) for Registries

Registries need only retain data for the duration of the life of the domain.

**Data Flow Map:**



**PURPOSE:**

In accordance with the relevant Registry Agreements and Registrar Accreditation Agreements, activate a registered name and allocate it to the Registered Name Holder.

**Data Elements Matrix:**

R = required  
O-RNH, O-Rr, O-CP = optional  
N/A=not applicable

Data Elements (Collected & Generated*)	Collection 1A-PA1	Transmission 1A-PA2	Publication 1A-PA3			
Domain Name	R	R	R			
Registry Domain ID*						
Registrar Whois Server* <sup>60</sup>						
Registrar URL*						
Updated Date*						
Creation Date*						
Registry Expiry Date*						
Registrar Registration Expiration Date*						
Registrar*						
Registrar IANA ID*						
Registrar Abuse Contact Email*						
Registrar Abuse Contact Phone*						
Reseller*						
Domain Status(es)* <sup>61</sup>						
Registry Registrant ID*						
Registrant Fields						
<input type="checkbox"/> Name						
<input type="checkbox"/> Organization (opt.)						
<input type="checkbox"/> Street						
<input type="checkbox"/> City						
<input type="checkbox"/> State/province						
<input type="checkbox"/> Postal code						
<input type="checkbox"/> Country						
<input type="checkbox"/> Phone						
<input type="checkbox"/> Phone ext (opt.)						
<input type="checkbox"/> Fax (opt.)						
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email						
2nd E-Mail address						
Admin ID*						
Admin Fields						
<input type="checkbox"/> Name						
<input type="checkbox"/> Organization (opt.)						
<input type="checkbox"/> Street						

<sup>60</sup> “Registrar Whois Server”, “Registrar URL”, “Registrar Abuse Contact Email” and “Registrar Abuse Contact Phone” are not transmitted to the registry with each registration in EPP; they are provided to the registry once by each registrar and used for each registration a registrar has.

<sup>61</sup> “Domain Status” (which is a field that can appear multiple times) may or may not be set by the registrar; some status are set by the registrar, some are set by the registry.

Data Elements (Collected & Generated*)	Collection 1A-PA1	Transmission 1A-PA2	Publication 1A-PA3			
<input type="checkbox"/> City						
<input type="checkbox"/> State/province						
<input type="checkbox"/> Postal code						
<input type="checkbox"/> Country						
<input type="checkbox"/> Phone						
<input type="checkbox"/> Phone ext (opt.)						
<input type="checkbox"/> Fax (opt.)						
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email						
Tech ID*						
Tech Fields						
<input type="checkbox"/> Name						
<input type="checkbox"/> Organization (opt.)						
<input type="checkbox"/> Street						
<input type="checkbox"/> City						
<input type="checkbox"/> State/province						
<input type="checkbox"/> Postal code						
<input type="checkbox"/> Country						
<input type="checkbox"/> Phone						
<input type="checkbox"/> Phone ext (opt.)						
<input type="checkbox"/> Fax (opt.)						
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email						
NameServer(s)	O-RNH	O-CP	O-CP			
DNSSEC	O-RNH	O-CP	O-CP			
Name Server IP Address(es)	O-RNH	O-CP	O-CP			
Last Update of Whois Database*						

# 1B

**PURPOSE:**

As subject to registry and registrar terms, conditions and policies, and ICANN consensus policies:

- (i) establish the rights of a Registered Name Holder in a registered name, and
- (ii) ensure that a Registered Name Holder may exercise its rights in the use, maintenance and disposition of the Registered Name.

**Purpose Rationale:**

**1) If the purpose is based on an ICANN contract, cite the relevant section of the ICANN contracts that corresponds to the above purpose, if any.**

- RAA - <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>

Yes, this purpose is lawful based on ICANN's mission to coordinate the allocation and assignment of names in the root zone of the Domain Name System. Specifically, Section 3.2 of the RAA "Submission of Registered Name Holder Data to Registry", Spec. 4, section 1.5 and Spec. 2 of the RA, all refers to what data elements must be placed in the Registry Database as a part of the domain registration

(<https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en> & <https://www.icann.org/resources/pages/registries/registries-agreements-en>).

**2) Is the purpose in violation with ICANN's bylaws?**

No, it is not in violation of ICANN's Bylaws. Specifically, Article 1, Section 1.1 Mission (a)(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System ("DNS") and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("gTLDs"). In this role, ICANN's scope is to coordinate the development and implementation of policies <https://www.icann.org/resources/pages/governance/bylaws-en/#article1>.

Further, Articles G-1 and G-2 stipulate, "issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet, registrar services, registry services, or the DNS;" and "Examples of the above include, without limitation: principles for allocation of registered names in a TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);"

**3) Are there any "picket fence" considerations related to this purpose?**

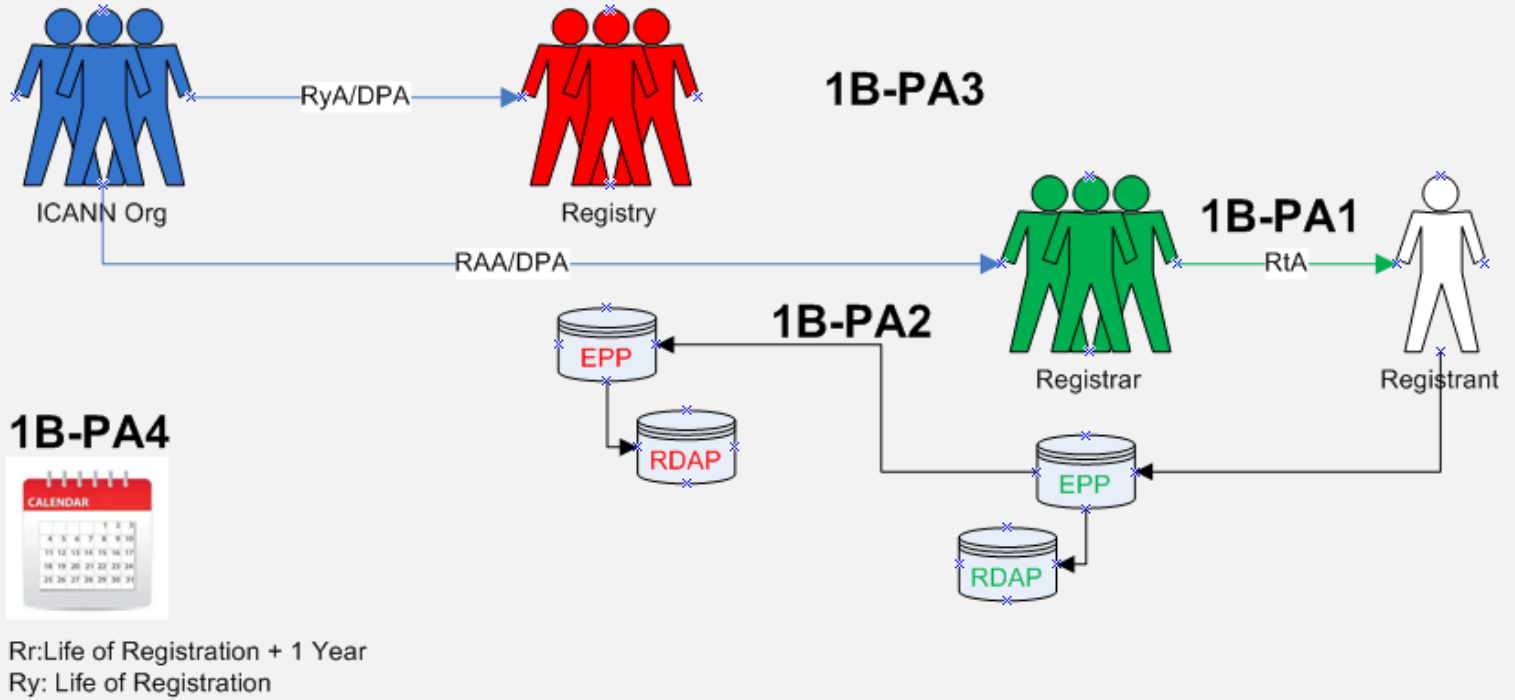
This purpose is related to WHOIS, which is within the Picket Fence. Specifically, Specification 1 of the Registry Agreement (Section 3.1(b)(iv) and (v) and Specification 4 of the Registrar Accreditation Agreement both refer to categories of issues and principles of allocation of registered names in a TLD.

**Lawfulness of Processing Test:**

<b>Processing Activity:</b>	<b>Responsible Party:</b> <small>(Charter Questions 3k, 3l, 3m)</small>	<b>Lawful Basis:</b> (Is the processing necessary to achieve the purpose?)
<p><b>1B-PA1:</b> Collection of registration data to establish registrant’s rights in a domain name string</p> <p>(Charter Question 2b)</p>	<p>ICANN Registrars Registries</p>	<p>6(1)(b) for Registrars</p> <p>This is a 6(1)(b) purpose for Registrars because it is necessary to collect registrant data to allocate a string to a registrant. Without collecting minimal registrant data, the contracted party has no way of tracing the string back to registrant and is not able to deliver its side of the contract.</p> <p>6(1)(f) for Registries and ICANN</p> <p>This is a 6(1)(f) purpose for Registries that require the collection of data to fulfill their terms, conditions and policies, this is a 6(1)(f) purpose.</p> <p>(NOTE: that registries collection of the data occurs only when the data is disclosed to them by the registrar as per 1B-PA2)</p>
<p><b>1B-PA2:</b> Transmission of registration data from Registrar to Registry</p> <p>(Charter Questions 2c, 2d, 2e, 2i)</p>	<p>ICANN Registrars Registries</p>	<p>Registries may direct a Registrar to provide a limited data set, (i.e. data set that differs from the from the Minimum Data Set as required as per the relevant consensus policy), where such a Registry Operator , due to varying business model and legal interpretations of obligations, require an alternate data set to fulfill, in their subjective evaluation, their specific policies, terms and conditions (for example, for the purpose of administering the application of a Registry Acceptable Use Policy (AUP)) in cases where such policies exist.</p> <p>The disclosure of the data by the registrar to the registry is justified under 6(1)(b) (vis á vis the registrar’s processing) for the valid purpose of enabling the registry to then, where necessary, directly enforce the registration terms or acceptable use policy of the registry, where such a registry chooses to do so.</p> <p>Note: Joint controllership results in a required element of the RA (Spec 11) vs. the interpretation of the Registry, where in some instances this is not considered to be required as this is a RA pass on. It is also accepted that some registry operators have the ability to ‘choose’ how to interpret their obligations under Spec 11, and therefore this additional exercising of</p>

		<p>control would tend to suggest that registries retain a relationship closer to a Joint Controller in the realization of purpose 1B.</p> <p>(NOTE: the Registry’s receipt of this data is the collection, as per 1B-PA1)</p>
<p><b>1B-PA3:</b> Disclosure of registration data for lawful purposes</p> <p>(Charter Questions 2f (gating questions), 2j)</p>	<p>ICANN Registrars Registries</p>	<p>Establishing the rights of a RNH, and ensuring, subject to Terms &amp; Conditions, that a RNH may exercise such benefits, may require disclosure of certain data elements, namely registrant details, IP addresses, domain names and name servers. The lawful basis would be 6(1)(f), should personal data be involved.</p>
<p><b>1B-PA4:</b> Retention of registration data by Registrar, Registry</p> <p>(Charter Questions 2g)</p> <p>Note, this PA is not represented on the data elements table, because data processed above represents what data elements will be retained</p>	<p>ICANN Registrars Registries</p>	<p>This is a 6(1)(f) purpose because although there is likely a legitimate interest in providing mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a dispute over ownership or an improper transfer, it is likely necessary for the registrar to retain the data to enforce their terms and conditions, however after the expiration of a domain, this retention is as per the register’s own controllership.</p> <p>-----</p> <p>6(1)(f) for Registrars</p> <p>This is a 6(1)(f) purpose because although there is likely a legitimate interest in providing mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a dispute over ownership or an improper transfer, it is not necessary from a technical perspective to retain the data in order to allocate a string to a registered name holder, and therefore is not necessary to perform the registration contract.</p> <p>The EPDP Team agreed to a period of one year following the life of the registration a registration as the retention period in order to conform with the Transfer Dispute Resolution Policy requirements. Refer to the details around retention in Recommendation #11</p> <p>6(1)(f) for Registries</p> <p>Registries need only retain data for the duration of the life of the domain.</p>

**Data Flow Map:**



**PURPOSE:**

As subject to registry and registrar terms, conditions and policies, and ICANN consensus policies:

- (i) establish the rights of a Registered Name Holder in a registered name, and
- (ii) ensure that a Registered Name Holder may exercise its rights in the use, maintenance and disposition of the registered name.

**Data Elements Matrix:**

R = required  
 O-RNH, O-Rr, O-CP = optional  
 N/A=not applicable

Data Elements (Collected & Generated*)	Collection 1B-PA1	Transmission 1B-PA2	Disclosure 1B-PA3			
Domain Name	R	R	R			
Registry Domain ID*						
Registrar Whois Server* <sup>62</sup>	R	O-CP	O-CP			
Registrar URL*	R	O-CP	O-CP			
Updated Date*		O-CP	O-CP			

<sup>62</sup> “Registrar Whois Server”, “Registrar URL”, “Registrar Abuse Contact Email” and “Registrar Abuse Contact Phone” are not transmitted to the registry with each registration in EPP; they are provided to the registry once by each registrar and used for each registration a registrar has. I’m not sure if you want to flag this or not.

Data Elements (Collected & Generated*)	Collection 1B-PA1	Transmission 1B-PA2	Disclosure 1B-PA3			
Creation Date*						
Registry Expiry Date*						
Registrar Registration Expiration Date*	O-Rr	O-CP	O-CP			
Registrar*	R	R	R			
Registrar IANA ID*	R	R	R			
Registrar Abuse Contact Email*	R	O-CP	O-CP			
Registrar Abuse Contact Phone*	R	O-CP	O-CP			
Reseller*	O-Rr	O-CP	O-CP			
Domain Status(es) <sup>63</sup>	R	O-CP	O-CP			
Registry Registrant ID*						
Registrant Fields						
<input checked="" type="checkbox"/> Name	R	O-CP	O-CP			
<input checked="" type="checkbox"/> Organization (opt.)	O-RNH	O-CP	O-CP			
<input checked="" type="checkbox"/> Street	R	O-CP	O-CP			
<input checked="" type="checkbox"/> City	R	O-CP	O-CP			
<input checked="" type="checkbox"/> State/province	R	O-CP	O-CP			
<input checked="" type="checkbox"/> Postal code	R	O-CP	O-CP			
<input checked="" type="checkbox"/> Country	R	O-CP	O-CP			
<input checked="" type="checkbox"/> Phone	R	O-CP	O-CP			
<input checked="" type="checkbox"/> Phone ext (opt.)						
<input checked="" type="checkbox"/> Fax (opt.)						
<input checked="" type="checkbox"/> Fax ext (opt.)						
<input checked="" type="checkbox"/> Email	R	O-CP	O-CP			
2nd E-Mail address						
Admin ID*						
Admin Fields						
<input checked="" type="checkbox"/> Name						
<input checked="" type="checkbox"/> Organization (opt.)						
<input checked="" type="checkbox"/> Street						
<input checked="" type="checkbox"/> City						
<input checked="" type="checkbox"/> State/province						
<input checked="" type="checkbox"/> Postal code						
<input checked="" type="checkbox"/> Country						
<input checked="" type="checkbox"/> Phone						
<input checked="" type="checkbox"/> Phone ext (opt.)						
<input checked="" type="checkbox"/> Fax (opt.)						

<sup>63</sup> "Domain Status" (which is a field that can appear multiple times) may or may not be set by the registrar; some status are set by the registrar, some are set by the registry.



Data Elements (Collected & Generated*)	Collection 1B-PA1	Transmission 1B-PA2	Disclosure 1B-PA3			
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email						
Tech ID*						
Tech Fields						
<input type="checkbox"/> Name						
<input type="checkbox"/> Organization (opt.)						
<input type="checkbox"/> Street						
<input type="checkbox"/> City						
<input type="checkbox"/> State/province						
<input type="checkbox"/> Postal code						
<input type="checkbox"/> Country						
<input type="checkbox"/> Phone						
<input type="checkbox"/> Phone ext (opt.)						
<input type="checkbox"/> Fax (opt.)						
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email						
NameServer(s)						
DNSSEC						
Name Server IP Address(es)						
Last Update of Whois Database*						

# 2

**PURPOSE:**

Contributing to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN’s mission through enabling responses to lawful data disclosure requests.

**Purpose Rationale:**

**1) If the purpose is based on an ICANN contract, cite the relevant section of the ICANN contracts that corresponds to the above purpose, if any.**

- RAA - <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>

Yes, this purpose is lawful based on ICANN’s mission to coordinate the allocation and assignment of names in the root zone of the Domain Name System. Specifically, ICANN contracts reference the requirement for the maintenance of and access to accurate and up-to-date information concerning domain name registrations.

**2) Is the purpose in violation with ICANN's bylaws?**

No, it is not in violation of ICANN’s Bylaws, see ICANN Bylaws - Section 1.1(d)(ii), Section 1.2(a), Section 4.6(e)(i), Annex G1 and G2.

**3) Are there any “picket fence” considerations related to this purpose?**

This is within the Picket Fence, as the purpose specially refers to data already collected.

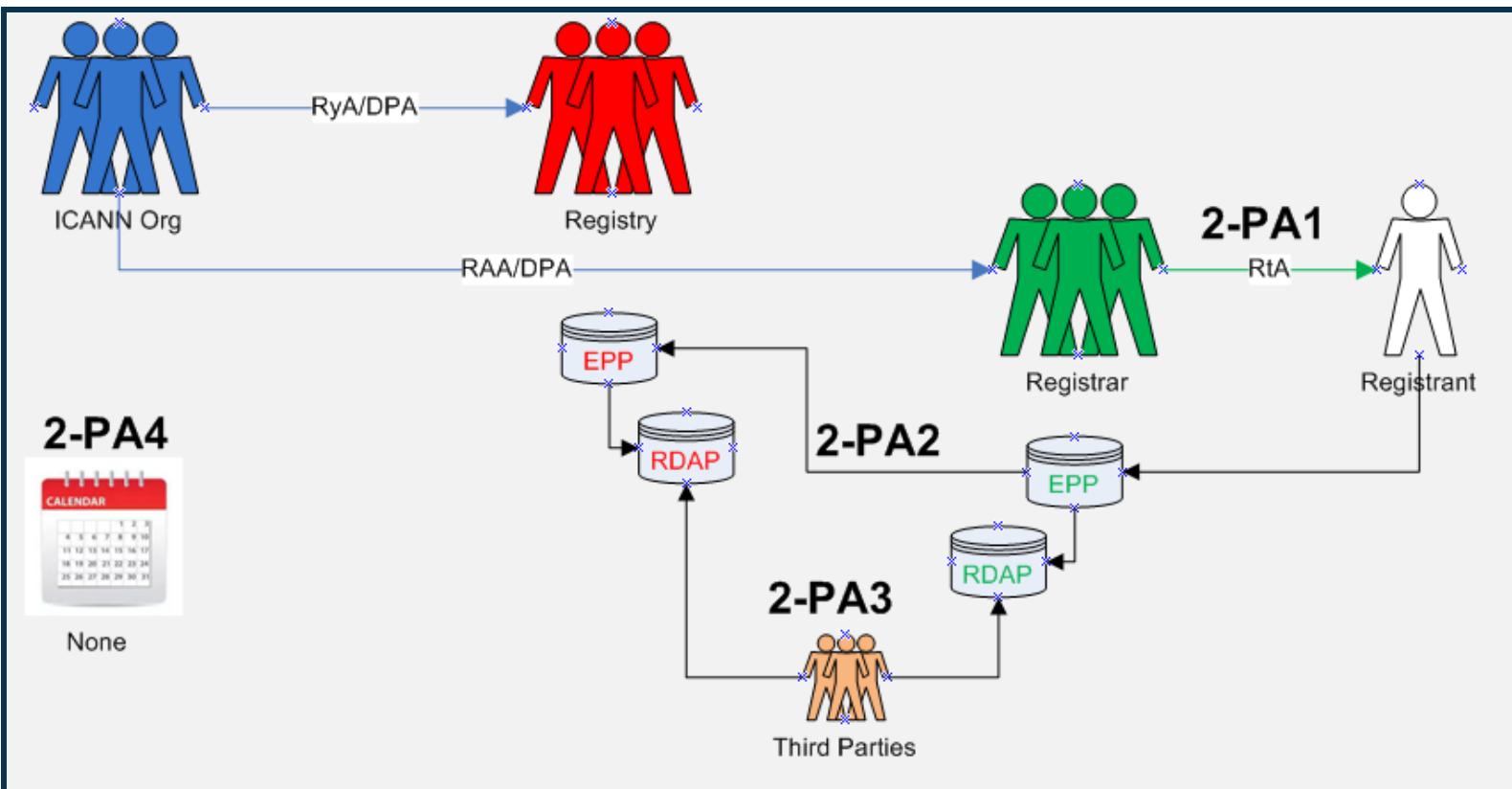
The WHOIS system, including 3rd party access, is within the Picket Fence, note specifically the Consensus Policies and Temporary Policies specification in the Registrar Accreditation Agreement (RAA) 1.3.4. maintenance of and access to accurate and up-to-date information concerning Registered Names and name servers; Registry Agreement (RA) - maintenance of and access to accurate and up-to-date information concerning domain name registrations.

**Lawfulness of Processing Test:**

Processing Activity:	Responsible Party: <small>(Charter Questions 3k, 3l, 3m)</small>	Lawful Basis: (Is the processing necessary to achieve the purpose?)
<p><b>2-PA1:</b> Collection of registration data by Registrar</p> <p>(Charter Question 2b)</p>	<p>ICANN Registrars Registries</p>	<p>The lawful basis for this processing activity is Art.6(1)(f) of the GDPR because although there may be a legitimate interest in disclosing non-public RDDS/WHOIS to third parties (such as law enforcement, IP interests, etc.), this disclosure is not technically necessary to perform the registration contract between the registrant and registrar.</p>

		(NOTE: that registries collection of the data occurs only when the data is disclosed to them by the registrar as per 2-PA2)
<p><b>2-PA2:</b> Transmission of registration data from Registrar to Registry</p> <p>(Charter Questions 2c, 2d, 2e, 2i)</p>	<p>ICANN Registrars Registries</p>	<p>This would be a 6(1)(f) processing activity because while there may be a legitimate interest in third parties contacting the registrant (for example, to inform the registrant or designee of a technical issue with the domain name), this is not necessary for the performance of the contract from a registry perspective.</p> <p>(NOTE: the Registry’s receipt of this data is the collection, as per 2-PA1)</p>
<p><b>2-PA3:</b> Disclosure of non-public, already collected, registration data to third parties</p> <p>(Charter Questions 2f (gating questions), 2j)</p>	<p>ICANN Registrars Registries Third Parties</p>	<p>This is a 6(1)(f) processing activity because although there may be a legitimate interest in disclosing non-public RDDS/WHOIS to third parties (such as law enforcement, IP interests, etc.), this disclosure is not technically necessary to perform the registration contract between the registrant and registrar.</p> <p>(Note: the requisite balancing test must be performed for each third-party type of disclosure and not for all registration data all the time.)</p>
<p><b>2-PA4:</b> Retention of registration data by registrar</p> <p>Note, this PA is not represented on the data elements table, because data processed above represents what data elements will be retained</p> <p>(Charter Questions 2g)</p>	<p>ICANN Registrars Registries</p>	<p>This processing activity is not required for the Purpose of providing lawful disclosures and further relies on retention as documented in Purpose 1A &amp; 1B.</p>

**Data Flow Map:**



**PURPOSE:**

Contributing to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN’s mission through enabling responses to lawful data disclosure requests.

**Data Elements Matrix:**

R = required  
 O-RNH, O-Rr, O-CP = optional  
 N/A=not applicable

Data Element (Collected & Generated*)	Collection 2-PA1	Transmission 2-PA2	Disclosure 2-PA3			
Domain Name	R	R	R			
Registry Domain ID*		R	R			
Registrar Whois Server*	R	R	R			
Registrar URL*	R	R	R			
Updated Date*		R	R			
Creation Date*		R	R			
Registry Expiry Date*		R	R			
Registrar Registration Expiration Date*	O-Rr	O-CP	O-CP			
Registrar*	R	R	R			
Registrar IANA ID*	R	R	R			
Registrar Abuse Contact Email*	R	R	R			

Data Element (Collected & Generated*)	Collection 2-PA1	Transmission 2-PA2	Disclosure 2-PA3			
Registrar Abuse Contact Phone*	R	R	R			
Reseller*	O-Rr	O-CP	O-CP			
Domain Status(es)*	R	R	R			
Registry Registrant ID*		R	R			
Registrant Fields						
<input checked="" type="checkbox"/> Name	R	O-CP	O-CP			
<input checked="" type="checkbox"/> Organization (opt.)	O-RNH	O-CP	O-CP			
<input checked="" type="checkbox"/> Street	R	O-CP	O-CP			
<input checked="" type="checkbox"/> City	R	O-CP	O-CP			
<input checked="" type="checkbox"/> State/province	R	O-CP	O-CP			
<input checked="" type="checkbox"/> Postal code	R	O-CP	O-CP			
<input checked="" type="checkbox"/> Country	R	O-CP	O-CP			
<input checked="" type="checkbox"/> Phone	R	O-CP	O-CP			
<input checked="" type="checkbox"/> Phone ext (opt.)						
<input checked="" type="checkbox"/> Fax (opt.)						
<input checked="" type="checkbox"/> Fax ext (opt.)						
<input checked="" type="checkbox"/> Email <sup>64</sup>	R	O-CP	O-CP			
2nd E-Mail address						
Admin ID*						
Admin Fields						
<input checked="" type="checkbox"/> Name						
<input checked="" type="checkbox"/> Organization (opt.)						
<input checked="" type="checkbox"/> Street						
<input checked="" type="checkbox"/> City						
<input checked="" type="checkbox"/> State/province						
<input checked="" type="checkbox"/> Postal code						
<input checked="" type="checkbox"/> Country						
<input checked="" type="checkbox"/> Phone						
<input checked="" type="checkbox"/> Phone ext (opt.)						
<input checked="" type="checkbox"/> Fax (opt.)						
<input checked="" type="checkbox"/> Fax ext (opt.)						
<input checked="" type="checkbox"/> Email						
Tech ID*		O-CP	O-CP			
Tech Fields						
<input checked="" type="checkbox"/> Name	O-RNH	O-CP	O-CP			
<input checked="" type="checkbox"/> Organization (opt.)						

<sup>64</sup> Per the current temp spec requirement: 2.5.1. Registrar MUST provide an email address or a web form to facilitate email communication with the relevant contact, but MUST NOT identify the contact email address or the contact itself.

Data Element (Collected & Generated*)	Collection 2-PA1	Transmission 2-PA2	Disclosure 2-PA3			
<input type="checkbox"/> Street						
<input type="checkbox"/> City						
<input type="checkbox"/> State/province						
<input type="checkbox"/> Postal code						
<input type="checkbox"/> Country						
<input type="checkbox"/> Phone	O-RNH	O-CP	O-CP			
<input type="checkbox"/> Phone ext (opt.)						
<input type="checkbox"/> Fax (opt.)						
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email	O-RNH	O-CP	O-CP			
NameServer(s)	O-RNH	O-CP	O-CP			
DNSSEC						
Name Server IP Address(es)	O-RNH	O-CP	O-CP			
Last Update of Whois Database*		R	R			

## 3

**PURPOSE:**

Enable communication with the Registered Name Holder on matters relating to the Registered Name.

**Purpose Rationale:**

**1) If the purpose is based on an ICANN contract, cite the relevant section of the ICANN contracts that corresponds to the above purpose, if any.**

Yes, this purpose is lawful based on ICANN's mission to coordinate the allocation and assignment of names in the root zone of the Domain Name System. Specifically, section 3.7.7.3 of the RAA refers to providing and updating contact information to facilitate timely resolution of any problems that arise in connection with the Registered Name.

**2) Is the purpose in violation with ICANN's bylaws?**

No, it is not in violation of ICANN's Bylaws. Specifically, Article 1, Section 1.1 Mission (a)(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System ("**DNS**") and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("**gTLDs**"). In this role, ICANN's scope is to coordinate the development and implementation of policies <https://www.icann.org/resources/pages/governance/bylaws-en/#article1>.

Further, Articles G-1 and G-2 stipulate, "issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet, registrar services, registry services, or the DNS;" and "Examples of the above include, without limitation: principles for allocation of registered names in a TLD (e.g., first-come/first-served, timely renewal, holding period after expiration);".

**3) Are there any "picket fence" considerations related to this purpose?**

This purpose is related to WHOIS, which is within the Picket Fence. Specifically, Specification 1 of the Registry Agreement and Specification 4 of the Registrar Accreditation Agreement both refer to categories of issues and principles of allocation of registered names in a TLD.

**Lawfulness of Processing Test:**

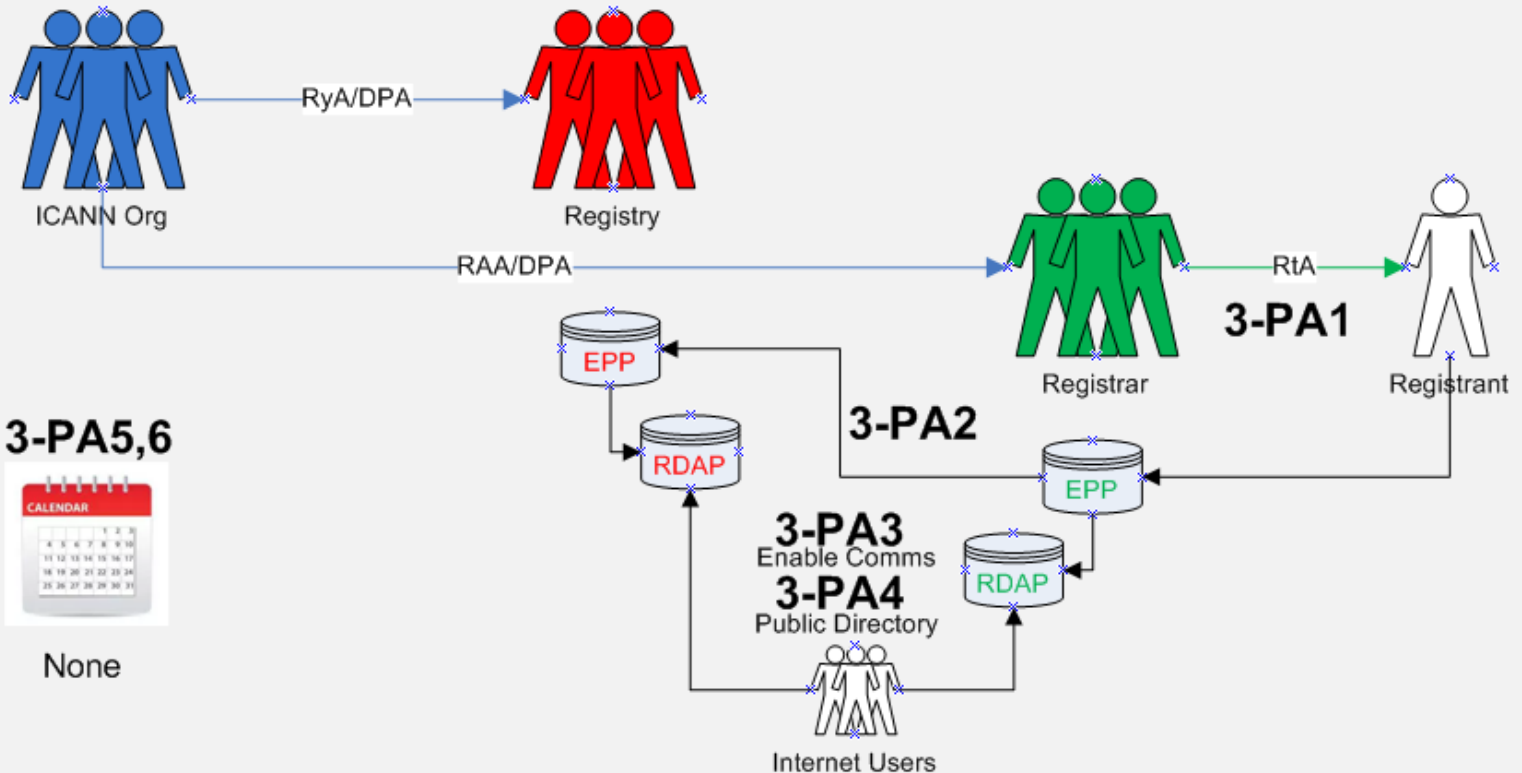
<b>Processing Activity:</b>	<b>Responsible Party:</b> (Charter Questions 3k, 3l, 3m)	<b>Lawful Basis:</b> (Is the processing necessary to achieve the purpose?)
<p><b>3-PA1:</b> Collection of registration data by Registrars  (Charter Question 2b)</p>	<p>ICANN Registrars Registries</p>	<p>For Registrars 6(1)(b) - For registrars: This is a 6(1)(b) purpose because it is necessary to collect registrant data so that the registrar can contact the registrant in the event a communication is necessary to maintain the domain operation.</p> <p>For Registries 6(1)(f) - For third parties who would like to report technical issues to a technical contact: This would be a 6(1)(f) purpose because while there may be a legitimate interest in third parties contacting the registrant (for example, to inform the registrant or designee of a technical issue with the domain name), this is not necessary for the performance of the contract.</p>
<p><b>3-PA2:</b> Transmission of registration data from Registrar to Registry  (Charter Questions 2c, 2d, 2e, 2i)</p>	<p>N/A</p>	<p>This processing activity is not applicable. The transfer of data from the Registrar to the Registry is not necessary to still enable Registry communication with the Registered Name Holder.</p> <p>Note that while a “transfer” of registration data as documented here is not required, the Registry will have still received non-public data as part of the registration process in EPP.</p>
<p><b>3-PA3:</b> Disclosure of registration data to enable communication with RNH  (Charter Questions 2f (gating questions), 2j)</p>	<p>ICANN Registrars Registries RNH</p>	<p>In compliance with GDPR, non-public information must not be improperly disclosed and when it is, it is only for a lawful and specific purpose.</p> <p>Occurs, for example, when responding to court orders.</p> <p>This processing activity occurs via publication as noted in 3-PA4 by Registrars and Registries. This will not be reflected as a column in the data elements table below.</p>
<p><b>3-PA4:</b> Publication of public, already collected, registration data to Internet Users</p>	<p>ICANN Registrars Registries Internet Users</p>	<p>A minimum public data set of registration data will be made available for query of gTLD second level domains in a freely accessible directory. Where a data element has been designated as non-public, it will be redacted, see 3-PA6.<sup>65</sup></p>

<sup>65</sup> Refer to recommendation #8 in regards to redaction and more information pertaining to a minimum public data set.



(Charter Questions 2f (gating questions), 2j)		In the data elements table below, take note of two columns, one for Registrars and one for Registries.
<b>3-PA5:</b> Redaction of registration data to Internet Users	ICANN Registrars Registries Internet Users	In compliance with GDPR, non-public information must not be improperly disclosed and when it is, it is only for a lawful and specific purpose. <sup>66</sup>
<b>3-PA6:</b> Retention of registration data  Note, this PA is not represented on the data elements table, because data processed above represents what data elements will be retained  (Charter Questions 2g)	ICANN Registrars Registries	N/A – A retention period of registration data is not required to meet the intent of this purpose.

**Data Flow Map:**



<sup>66</sup> idem

**PURPOSE:**

Enable communication with the Registered Name Holder on matters relating to the Registered Name.

**Data Elements Matrix:**

R = required

O-RNH, O-Rr, O-CP = optional

N/A=not applicable

Data Element (Collected & Generated*)	Collection 3-PA1	Transmission 3-PA2	Publication (registry) 3-PA4	Publication (registrar) 3-PA4	Redaction 3-PA5
Domain Name	R	R	R	R	No
Registry Domain ID*		R	R	R	Yes
Registrar Whois Server*	R	R	R	R	No
Registrar URL*	R	R	R	R	No
Updated Date*		R	R	R	No
Creation Date*		R	R	R	No
Registry Expiry Date*		R	R	R	No
Registrar Registration Expiration Date*	O-Rr	O-CP	O-CP	O-CP	No
Registrar*	R	R	R	R	No
Registrar IANA ID*	R	R	R	R	No
Registrar Abuse Contact Email*	R	R	R	R	No
Registrar Abuse Contact Phone*	R	R	R	R	No
Reseller*	O-Rr	O-CP	O-CP	O-CP	No
Domain Status(es)*	R	R	R	R	No
Registry Registrant ID*		R	R	R	Yes
Registrant Fields					
<input checked="" type="checkbox"/> Name	R	O-CP	O-CP	R	Yes
<input checked="" type="checkbox"/> Organization (opt.)	O-RNH	O-CP	O-CP	O-CP	Yes <sup>67</sup>
<input checked="" type="checkbox"/> Street	R	O-CP	O-CP	R	Yes
<input checked="" type="checkbox"/> City	R	O-CP	O-CP	R	Yes <sup>68</sup>
<input checked="" type="checkbox"/> State/province	R	O-CP	O-CP	R	No
<input checked="" type="checkbox"/> Postal code	R	O-CP	O-CP	R	Yes
<input checked="" type="checkbox"/> Country	R	O-CP	O-CP	R	No
<input checked="" type="checkbox"/> Phone	R	O-CP	O-CP	R	Yes

<sup>67</sup> Refer to Recommendation #10 about publication and redaction of the Organization field

<sup>68</sup> Refer to Recommendation #11 about the redaction of the city field.

Data Element (Collected & Generated*)	Collection 3-PA1	Transmission 3-PA2	Publication (registry) 3-PA4	Publication (registrar) 3-PA4	Redaction 3-PA5
<input type="checkbox"/> Phone ext (opt.)					
<input type="checkbox"/> Fax (opt.)					
<input type="checkbox"/> Fax ext (opt.)					
<input type="checkbox"/> Email	R	O-CP	O-CP	R	Yes <sup>69</sup>
2nd E-Mail address					
Admin ID*					
Admin Fields					
<input type="checkbox"/> Name					
<input type="checkbox"/> Organization (opt.)					
<input type="checkbox"/> Street					
<input type="checkbox"/> City					
<input type="checkbox"/> State/province					
<input type="checkbox"/> Postal code					
<input type="checkbox"/> Country					
<input type="checkbox"/> Phone					
<input type="checkbox"/> Phone ext (opt.)					
<input type="checkbox"/> Fax (opt.)					
<input type="checkbox"/> Fax ext (opt.)					
<input type="checkbox"/> Email					
Tech ID*		O-CP	O-CP	R	Yes
Tech Fields					
<input type="checkbox"/> Name	O-RNH	O-CP	O-CP	R	Yes
<input type="checkbox"/> Organization (opt.)					
<input type="checkbox"/> Street					
<input type="checkbox"/> City					
<input type="checkbox"/> State/province					
<input type="checkbox"/> Postal code					
<input type="checkbox"/> Country					
<input type="checkbox"/> Phone	O-RNH	O-CP	O-CP	R	Yes
<input type="checkbox"/> Phone ext (opt.)					
<input type="checkbox"/> Fax (opt.)					
<input type="checkbox"/> Fax ext (opt.)					
<input type="checkbox"/> Email	O-RNH	O-CP	O-CP	R	Yes <sup>70</sup>
NameServer(s)	O-RNH	O-CP	O-CP	O-CP	No
DNSSEC	O-RNH	O-CP	O-CP	O-CP	No

<sup>69</sup> Refer to recommendation #14 about how web forms and email addresses are used here for publication and communication.

<sup>70</sup> Refer to recommendation #14 about how web forms and email addresses are used here for publication and communication.

---

<b>Data Element (Collected &amp; Generated*)</b>	<b>Collection 3-PA1</b>	<b>Transmission 3-PA2</b>	<b>Publication (registry) 3-PA4</b>	<b>Publication (registrar) 3-PA4</b>	<b>Redaction 3-PA5</b>
Name Server IP Address(es)	O-RNH	O-CP	O-CP	O-CP	No
Last Update of Whois Database*		R	R	R	No

## 4A

**PURPOSE:**

--For Registrars Only--

Provide mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure of a Registrar or Registry Operator, or unavailability of a Registrar or Registry Operator, as described in the RAA and RA, respectively.

**Purpose Rationale:**

**1) If the purpose is based on an ICANN contract, cite the relevant section of the ICANN contracts that corresponds to the above purpose, if any.**

- Registrar Data Escrow Program: <https://www.icann.org/resources/pages/registrar-data-escrow-2015-12-01-en>
- Data Fields Source: <https://www.icann.org/en/system/files/files/rde-specs-09nov07-en.pdf>

Escrowing the data is supported by ICANN's mandate to provide for security and stability in the DNS and this purpose is primarily protecting the registrant's rights. Escrow exists because Registrants have a reasonable expectation of business continuity.

It is reasonable to expect that a DPA would consider the escrow of customer data critical to the delivery of the service being provided to be common business practice and legal under GDPR provided appropriate contractual relationships are in place with the escrow agent to ensure that the data, once transferred to the escrow agent is afforded appropriate protection.

While technical and business resiliency could be achieved via other mechanisms, the escrow of data necessary to deliver the service is a generally accepted practice that is likely to be considered necessary to achieve the purpose of "...safeguarding registered name holder's registration data in the event of a business or technical failure, or other unavailability..."

While all contracted parties that have to be compliant with GDPR need to make sure there are protections against data loss and mechanisms to enable swift data recovery, ICANN is operating at the global level where customers can register domain names with registrars globally and the registry operators are based in numerous jurisdictions, it is important to have interoperability of escrow agents. Requiring all contracted parties to use the same policies for both escrowing data and applying the same standards to escrow agents for making data available, is necessary for contingency planning at the global level.

**2) Is the purpose in violation with ICANN's bylaws?**

No, providing a safety net for registrants in the event of registry technical or business failure seems within ICANN's remit.

1.1(a)(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System ("DNS") and coordinates the development and implementation of policies concerning the registration of second-level

domain names in generic top-level domains ("gTLDs"). In this role, ICANN's scope is to coordinate the development and implementation of policies:

- For which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS including, with respect to gTLD registrars and registries, policies in the areas described in Annex G-1 and Annex G-2; and
- That are developed through a bottom-up consensus-based multistakeholder process and designed to ensure the stable and secure operation of the Internet's unique names systems.

The issues, policies, procedures, and principles addressed in Annex G-1 and Annex G-2 with respect to gTLD registrars and registries shall be deemed to be within ICANN's Mission.

**3) Are there any “picket fence” considerations related to this purpose?**

Only with respect to the data model(s) defined within RDDS/Whois consensus policies. Agreements between ICANN and escrow providers are not within scope of the picket fence.

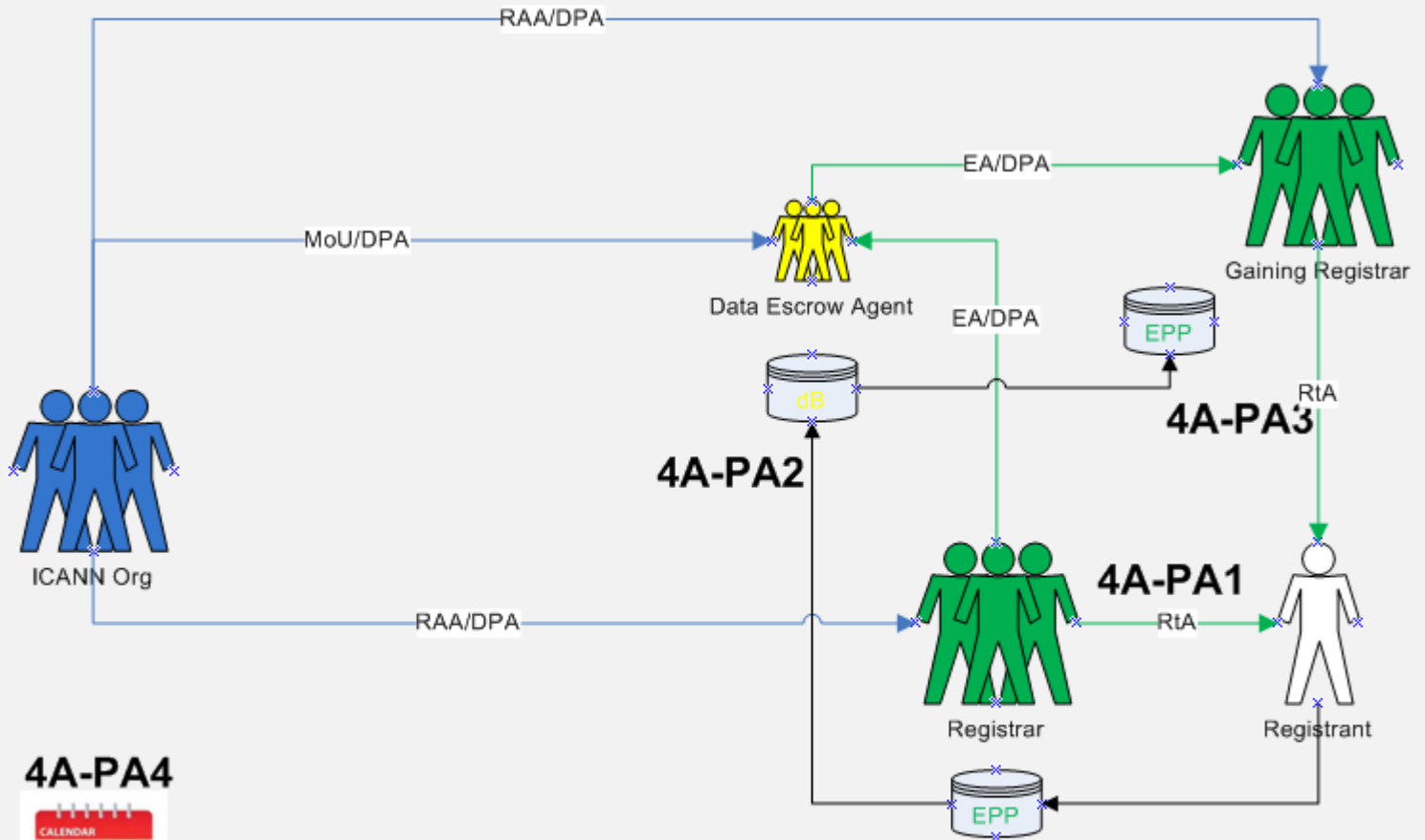
**Lawfulness of Processing Test:**

<b>Processing Activity:</b>	<b>Responsible Party:</b> <small>(Charter Questions 3k, 3l, 3m)</small>	<b>Lawful Basis:</b> <small>(Is the processing necessary to achieve the purpose?)</small>
<p><b>4A-PA1:</b> Collection of registration data by Registrar  (Charter Question 2b)</p>	<p>ICANN Registrars</p>	<p>6(1)(f)  This Processing Activity of Collection is not required to be documented within the Purpose for Registrar Escrow because the processing activity for transmission of registration data to the Data Escrow Agent (as noted below) has already been collected or generated from other ICANN Purposes that also contain processing activities for the collection of registration data.  However, the transparency of collection to the Registrant/Data Subject for the purpose of escrow is required. Refer to the Purpose for establishing the rights of the Registered Name Holder.</p>
<p><b>4A-PA2:</b> Transmission of registration data to Data Escrow Agent  (Charter Questions 2c, 2d, 2e, 2i)</p>	<p>ICANN Registrars Data Escrow Agent</p>	<p>This is a 6(1)(f) lawful basis because although there is likely a legitimate interest in providing mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure, or other unavailability of a Registrar or Registry Operator, it is not technically necessary to transmit data to an escrow agent in order to allocate a string to a registered name holder, and is therefore not necessary to perform the registration contract.</p>

<p><b>4A-PA3:</b> Disclosure of registration data to Gaining Registrar</p> <p>(Charter Questions 2f (gating questions), 2j)</p>	<p>ICANN Data Escrow Agent Gaining Registrar</p>	<p>This is a 6(1)(f) lawful basis because although there is likely a legitimate interest in providing mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure, or other unavailability of a Registrar or Registry Operator, it is not technically necessary to transmit data to an escrow agent in order to allocate a string to a registered name holder, and is therefore not necessary to perform the registration contract.</p> <p>Data is not made public for escrow purposes, but a transfer to the escrow agent and - in case of contingencies - the transfer to a Gaining Registrar is required to ensure that operations are not impaired.</p> <p>How and who ICANN chooses as the Gaining Registrar may have additional implications to the lawfulness should the Gaining Registrar not reside within the EU when the Losing Registrar did reside within the EU.</p>
<p><b>4A-PA4:</b> Retention of registration data by Data Escrow Agent</p> <p>Note, this PA is not represented on the data elements table, because data processed above represents what data elements will be retained</p> <p>(Charter Questions 2g)</p>	<p>ICANN Data Escrow Agent</p>	<p>This is a 6(1)(f) lawful basis due to the connection of Retention with Transmission of registration data to the Data Escrow Agent from the Registry.</p> <p>From the Escrow Specification (3.3.1.6), deposits to Third-Party Escrow Agents two copies are held for one year.</p> <p>Questions about the validity of the one year for TPP, noting that no retention is listed for ICANN approved vendors, given that once a new deposit occurs and is verified, it renders prior deposits useless.</p> <p>The EPDP also discussed that perhaps some minimal retention could be necessary from an overall continuity perspective.<sup>71</sup></p>

<sup>71</sup> Refer to the preliminary recommendation on Retention of Purpose E-Ry. A retention change should be validated to ensure technical requirements are not jeopardized by lowering the retention duration.

**Data Flow Map:**



**4A-PA4**



Current Policy: 1 Year

**PURPOSE:**

--For Registrars Only--

Provide mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure of a Registrar or Registry Operator, or unavailability of a Registrar or Registry Operator, as described in the RAA and RA, respectively.

**Data Elements Matrix:**

- R = required
- O-RNH, O-Rr, O-CP = optional
- N/A=not applicable



Data Element (Collected & Generated*)	Collection 4A-PA1	Transmission 4A-PA2	Disclosure 4A-PA3			
Domain Name	R	R <sup>72</sup>	R			
Registry Domain ID*						
Registrar Whois Server*						
Registrar URL*						
Updated Date*						
Creation Date*						
Registry Expiry Date*						
Registrar Registration Expiration Date*	O-Rr	R	R			
Registrar*	R	R	R			
Registrar IANA ID*						
Registrar Abuse Contact Email*						
Registrar Abuse Contact Phone*						
Reseller*	O-Rr	R	R			
Domain Status(es)*						
Registry Registrant ID*						
Registrant Fields						
<input checked="" type="checkbox"/> Name	R	R	R			
<input checked="" type="checkbox"/> Organization (opt.)						
<input checked="" type="checkbox"/> Street	R	R	R			
<input checked="" type="checkbox"/> City	R	R	R			
<input checked="" type="checkbox"/> State/province	R	R	R			
<input checked="" type="checkbox"/> Postal code	R	R	R			
<input checked="" type="checkbox"/> Country	R	R	R			
<input checked="" type="checkbox"/> Phone	R	R	R			
<input checked="" type="checkbox"/> Phone ext (opt.)	O-RNH	O-CP	O-CP			
<input checked="" type="checkbox"/> Fax (opt.)	O-RNH	O-CP	O-CP			
<input checked="" type="checkbox"/> Fax ext (opt.)	O-RNH	O-CP	O-CP			
<input checked="" type="checkbox"/> Email	R	R	R			
2nd E-Mail address						
Admin ID*						
Admin Fields						
<input checked="" type="checkbox"/> Name						
<input checked="" type="checkbox"/> Organization (opt.)						
<input checked="" type="checkbox"/> Street						
<input checked="" type="checkbox"/> City						
<input checked="" type="checkbox"/> State/province						

<sup>72</sup> Note, the fields identified here came from what is listed in the 2013 RAA, RDE Specification for Escrow. While a Registrar may process other data elements, only this minimal data set is required to recover registration data that is made ready for a Gaining Registrar to operate.

<b>Data Element (Collected &amp; Generated*)</b>	<b>Collection 4A-PA1</b>	<b>Transmission 4A-PA2</b>	<b>Disclosure 4A-PA3</b>			
<input type="checkbox"/> Postal code						
<input type="checkbox"/> Country						
<input type="checkbox"/> Phone						
<input type="checkbox"/> Phone ext (opt.)						
<input type="checkbox"/> Fax (opt.)						
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email						
Tech ID*						
Tech Fields						
<input type="checkbox"/> Name	O-RNH	O-CP	O-CP			
<input type="checkbox"/> Organization (opt.)						
<input type="checkbox"/> Street						
<input type="checkbox"/> City						
<input type="checkbox"/> State/province						
<input type="checkbox"/> Postal code						
<input type="checkbox"/> Country						
<input type="checkbox"/> Phone	O-RNH	O-CP	O-CP			
<input type="checkbox"/> Phone ext (opt.)						
<input type="checkbox"/> Fax (opt.)						
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email	O-RNH	O-CP	O-CP			
NameServer(s)						
DNSSEC						
Name Server IP Address(es)						
Last Update of Whois Database*						

## 4B

**PURPOSE:**

--For Registries Only--

Provide mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure of a Registrar or Registry Operator, or unavailability of a Registrar or Registry Operator, as described in the RAA and RA, respectively.

**Purpose Rationale:**

**1) If the purpose is based on an ICANN contract, cite the relevant section of the ICANN contracts that corresponds to the above purpose, if any.**

- Registry EBERO Program - <https://www.icann.org/resources/pages/ebero-2013-04-02-en>
- Registry Data Escrow Specification: <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html#specification2>
- Data Fields Sources:
  - <http://tools.ietf.org/html/draft-arias-noguchi-registry-data-escrow>
  - <https://tools.ietf.org/html/draft-arias-noguchi-dnrd-objects-mapping-09>

Escrowing the data is supported by ICANN's mandate to provide for security and stability in the DNS and this purpose is primarily protecting the registrant's rights. Escrow exists because Registrants have a reasonable expectation of business continuity.

It is reasonable to expect that a DPA would consider the escrow of customer data critical to the delivery of the service being provided to be common business practice and legal under GDPR provided appropriate contractual relationships are in place with the escrow agent to ensure that the data, once transferred to the escrow agent is afforded appropriate protection.

While technical and business resiliency could be achieved via other mechanisms, the escrow of data necessary to deliver the service is a generally accepted practice that is likely to be considered necessary to achieve the purpose of "...safeguarding registered name holder's registration data in the event of a business or technical failure, or other unavailability..."

While all contracted parties that have to be compliant with GDPR need to make sure there are protections against data loss and mechanisms to enable swift data recovery, ICANN is operating at the global level where customers can register domain names with registrars globally and the registry operators are based in numerous jurisdictions, it is important to have interoperability of escrow agents. Requiring all contracted parties to use the same policies for both escrowing data and applying the same standards to escrow agents for making data available, is necessary for contingency planning at the global level.<sup>73</sup>

<sup>73</sup> Draft Recommendation: Data processing agreements are necessary to ensure GDPR compliance. Recognizing that different escrow agreements exist depending on the TLD, the working group recommends that ICANN and/or the registry review the applicable escrow agreement and where necessary negotiate new GDPR compliant escrow agreements.

Within the Temporary Specification, EBERO is mentioned as Processing Activity under Appendix C. The Charter Question, Part 2i, tasks the EPDP to consider if this Processing Activity should be eliminated or adjusted. Based on initial research of the EBERO process, Registry Escrow is invoked as a component of the overall process with no indication that registration data other than what is identified here is transferred within any of the other EBERO components. The EPDP concluded that documentation of EBERO can be satisfied within the processing activities defined for this purpose of Registry Escrow.

**2) Is the purpose in violation with ICANN's bylaws?**

No, providing a safety net for registrants in the event of registry technical or business failure seems within ICANN's remit.

1.1(a)(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System ("DNS") and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("gTLDs"). In this role, ICANN's scope is to coordinate the development and implementation of policies:

- For which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS including, with respect to gTLD registrars and registries, policies in the areas described in Annex G-1 and Annex G-2; and
- That are developed through a bottom-up consensus-based multistakeholder process and designed to ensure the stable and secure operation of the Internet's unique names systems.

The issues, policies, procedures, and principles addressed in Annex G-1 and Annex G-2 with respect to gTLD registrars and registries shall be deemed to be within ICANN's Mission.

**3) Are there any “picket fence” considerations related to this purpose?**

Only with respect to the data model(s) defined within RDDS/Whois consensus policies. Agreements between ICANN and Data Escrow Providers are not within scope of the picket fence.

**Lawfulness of Processing Test:**

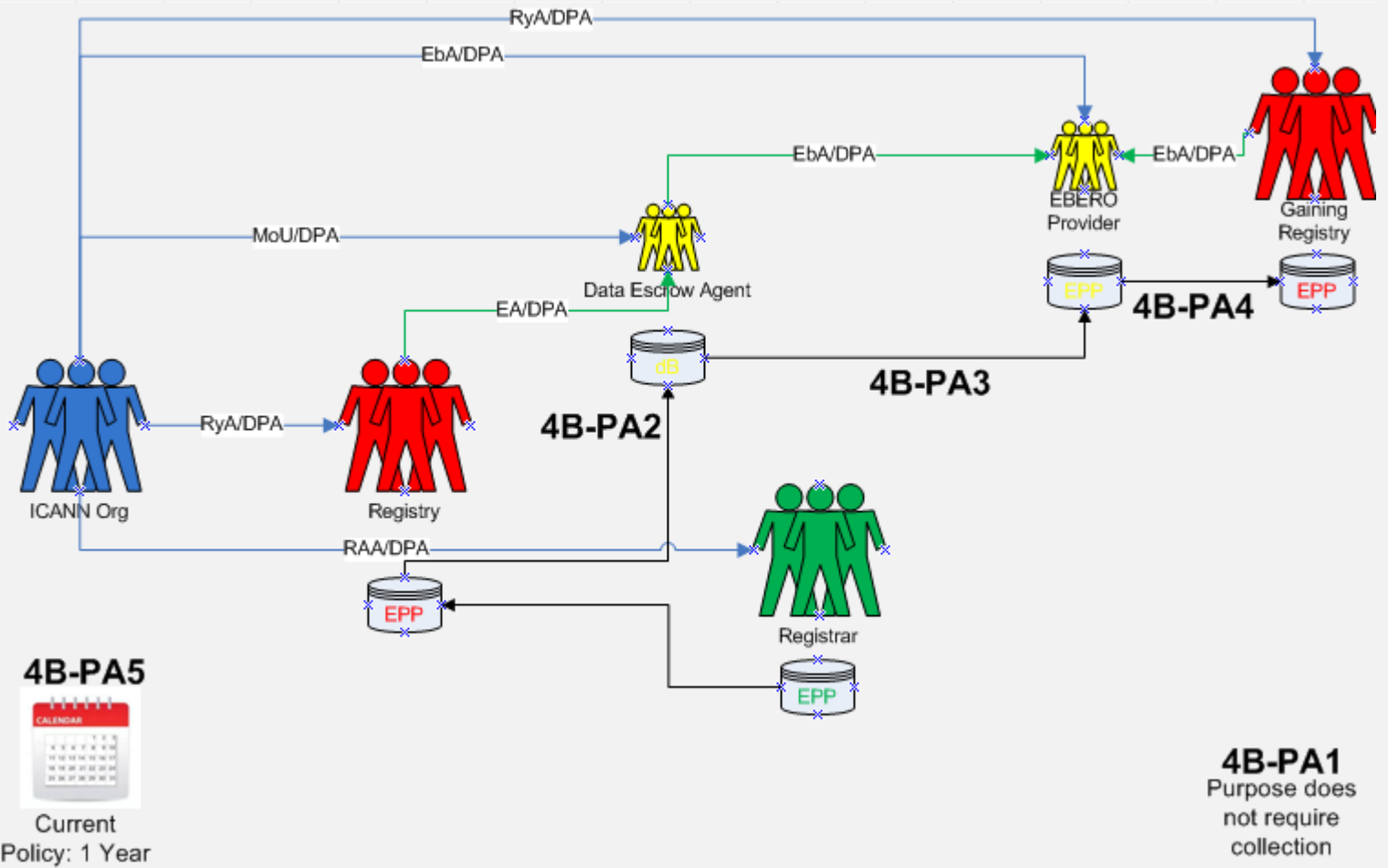
Processing Activity:	Responsible Party: <small>(Charter Questions 3k, 3l, 3m)</small>	Lawful Basis: (Is the processing necessary to achieve the purpose?)
<p><b>4B-PA1:</b> Collection of registration data by Registry  (Charter Question 2b)</p>	<p>ICANN Registries</p>	<p>6(1)(f) This Processing Activity of Collection is not required to be documented within the Purpose for Registry Escrow because the processing activity for transmission of registration data to the Data Escrow Agent (as noted below) has already been collected or generated from other ICANN Purposes that also contain Processing Activities for the transfer of registration data from the Registrar to the Registry.</p>

		<p>However, the transparency of collection to the Registrant/Data Subject for the purpose of escrow is required. Refer to the Purpose for establishing the rights of the Registered Name Holder.</p>
<p><b>4B-PA2:</b> Transmission of registration data to Data Escrow Agent  (Charter Questions 2c, 2d, 2e, 2i)</p>	<p>ICANN Registries Data Escrow Agent</p>	<p>This is a 6(1)(f) lawful basis because although there is likely a legitimate interest in providing mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure, or other unavailability of a Registrar or Registry Operator, it is not technically necessary to transmit data to an escrow agent in order to allocate a string to a registered name holder, and is therefore not necessary to perform the registration contract.</p>
<p><b>4B-PA3:</b> Disclosure of registration data to EBERO Provider  (Charter Questions 2f (gating questions), 2j)</p>	<p>ICANN Data Escrow Agent EBERO Provider</p>	<p>This is a 6(1)(f) lawful basis because although there is likely a legitimate interest in providing mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure, or other unavailability of a Registrar or Registry Operator, it is not technically necessary to transmit data to an escrow agent in order to allocate a string to a registered name holder, and is therefore not necessary to perform the registration contract.</p> <p>Specification 2, Part B “Legal Requirements”, #6 under “Integrity and Confidentiality” stipulates how the release of a deposit is made.</p> <p>How and who ICANN chooses as the EBERO Provider may have additional implications to the lawfulness should the EBERO Provider not reside within the EU when the Losing Registry did reside within the EU.</p>
<p><b>4B-PA4:</b> Disclosure of registration data to Gaining Registry  (Charter Questions 2f (gating questions), 2j)</p>	<p>ICANN EBERO Provider Gaining Registry</p>	<p>This is a 6(1)(f) lawful basis because although there is likely a legitimate interest in providing mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure, or other unavailability of a Registrar or Registry Operator, it is not technically necessary to transmit data to an escrow agent in order to allocate a string to a registered name holder, and is therefore not necessary to perform the registration contract.</p> <p>Specification 2, Part B “Legal Requirements”, #6 under “Integrity and Confidentiality” stipulates how the release of a deposit is made.</p>

<p><b>4B-PA5:</b> Retention of registration data by Data Escrow Agent</p> <p>Note, this PA is not represented on the data elements table, because data processed above represents what data elements will be retained</p> <p>(Charter Questions 2g)</p>	<p>ICANN Data Escrow Agent</p>	<p>This is a 6(1)(f) lawful basis due to the connection between the Retention processing activity with that of the Transmission of registration data to the Data Escrow Agent from the Registry.</p> <p>Specification 2, Part B “Legal Requirements”, #4 under “Integrity and Confidentiality” stipulates “(iii) keep and safeguard each Deposit for one (1) year.”</p> <p>Once a full escrow deposit has been successfully received and validated by the escrow agent, any previous deposits are obsolete and of no value. In the event of differential deposits, a 1-week retention would be required. The working group recommends that a 1 month minimum retention period by the escrow agent be established to provide an additional buffer against technical failure by the escrow agent.<sup>74</sup></p>
<p><b>4B-PA6:</b> Retention of registration data by EBERO Provider</p> <p>Note, this PA is not represented on the data elements table, because data processed above represents what data elements will be retained</p> <p>(Charter Questions 2g)</p>	<p>ICANN EBERO Provider</p>	<p>This processing activity needs to be investigated further. Refer to language listed under 4B-PA5.</p> <p>Current policy is one year.</p>

<sup>74</sup> This preliminary recommendation should be validated to ensure technical requirements are not jeopardized by lowering the retention duration.

**Data Flow Map:**



**PURPOSE:**

--For Registries Only--

Provide mechanisms for safeguarding Registered Name Holders’ Registration Data in the event of a business or technical failure of a Registrar or Registry Operator, or unavailability of a Registrar or Registry Operator, as described in the RAA and RA, respectively.

**Data Elements Matrix:**

R = required  
 O-RNH, O-Rr, O-CP = optional  
 N/A=not applicable

Data Element (Collected & Generated*)	Collection 4B-PA1	Transmission 4B-PA2	Disclosure 4B-PA3	Disclosure 4B-PA4		
Domain Name	R <sup>75</sup>	R	R	R		
Registry Domain ID*	R	R	R	R		
Registrar Whois Server*	R	R	R	R		
Registrar URL*	R	R	R	R		
Updated Date*	R	R	R	R		
Creation Date*	R	R	R	R		
Registry Expiry Date*	R	R	R	R		
Registrar Registration Expiration Date*	O-CP	O-CP	O-CP	O-CP		
Registrar*	R	R	R	R		
Registrar IANA ID*	R	R	R	R		
Registrar Abuse Contact Email*	R	R	R	R		
Registrar Abuse Contact Phone*	R	R	R	R		
Reseller*	O-CP	O-CP	O-CP	O-CP		
Domain Status(es)*	R	R	R	R		
Registry Registrant ID*	R	R	R	R		
Registrant Fields						
<input checked="" type="checkbox"/> Name	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Organization (opt.)	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Street	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> City	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> State/province	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Postal code	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Country	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Phone	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Phone ext (opt.)	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Fax (opt.)	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Fax ext (opt.)	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Email	O-CP	O-CP	O-CP	O-CP		
2nd E-Mail address						
Admin ID*						
Admin Fields						
<input checked="" type="checkbox"/> Name						
<input checked="" type="checkbox"/> Organization (opt.)						
<input checked="" type="checkbox"/> Street						
<input checked="" type="checkbox"/> City						

<sup>75</sup> Purpose E-Ry, Escrow for Registries depends on the collection of all registration data across all purposes. The 4B-PA1 column is populated based on the total complication of data collected across the six other purposes by Registries. Transparency of collection to the Registrant (Data Subject) is a requirement for purpose of escrow.



Data Element (Collected & Generated*)	Collection 4B-PA1	Transmission 4B-PA2	Disclosure 4B-PA3	Disclosure 4B-PA4		
<input checked="" type="checkbox"/> State/province						
<input checked="" type="checkbox"/> Postal code						
<input checked="" type="checkbox"/> Country						
<input checked="" type="checkbox"/> Phone						
<input checked="" type="checkbox"/> Phone ext (opt.)						
<input checked="" type="checkbox"/> Fax (opt.)						
<input checked="" type="checkbox"/> Fax ext (opt.)						
<input checked="" type="checkbox"/> Email						
Tech ID*	O-CP	O-CP	O-CP	O-CP		
Tech Fields						
<input checked="" type="checkbox"/> Name	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Organization (opt.)						
<input checked="" type="checkbox"/> Street						
<input checked="" type="checkbox"/> City						
<input checked="" type="checkbox"/> State/province						
<input checked="" type="checkbox"/> Postal code						
<input checked="" type="checkbox"/> Country						
<input checked="" type="checkbox"/> Phone	O-CP	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Phone ext (opt.)						
<input checked="" type="checkbox"/> Fax (opt.)						
<input checked="" type="checkbox"/> Fax ext (opt.)						
<input checked="" type="checkbox"/> Email	O-CP	O-CP	O-CP	O-CP		
NameServer(s)	O-RNH	O-CP	O-CP	O-CP		
DNSSEC	O-RNH	O-CP <sup>76</sup>	O-CP	O-CP		
Name Server IP Address(es)	O-RNH	O-CP	O-CP	O-CP		
Last Update of Whois Database*						
· Additional data elements as identified by Registry Operator in its registration policy, such as (i) status as Registry Operator Affiliate or Trademark Licensee [.MICROSOFT]; (ii) membership in community [.ECO]; (iii) licensing, registration or appropriate permits (.PHARMACY, .LAW) place of domicile [.NYC]; (iv) business entity or activity [.BANK, .BOT]	O-CP	O-CP	O-CP	O-CP		

<sup>76</sup> “DNSSEC” is not escrowed. Instead the related DNSKEY or DS records from which this field is derived must be escrowed.

## 5

**PURPOSE:**

- i) Handle contractual compliance monitoring requests and audit activities consistent with the terms of the Registry agreement and the Registrar accreditation agreements and any applicable data processing agreements, by processing specific data only as necessary;
- i) Handle compliance complaints initiated by ICANN, or third parties consistent with the terms of the Registry agreement and the Registrar accreditation agreements.

**Purpose Rationale:**

**1) If the purpose is based on an ICANN contract, cite the relevant section of the ICANN contracts that corresponds to the above purpose, if any.**

RA - <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html>

Registry:

2.2 Compliance with Consensus Policies and Temporary Policies

2.11 Contractual and Operational Compliance Audits

Specification 4, 3.1 Periodic Access to Thin Registration Data

Specification 11 Public Interest Commitments

RAA - <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>

Registrar:

Registrar Obligations - 3.4.3, 3.7.7

3.15 Registrar Self-Assessment and Audits

4.1 Compliance with Consensus Policies and Temporary Policies

Data Retention Specification, 2.

If a contractual compliance complaint is filed, the complainant provides certain information regarding the issue, which may contain personal data. Depending on the nature of the issue, ICANN Compliance may ask the Registrar or Registry Operator for the minimum data needed to investigate the complaint. Compliance may also look at the public WHOIS to supplement its review or processing.

For ICANN Contractual Compliance audits, ICANN sends audit questionnaires to Registry Operators and Registrars. In responding to the questionnaire, the Registry Operator and Registrar could include personal data in its responses. Further, to allow ICANN to carry out accuracy audits of registration contact data, ICANN may request from Registry Operators and Registrars the minimum data for randomly selected registrations.

Also, as part of Registry Operator audits, ICANN Contractual Compliance requests escrowed data to cross-reference information between data escrow and zone file and bulk registration data access for a sample of 25 domain names to ensure consistency.

**2) Is the purpose in violation with ICANN's bylaws?**

No. Per ICANN's Mission, Section 1.1(a)(i):

“..In this role, ICANN's scope is to coordinate the development and implementation of policies: ...That are developed through a bottom-up consensus-based multistakeholder process and designed to ensure the stable and secure operation of the Internet's unique names systems. ..The issues, policies, procedures, and principles addressed in Annex G-1 and Annex G-2 with respect to gTLD registrars and registries shall be deemed to be within ICANN's Mission.”

**3) Are there any “picket fence” considerations related to this purpose?**

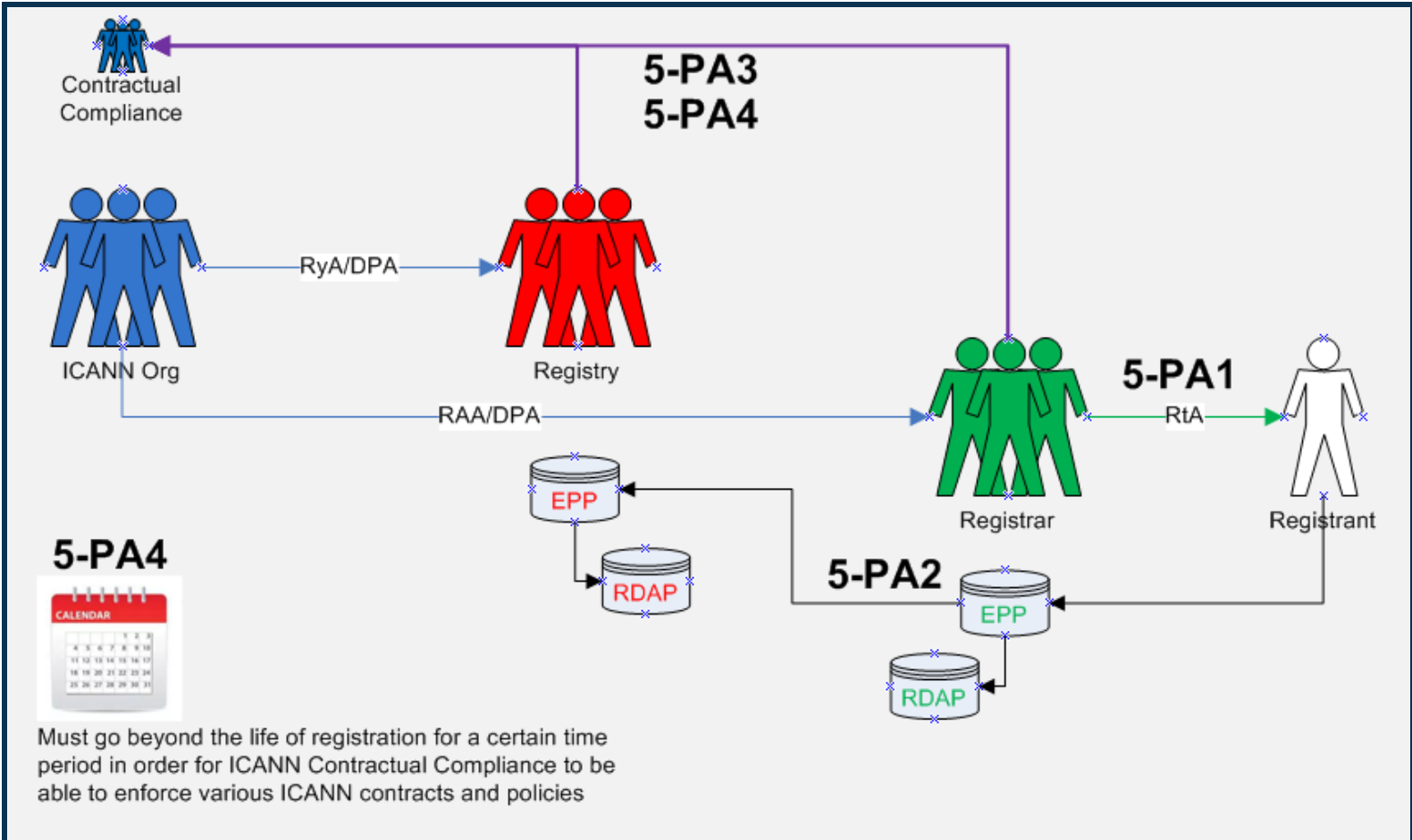
No. Registration Directory Services is within the “picket fence” as noted in ICANN Mission and Bylaws and contracts with ICANN to Registries and Registrars.

**Lawfulness of Processing Test:**

Processing Activity:	Responsible Party: (Charter Questions 3k, 3l, 3m)	Lawful Basis: (Is the processing necessary to achieve the purpose?)
<p><b>5-PA1:</b> Collection of registration data for compliance with ICANN contracts  (Charter Question 2b)</p>	<p>ICANN Registrars Registries</p>	<p>This is a 6(1)(f) purpose because although there may be a legitimate interest in collecting registration data for ICANN org compliance to confirm compliance with the RAA/RA, this collection is not technically necessary to perform the registration contract.</p> <p>The BC and IPC disagree that Purpose 5 is a 6(1)(f) purpose. The Team tentatively agreed to the following: (a) 6(1)(f) is an appropriate legal basis for the compliance purpose; (b) Some (BC and IPC) believe Purpose F may be a 6(1)(b); (c) There are concerns that 6(1)(f) may cause issues where the controller determines that the privacy rights outweigh the legitimate interest and therefore data cannot be provided.</p>
<p><b>5-PA2:</b> Transmission of registration data from Registrar to Registry  (Charter Questions 2c, 2d, 2e, 2i)</p>	<p>N/A</p>	<p>This is a 6(1)(f) purpose because although there may be a legitimate interest in collecting registration data for ICANN org compliance to confirm compliance with the RAA/RA, this transmission is not technically necessary to perform the registration contract.</p>
<p><b>5-PA3:</b> Transmission of registration data to ICANN org  (Charter Questions 2c, 2d, 2e, 2i)</p>	<p>N/A</p>	<p>This is a 6(1)(f) purpose because although there may be a legitimate interest in transmitting registration data to ICANN org compliance to confirm compliance with the RAA/RA, this transmission is not technically necessary to perform the registration contract.</p> <p>(Note: the requisite balancing test must be performed for each third-party type of disclosure and not for all registration data all the time.)</p>

<p><b>5-PA4:</b> Disclosure of registration data to ICANN org</p> <p>(Charter Questions 2f (gating questions), 2j)</p>	<p>N/A</p>	<p>This is a 6(1)(f) purpose because although there may be a legitimate interest in transmitting registration data to ICANN org compliance to confirm compliance with the RAA/RA, this disclosure is not technically necessary to perform the registration contract.</p> <p>(Note: the requisite balancing test must be performed for each third-party type of disclosure and not for all registration data all the time.)</p>
<p><b>5-PA5:</b> Retention of registration data by ICANN org</p> <p>Note, this PA is not represented on the data elements table, because data processed above represents what data elements will be retained</p> <p>(Charter Questions 2g)</p>	<p>ICANN</p>	<p>May go beyond the life of registration in order to complete accuracy audit and compliance processing, not to exceed one year.</p>

**Data Flow Map:**



**PURPOSE:**

- i) Handle contractual compliance monitoring requests and audit activities consistent with the terms of the Registry agreement and the Registrar accreditation agreements and any applicable data processing agreements, by processing specific data only as necessary;
- ii) Handle compliance complaints initiated by ICANN, or third parties consistent with the terms of the Registry agreement and the Registrar accreditation agreements.

**Data Elements Matrix:**

R = required  
 O-RNH, O-Rr, O-CP = optional  
 N/A=not applicable

The data element designations below are not “automatic” transmission and disclosure activities as documented in Purposes 1, 3 and 4, that occur every time with every domain registration. Rather, these activities are processed as needed in accordance with the contracts.

Data Element (Collected & Generated*)	Collection 5-PA1	Transmission 5-PA2	Transmission (to ICANN) 5-PA3	Disclosure (to ICANN) 5-PA4		
Domain Name	R	R	R	R		
Registry Domain ID*		R	R	R		

Data Element (Collected & Generated*)	Collection 5-PA1	Transmission 5-PA2	Transmission (to ICANN) 5-PA3	Disclosure (to ICANN) 5-PA4		
Registrar Whois Server*	R	R	R	R		
Registrar URL*	R	R	R	R		
Updated Date*		R	R	R		
Creation Date*		R	R	R		
Registry Expiry Date*		R	R	R		
Registrar Registration Expiration Date*	O-Rr	O-CP	O-CP	O-CP		
Registrar*	R	R	R	R		
Registrar IANA ID*	R	R	R	R		
Registrar Abuse Contact Email*	R	R	R	R		
Registrar Abuse Contact Phone*	R	R	R	R		
Reseller*	O-Rr	O-CP	O-CP	O-CP		
Domain Status(es)*	R	R	R	R		
Registry Registrant ID*		R	R	R		
Registrant Fields						
<input checked="" type="checkbox"/> Name	R	O-CP	R	R		
<input checked="" type="checkbox"/> Organization (opt.)	O-RNH	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Street	R	O-CP	R	R		
<input checked="" type="checkbox"/> City	R	O-CP	R	R		
<input checked="" type="checkbox"/> State/province	R	O-CP	R	R		
<input checked="" type="checkbox"/> Postal code	R	O-CP	R	R		
<input checked="" type="checkbox"/> Country	R	O-CP	R	R		
<input checked="" type="checkbox"/> Phone	R	O-CP	R	R		
<input checked="" type="checkbox"/> Phone ext (opt.)	O-RNH	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Fax (opt.)	O-RNH	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Fax ext (opt.)	O-RNH	O-CP	O-CP	O-CP		
<input checked="" type="checkbox"/> Email	R	O-CP	R	R		
2nd E-Mail address						
Admin ID*						
Admin Fields						
<input checked="" type="checkbox"/> Name						
<input checked="" type="checkbox"/> Organization (opt.)						
<input checked="" type="checkbox"/> Street						
<input checked="" type="checkbox"/> City						
<input checked="" type="checkbox"/> State/province						
<input checked="" type="checkbox"/> Postal code						
<input checked="" type="checkbox"/> Country						
<input checked="" type="checkbox"/> Phone						
<input checked="" type="checkbox"/> Phone ext (opt.)						

Data Element (Collected & Generated*)	Collection 5-PA1	Transmission 5-PA2	Transmission (to ICANN) 5-PA3	Disclosure (to ICANN) 5-PA4		
<input type="checkbox"/> Fax (opt.)						
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email						
Tech ID*		O-CP	O-CP	OP-CP		
Tech Fields						
<input type="checkbox"/> Name	O-RNH	O-CP	O-CP	O-CP		
<input type="checkbox"/> Organization (opt.)						
<input type="checkbox"/> Street						
<input type="checkbox"/> City						
<input type="checkbox"/> State/province						
<input type="checkbox"/> Postal code						
<input type="checkbox"/> Country						
<input type="checkbox"/> Phone	O-RNH	O-CP	O-CP	O-CP		
<input type="checkbox"/> Phone ext (opt.)						
<input type="checkbox"/> Fax (opt.)						
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email	O-RNH	O-CP	O-CP	O-CP		
NameServer(s)	O-RNH	O-CP	O-CP	O-CP		
DNSSEC	O-RNH	O-CP	O-CP	O-CP		
Name Server IP Address(es)	O-RNH	O-CP	O-CP	O-CP		
Last Update of Whois Database*		R	R	R		

## 6

**PURPOSE:**

Operationalize policies for the resolution of disputes regarding or relating to the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names), namely the UDRP, URS, PDDRP, RRDRP<sup>77</sup>, and the TDRP.

**Purpose Rationale:**

**1) If the purpose is based on an ICANN contract, cite the relevant section of the ICANN contracts that corresponds to the above purpose, if any.**

- RAA - <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>
  - Section 3.8
- RyA - <https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html>
  - Specification 7

ICANN Org to provide EPDP Team with copy of agreements with UDRP/URS providers in relation to data protection / transfer of data as well as the relevant data protection policies that dispute resolution providers have in place.

Rights Protection Mechanisms (RPMs) provisions exist within both the Registry and Registrar agreements as connected to ICANN Bylaws. This purpose is connected to Rights Protection Mechanisms of Uniform Dispute Resolution Mechanism (UDRP) and Uniform Rapid Suspension (URS), but it does not preclude RPMs that could be created or modified in the future.

RRDRP and PDDRP RPMs were also considered whether they should be connected to this purpose. Because these DRPs have not been tested, their inclusion here is to act as a marker for future consideration if/when they are used.

**2) Is the purpose in violation with ICANN's bylaws?**

No.

ICANN bylaws, Section 1.1(a)(i), as a part of "Mission" refer to Annexes G1 and G2. Annex G-1 contains a provision for Registrars, "resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names)" Annex G-2 also contains, "resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names)".

**3) Are there any "picket fence" considerations related to this purpose?**

<sup>77</sup> The PDDRP and RRDRP have yet to be invoked as a dispute procedure. As such, it's not clear exactly which data elements are required to process a complaint. The processing activities and data elements tables are completed with UDRP, URS and TDRP in mind.



Resolution of disputes regarding or relating to the registration of domain names (as opposed to the use of such domain names) are considered within the picket fence for the development of consensus policies. The purpose and the processing hereunder, as specified by the collection, transmission and disclosure of the data elements identified, are considered within the picket fence based upon the coordination, operationalization and facilitation of the dispute resolution mechanisms listed. The Temp Spec (Appendix D & E) now makes reference to who an RPM provider must contact based on Thick or Thin RDS to obtain registration data for the complaint.

**Lawfulness of Processing Test:**

<b>Processing Activity:</b>	<b>Responsible Party:</b> (Charter Questions 3k, 3l, 3m)	<b>Lawful Basis:</b> (Is the processing necessary to achieve the purpose?)
<p><b>6-PA1:</b> Collection of registration data to implement the UDRP, URS and TDRP</p> <p>(Charter Question 2b)</p>	<p>ICANN Registrars</p>	<p>This is a 6(1)(b) purpose because it is necessary to collect registration data in order to implement a UDRP or URS decision. For example, in the case of a UDRP/URS proceeding, the Registrant must agree to be bound by the UDRP/URS in order to register a domain name, so the collection of data for this purpose is necessary to fulfill the registration agreement.</p>
	<p>ICANN Registries</p>	<p>This is a 6(1)(f) purpose because ICANN and Registries do not have a direct contract with the registrant. The Registry must process data to fulfill its obligations regarding the RPMs, compliance with which are incorporated into the Registry Agreement.</p> <p>Under Article 6(1)(f) with regard to the URS and UDRP for registries and ICANN, because the processing is necessary for the purposes of pursued legitimate interests that are not overridden by the interests or fundamental rights and freedoms of the data subject.<sup>78</sup> With regard to this balancing test, we note that the contacts are important to ensure due process for the registrant so that they have notice of the proceedings and can avoid losing their domain name through a default.</p>
<p><b>6-PA1Z:</b> Collection of registration data to implement the RDDR and PDDR</p> <p>Note: these two DRPs are not represented on the data elements table below.</p>	<p>ICANN Registries Registrars</p>	<p>This is a 6(1)(f) with regard to the RDDR and PDDR for registrars, registries, and ICANN, because the processing is necessary for the purposes of pursued legitimate interests that are not overridden by the interests or fundamental rights and freedoms of the data subject.</p>

<sup>78</sup> Certain registrant contact information may be needed (e.g., in the UDRP context) for due process purposes in the registrant’s benefit.

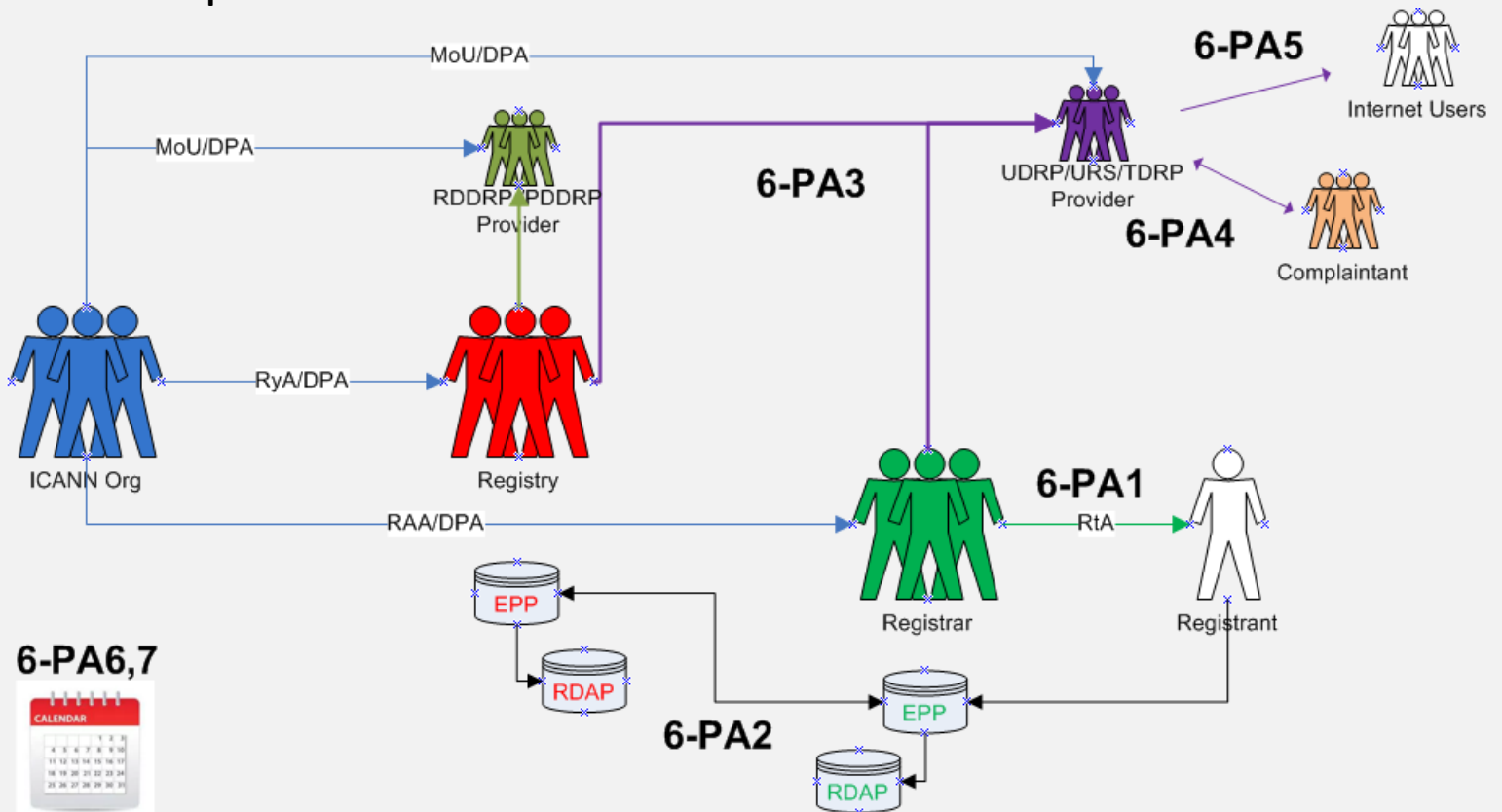
(Charter Question 2b)		
<b>6-PA2:</b> Transmission of registration data from Registrar to Registry	ICANN Registrars	This is a 6(1)(b) purpose because transmission of (at least minimal) registration data from the Registrar to the Registry is necessary to identify the Registrant for purposes of dispute resolution.
(Charter Questions 2c, 2d, 2e, 2i)	ICANN Registries	This is a 6(1)(f) purpose because although there is a legitimate interest in transmitting registration data to the Registry, this transmission is not technically necessary to perform the registration contract. The Registry must process data to fulfill its obligations regarding the RPMs and DRPs, compliance with which are incorporated into the Registry Agreement.
<b>6-PA3:</b> Transmission of registration data to Dispute Resolution Provider to administer the UDRP, URS, & TDRP	ICANN Registrars Registries Dispute Resolution Provider	6(1)(b) for Registrars 6(1)(f) for Registries and ICANN  This is a 6(1)(f) purpose because although there may be a legitimate interest in transmitting registration data to Dispute Resolution Providers, this transmission is not technically necessary to perform the registration contract.
(Charter Questions 2c, 2d, 2e, 2i)		
<b>6-PA3Z:</b> Transmission of registration data to Dispute Resolution Provider to administer the RDDRP and PDDRP	ICANN Registrars Registries Dispute Resolution Provider	6(1)(b) for Registrars 6(1)(f) for Registries and ICANN  This is a 6(1)(f) purpose because although there may be a legitimate interest in transmitting registration data to Dispute Resolution Providers, this transmission is not technically necessary to perform the registration contract.
Note: these two DRPs are not represented on the data elements table below.		
(Charter Questions 2c, 2d, 2e, 2i)		
<b>6-PA4:</b> Disclosure of registration data used for complaints to Complainant	ICANN Dispute Resolution Provider Complainant	6(1)(f). This activity allows for the filing of John Doe complaints and the ability to amend the complaint as needed with the proper Registrant data so that the proceeding can go forward. The provision of this data to the complainant is important to help ensure due process for the registrant: it allows the complainant to withdraw a URS/UDRP claim where it becomes clear from the identity of the registrant that they have a right or legitimate interest to use the name, or that they have not registered the name in bad faith. It also enables, in some
(Charter Questions 2f (gating questions), 2j)		

		<p>circumstances, requests to consolidate related claims, which has cost-saving benefits for all parties. In addition, the provision of this information to complainants supports case settlement (roughly 20% of cases) saving all parties time and expense.</p>
<p><b>6-PA5:</b> Publication of registration data used for complaints on Dispute Resolution Provider websites to Internet Users</p> <p>(Charter Questions 2f (gating questions), 2j)</p>	<p>ICANN Dispute Resolution Provider Internet Users</p>	<p>6(1)(f)</p> <p>WIPO’s GDPR FAQ: Paragraph 4(j) of the UDRP mandates that “[a]ll (successful and unsuccessful) decisions under this Policy will be published in full over the Internet, except when an Administrative Panel determines in an exceptional case to redact portions of its decision.” In this respect, through their acceptance of the applicable registration terms and conditions, domain name registrants subject to a UDRP proceeding are bound by this provision as well as the other UDRP terms. Publication of party names in UDRP decisions is essential to the overall functioning of the UDRP in that it helps to explain the panel’s findings, supports jurisprudential consistency, facilitates the conduct of other cases as appropriate, and furthermore can provide a deterrent effect. Against the background of the above-mentioned purposes, any request to redact a party’s name from a decision should normally be submitted for the panel’s consideration during the UDRP proceeding. Also in light of the above-mentioned reasons for full decision publication, any such request should be appropriately motivated.</p>
<p><b>6-PA6:</b> Retention of registration data used for complaints by Dispute Resolution Providers</p> <p>Note, this PA is not represented on the data elements table, because data processed above represents what data elements will be retained</p> <p>(Charter Questions 2g)</p>	<p>ICANN Dispute Resolution Provider</p>	<p>6(1)(f)</p> <p>The EPDP Team is not aware of any current data retention requirements by dispute resolution providers.</p> <p>Retention<sup>79</sup> of full registration data (See 6-PA3) by the Provider after the complaint has closed: Retention Period: TBD based on DRP data protection policies and transfer agreements in place between DRPs and ICANN.</p> <p>Retention of Complainant and Respondent data (See 6-PA5) such as Domain Name, Registrar, Name, Organization, City,</p>

<sup>79</sup> It is difficult to know what the appropriate retention period should be, but on occasion a query from a losing registrant is sent claiming they were not aware of the complaint, and in those situations it is useful to be able to provide copies of correspondence which includes contact information and email address.

		<p>State Country, on the Provider Site displaying closed complaints: Retention Period: TBD based on DRP data protection policies and transfer agreements in place between DRPs and ICANN.</p>
<p><b>6-PA7:</b> Retention of registration data used for complaints by Complainants</p> <p>Note, this PA is not represented on the data elements table, because data processed above represents what data elements will be retained</p> <p>(Charter Questions 2g)</p>	<p>ICANN Dispute Resolution Provider</p>	<p>This processing activity is listed because the role of the Complainant is defined in the Processing Activity 6-PA4.</p> <p>The IPC believes this Processing Activity is out of scope and should be deleted. This has yet to be explored in detail by the EPDP Plenary.</p>

**Data Flow Map:**



**6-PA6,7**



Refer to PAs for retention

**PURPOSE:**

Operationalize policies for the resolution of disputes regarding or relating to the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names), namely the UDRP, URS, PDDRP, RRDRP, and the TDRP.

**Data Elements Matrix:**

R = required

O-RNH, O-Rr, O-CP = optional

N/A=not applicable

Data Element (Collected & Generated*)	Collection 6-PA1	Transmission 6-PA2	Transmission 6-PA3	Disclosure 6-PA4	Publication 6-PA5	
Domain Name	R	R	R	R	R	
Registry Domain ID*						
Registrar Whois Server*	R	R	R	R		
Registrar URL*	R	R	R	R		
Updated Date*			R	R		
Creation Date*			R	R		
Registry Expiry Date*			R	R		
Registrar Registration Expiration Date*	O-Rr	O-CP	O-CP	R		
Registrar*	R	R	R	R	R	
Registrar IANA ID*	R	R	R	R		
Registrar Abuse Contact Email*	R	R	R	R		
Registrar Abuse Contact Phone*	R	R	R	R		
Reseller*	O-Rr	O-CP	O-CP	R		
Domain Status(es)*	R	R	R	R		
Registry Registrant ID*						
Registrant Fields						
<input checked="" type="checkbox"/> Name	R	O-CP	R	R	R	
<input checked="" type="checkbox"/> Organization (opt.)	O-RNH	O-CP	O-CP	R	R	
<input checked="" type="checkbox"/> Street	R	O-CP	R	R		
<input checked="" type="checkbox"/> City	R	O-CP	R	R	R	
<input checked="" type="checkbox"/> State/province	R	O-CP	R	R	R	
<input checked="" type="checkbox"/> Postal code	R	O-CP	R	R		
<input checked="" type="checkbox"/> Country	R	O-CP	R	R	R	
<input checked="" type="checkbox"/> Phone	R	O-CP	R	R		
<input checked="" type="checkbox"/> Phone ext (opt.)	O-RNH	O-CP	O-CP	R		
<input checked="" type="checkbox"/> Fax (opt.)	O-RNH	O-CP	O-CP	R		
<input checked="" type="checkbox"/> Fax ext (opt.)	O-RNH	O-CP	O-CP	R		
<input checked="" type="checkbox"/> Email	R	O-CP	R	R		
2nd E-Mail address						

Data Element (Collected & Generated*)	Collection 6-PA1	Transmission 6-PA2	Transmission 6-PA3	Disclosure 6-PA4	Publication 6-PA5	
Admin ID*						
Admin Fields						
<input type="checkbox"/> Name						
<input type="checkbox"/> Organization (opt.)						
<input type="checkbox"/> Street						
<input type="checkbox"/> City						
<input type="checkbox"/> State/province						
<input type="checkbox"/> Postal code						
<input type="checkbox"/> Country						
<input type="checkbox"/> Phone						
<input type="checkbox"/> Phone ext (opt.)						
<input type="checkbox"/> Fax (opt.)						
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email						
Tech ID*						
Tech Fields						
<input type="checkbox"/> Name						
<input type="checkbox"/> Organization (opt.)						
<input type="checkbox"/> Street						
<input type="checkbox"/> City						
<input type="checkbox"/> State/province						
<input type="checkbox"/> Postal code						
<input type="checkbox"/> Country						
<input type="checkbox"/> Phone						
<input type="checkbox"/> Phone ext (opt.)						
<input type="checkbox"/> Fax (opt.)						
<input type="checkbox"/> Fax ext (opt.)						
<input type="checkbox"/> Email						
NameServer(s)	O-RNH	O-CP	O-CP	R		
DNSSEC						
Name Server IP Address(es)						
Last Update of Whois Database*			R	R		

# 7

**PURPOSE:**

Enabling validation to confirm that Registered Name Holder meets gTLD registration policy eligibility criteria voluntarily adopted by Registry Operator and that are described or referenced in the Registry Agreement for that gTLD.<sup>80</sup>

**Purpose Rationale:**

**1) If the purpose is based on an ICANN contract, is this lawful as tested against GDPR and other laws?**

Yes. Registry Agreement allows Registry Operators to establish, publish, and adhere to clear registration policies (e.g., Spec. 11, 3(d); Spec. 12; Spec. 13). See also ICANN Bylaws (Art. 1.1(a)(i) and Annex G-2). Enabling validation to confirm that Registered Name Holder meets registration policy eligibility criteria introduces innovation and differentiation in the gTLD space.

**2) Is the purpose in violation with ICANN's bylaws?**

No. This purpose is consistent with ICANN’s Mission of coordinating the development and implementation of policies concerning the registration of second-level domain names in gTLDs (Introduction of New gTLDs and Applicant Guidebook), and principles for allocation of registered names in a TLD (Annex G-2)

**3) Are there any “picket fence” considerations related to this purpose?**

This purpose is related to WHOIS, which is within the Picket Fence. Specifically, Specification 1 of the Registry Agreement (Section 3.1(b)(iv) and (v) and Specification 4 of the Registrar Accreditation Agreement both refer to categories of issues and principles of allocation of registered names in a TLD.

**Lawfulness of Processing Test:**

Processing Activity:	Responsible Party: <small>(Charter Questions 3k, 3l, 3m)</small>	Lawful Basis: (Is the processing necessary to achieve the purpose?)
<p><b>7-PA1:</b> Collecting specific data for Registry Agreement-mandated eligibility requirements</p> <p>(Charter Question 2b)</p>	<p>Registries</p>	<p>6(1)(b) (for ICANN, registrars- or Registry-mandated eligibility requirements) because it is necessary to collect specific Registrant data to confirm the registrant meets the specific requirements of the registration agreement, i.e., registrar needs to verify the registrant is a licensed attorney to register a .abogado domain name.</p> <p>6(1)(f) for Registries, which are not parties to the registration agreement, but process the data in accordance with the</p>

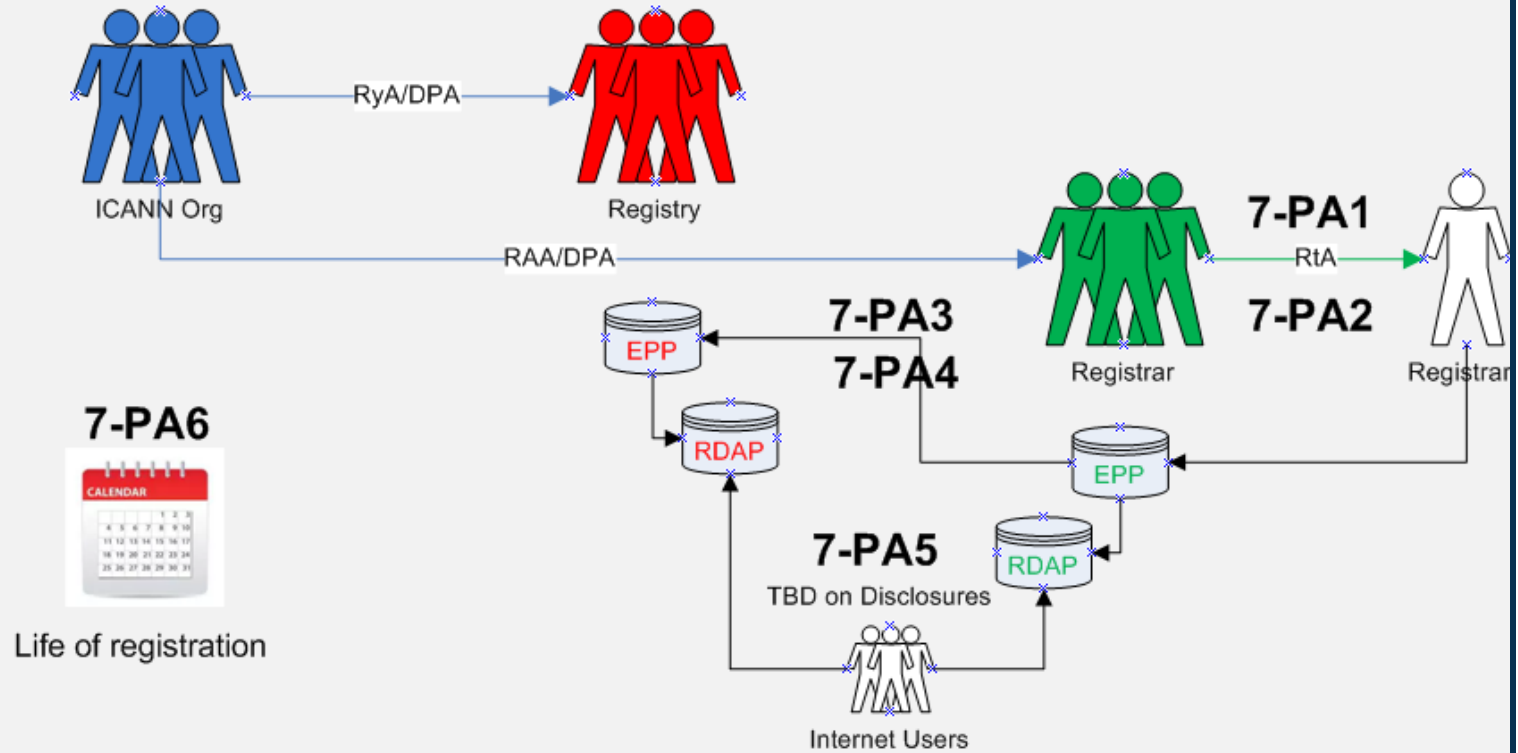
<sup>80</sup> The EPDP Team’s approval of Purpose 7 does not prevent and should not be interpreted as preventing Registry Operators from voluntarily adopting gTLD registration policy eligibility criteria that are not described or referenced in their respective Registry Agreements.

		obligations under the Registry-Registrar Agreement to allocate and activate domain names for registered name holders that meet the registration policy eligibility requirements
<p><b>7-PA2:</b> Collecting specific data for Registry Operator-adopted eligibility requirements</p> <p>(Charter Question 2b)</p>	Registries	<p>6(1)(b) for Registrars because it is necessary to collect specific registrant data to confirm the registrant meets the specific requirements of the registration agreement, i.e., registrar needs to verify the registrant is a licensed attorney to register a .abogado domain name</p> <p>6(1)(f) for Registries, which are not parties to the registration agreement, but process the data in accordance with the obligations under the Registry-Registrar Agreement to allocate and activate domain names for Registered Name Holders that meet the registration policy eligibility requirements</p>
<p><b>7-PA3:</b> Transfer of registration data from registrar to registry</p> <p>(Charter Questions 2c, 2d, 2e, 2i)</p>	RA-mandated eligibility requirements Registries	<p>6(1)(b) for Registrars because transfer from Registrar to Registry of registration data elements that demonstrate satisfaction of registration policy eligibility criteria is necessary so that the registry may validate satisfaction of eligibility criteria, and comply with ICANN audit requests.</p> <p>6(1)(f) for Registries. The transfer is necessary so that the Registry may validate satisfaction of eligibility criteria and comply with ICANN audit requests.</p>
<p><b>7-PA4:</b> Transfer of registration data from registrar to registry</p> <p>(Charter Questions 2c, 2d, 2e, 2i)</p>	Registry-adopted eligibility requirements Registries	<p>6(1)(b) for registrars because transfer from registrar to registry of registration data elements that demonstrate satisfaction of registration policy eligibility criteria is necessary so that the registry may validate satisfaction of eligibility criteria.</p> <p>6(1)(f) for registries. The transfer is necessary so that the registry may validate satisfaction of eligibility criteria and comply with ICANN audit requests.</p>
<p><b>7-PA5:</b> Disclosure of registration data to Internet Users</p> <p>(Charter Questions 2f (gating questions), 2j)</p>	Registries	<p>A lawful basis needs to be further investigated and can vary depending on the eligibility requirement.</p> <p>Some Registry Operators, as part of their business model, may require the publication as part of their eligibility requirements and perhaps published in the freely available RDDS as noted under Purpose 3.</p>



<p><b>7-PA6:</b> Retention of registration data</p>	<p>Registries</p>	<p>6(1)(f)</p>
<p>Note, this PA is not represented on the data elements table, because data processed above represents what data elements will be retained</p>		
<p>(Charter Questions 2g)</p>		

**Data Flow Map:**



**PURPOSE:**

Enabling validation to confirm that Registered Name Holder meets gTLD registration policy eligibility criteria voluntarily adopted by Registry Operator and that are described or referenced in the Registry Agreement for that gTLD.

**Data Elements Matrix:**

R = required  
 O-RNH, O-Rr, O-CP = optional  
 N/A=not applicable

Data Element (Collected & Generated*)	Collection 7-PA1	Collection 7-PA2	Transmission 7-PA3	Transmission 7-PA4	Disclosure 7-PA5	
Domain Name						
Registry Domain ID*						
Registrar Whois Server*						
Registrar URL*						
Updated Date*						
Creation Date*						
Registry Expiry Date*						
Registrar Registration Expiration Date*						
Registrar*						
Registrar IANA ID*						
Registrar Abuse Contact Email*						
Registrar Abuse Contact Phone*						
Reseller*						
Domain Status(es)*						
Registry Registrant ID*						
Registrant Fields						
· Name						
· Organization (opt.)						
· Street						
· City						
· State/province						
· Postal code						
· Country						
· Phone						
· Phone ext (opt.)						
· Fax (opt.)						
· Fax ext (opt.)						
· Email						
2nd E-Mail address						
Admin ID*						
Admin Fields						
· Name						
· Organization (opt.)						
· Street						
· City						
· State/province						
· Postal code						
· Country						
· Phone						

Data Element (Collected & Generated*)	Collection 7-PA1	Collection 7-PA2	Transmission 7-PA3	Transmission 7-PA4	Disclosure 7-PA5	
· Phone ext (opt.)						
· Fax (opt.)						
· Fax ext (opt.)						
· Email						
Tech ID*						
Tech Fields						
· Name						
· Organization (opt.)						
· Street						
· City						
· State/province						
· Postal code						
· Country						
· Phone						
· Phone ext (opt.)						
· Fax (opt.)						
· Fax ext (opt.)						
· Email						
NameServer(s)						
DNSSEC						
Name Server IP Address(es)						
Last Update of Whois Database*						
Other Data:						
· Additional data elements as identified by Registry Operator in its registration policy, such as (i) status as Registry Operator Affiliate or Trademark Licensee [.MICROSOFT]; (ii) membership in community [.ECO]; (iii) licensing, registration or appropriate permits (.PHARMACY, .LAW) place of domicile [.NYC]; (iv) business entity or activity [.BANK, .BOT]	O-CP	O-CP	O-CP	O-CP	O-CP	

# Annex E - Consensus Call Process and Designations

## Consensus Designations:

The Consensus designation were made in accordance with the Charter, balancing the bicameral and Stakeholder Group structure of the GNSO Council, the Charter identification of "groups" participating in the EPDP, and the inclusion and beneficial participation of Advisory Committees.

In the table below and consistent with the groupings identified in the Charter:

- NCSG, RrSG and RySG refer to the Non-Commercial, Registrar and Registry Stakeholder Groups respectively.
- BC, IPC and ISPC refer to the Business, Intellectual Property and Internet Service Provider Constituencies respectively that form the Commercial Stakeholder Group
- ALAC, GAC and SSAC refer to the At-Large, Governmental and Security & Stability Advisory Committees respectively.

Note the [BC / IPC minority statement](#). All other groups support the Final Report.

Also note that several Recommendations are designated as Full Consensus / Consensus. While no group disagreed with the Recommendation in these cases, the designation was made in deference to the significant compromise **made in developing this set of Recommendations**.

Purpose / Recommendation	Chair Proposed / Team Reviewed Designation	Groups Not Supporting Purpose / Recommendation
Purpose 1 – Establish the rights of a Registered Name Holder	Full Consensus / Consensus	
Purpose 2 – Maintaining SSR through enabling of lawful access	Consensus	IPC / BC
Purpose 3 – Enable communication with RNH	Full Consensus / Consensus	
Purpose 4 – Safeguarding RNH's Registration Data	Full Consensus / Consensus	
Purpose 5 – Handling Contractual Compliance	Full Consensus / Consensus	
Purpose 6 – Resolution of DRPs	Full Consensus / Consensus	
Purpose 7 – gTLD registration policy eligibility criteria	Consensus	NCSG
Recommendation #2 – Additional Purposes	Divergence	NCSG RySG RrSG

Purpose / Recommendation	Chair Proposed / Team Reviewed Designation	Groups Not Supporting Purpose / Recommendation
Recommendation #3 – Commitment to consider a system for Standardized Access to non-public Registration Data	Full Consensus / Consensus	
Recommendation #4 – Requirements related to accuracy	Full Consensus / Consensus	
Recommendation #5 – Data Elements to be collected by Registrars	Full Consensus / Consensus*	*Note: Consensus designation applies to data elements to be collected (except for the Tech Fields) and which data elements are optional for RNHs to provide. For the Tech Fields, there is no consensus on the issue of whether registrars are required to collect Tech Fields data.
Recommendation #6 – Consent to publish additional contact information	Full consensus / Consensus	
Recommendation #7 – Data elements to be transferred from Registrars to Registries	Full Consensus / Consensus	
Recommendation #8 – Escrow Providers	Full Consensus / Consensus	
Recommendation #9 – Contractual Compliance	Full Consensus / Consensus	
Recommendation #10 – Data redaction	Full Consensus / Consensus	
Recommendation #11 – City Field	Full Consensus / Consensus	
Recommendation #12 – Organization Field	Full Consensus / Consensus	
Recommendation #13 – Email Communication	Full Consensus / Consensus	
Recommendation #14 – Privacy/Proxy Registrations	Full Consensus / Consensus	
Recommendation #15 – Data Retention	Full Consensus / Consensus	
Recommendation #16 – Geographic Basis	Divergence	IPC / BC, SSAC ALAC

Purpose / Recommendation	Chair Proposed / Team Reviewed Designation	Groups Not Supporting Purpose / Recommendation
Recommendation #17 – Natural vs. Legal	Consensus	SSAC
Recommendation #18 – Requests for Lawful Disclosure	Consensus	IPC / BC
Recommendation #19 – Controller Agreement	Full Consensus / Consensus	
Recommendation #20	Full Consensus / Consensus	
Recommendation #21 – URS / UDRP	Full Consensus / Consensus	
Recommendation #22 – Instructions for RPM PDP WG	Full Consensus / Consensus	
Recommendation #23 – Data processing agreements with dispute resolution providers	Full Consensus / Consensus	
Recommendation #24 – Transfer Policy	Full Consensus / Consensus	
Recommendation #25 – Input to Transfer Policy review	Full Consensus / Consensus	
Recommendation #26 – Data processing agreements with non-Contracted Party entities involved in registration data processing	Full Consensus / Consensus	
Recommendation #27 – Impact on other policies	Full Consensus / Consensus	
Recommendation #28 – Implementation Transition Period	Full Consensus / Consensus	
Recommendation #29 – Admin Contact Transition	Full Consensus / Consensus	

# Annex F – Minority Statement

## BUSINESS CONSTITUENCY AND INTELLECTUAL PROPERTY CONSTITUENCY CONSENSUS STATEMENT ON EPDP PHASE 1 FINAL REPORT

The BC and IPC are staunch supporters of the ICANN bottom-up, consensus-driven multistakeholder model, as shown by BC and IPC’s good faith participation in this EPDP. Throughout this process both constituencies sought a *full consensus* result. The BC and IPC seek a robust multistakeholder process to drive full consensus that serves the public interest and protects consumers. All voices should be given due consideration, and initial disagreement should drive collaboration leading to true consensus. Purported consensus--where there actually is not consensus--would undermine ICANN’s bottom-up, consensus-driven multistakeholder model. That is an outcome the BC and IPC hope to avoid.

Accordingly, while we welcome progress made by the EPDP team and are thankful for the efforts of our colleagues and ICANN Org, we cannot support certain parts of the Final Report as set forth below. Our hope is that by clarifying our position, consistent with numerous BC and IPC statements on WHOIS, GDPR, and the Interim Report, the EPDP team will redouble its effort to achieve full consensus. We remain committed to working with the community and the EPDP team to develop policy that meets the needs of the full community and honors ICANN's commitment to ensure GDPR compliance while maintaining the existing WHOIS system to the greatest extent possible.

We look forward to constructive engagement on these remaining issues.

To support the EPDP Phase 1 Final Report, the IPC and BC require the following five amendments:

### **Recommendation #1: Purpose 2**

Purpose 2 of Recommendation 1 is insufficient for GDPR, and is inadequate to support Phase 2 work on Standardized Access (UAM). Specifically, Purpose 2 of Recommendation 1 must be revised as follows:

*“Contributing to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN’s mission through enabling lawful responses to reasonable disclosure requests related to ~~lawful data disclosure requests.~~ <sup>(3)</sup> consumer protection, cybersecurity, intellectual property, or law enforcement.”*

**Recommendation #18: Requests for Lawful Disclosure** Recommendation #18 must be updated as follows:

Second, delivery of a properly-formed Reasonable Request for Lawful Disclosure to a Registrar or Registry Operator does NOT require automatic disclosure of information, **but requires a Registrar or Registry Operator to reasonably consider the request.**

Timeline & Criteria for Registrar and Registry Operator Responses:

- Response time for acknowledging receipt of a Reasonable Request for Lawful Disclosure. Without undue delay, but not more than two (2) business days from receipt, unless shown circumstances does not make this possible.
- Requirements for what information responses should include. Responses where disclosure of data (in whole or in part) has been denied should include: rationale sufficient for the requestor to understand the reasons for the decision, including, for example, an analysis and explanation of how the balancing test was applied (if applicable).
- Logs of Requests, Acknowledgements and Responses should be maintained in accordance with standard business recordation practices so that they are available to be produced as needed including, but not limited to, for audit purposes by ICANN Compliance;
- Response time for a response to the requestor will occur without undue delay **and where 95% of responses occur within 15 days.** ~~and in any event within [X business] days of receipt of the request. (A finalized time frame to be set during implementation.)~~
- **A substantially shorter timeline** ~~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].

The suggested response time service level for disclosure requests (95% within 15 days) could be revisited if disclosure request volumes are excessive.

The EPDP Team recommends that the above be implemented and further work on defining these criteria commences as needed and as soon as possible.

#### **Recommendation #14 - Privacy/Proxy Registrations - Must be Updated and Clarified**

This Recommendation must take into account the eventual implementation of the Privacy/Proxy Services Accreditation Consensus Policy, allowing for the support for accredited services in addition to affiliated services. The current Recommendation #14 language must be amended as follows:

In the case of a domain name registration where an “affiliated **or accredited** ”\* privacy/proxy service used (e.g. where data associated with a natural person is masked), Registrar (and Registry where applicable) MUST include in the public RDDS and return in response to any query full non-personal RDDS data of the privacy/proxy service, which MAY also include the existing privacy/proxy pseudonymized email.

*In addition, the implementation of the Privacy/Proxy Services Accreditation Consensus Policy must be completed within 90 days after the adoption of the EPDP policy recommendations by the Board.*

#### **Recommendation #12 – Organization Field Implementation**

With respect to Organizational field data, Recommendation #12 must be updated as follows –



**Implementation advice:** the implementation review team should consider the following implementation model discussed by the EPDP Team:

For existing registrations, the first step will be to confirm the correctness / accuracy of the existing Organization field data.

For the period between the adoption of EPDP policy recommendations ~~and some future “date certain” to be determined by the implementation review~~ and one hundred and five (105) days thereafter, consisting of forty-five (45) days for implementation procedural set-up to be devised and agreed to and sixty (60) days for implementation:

### **Recommendations #16 and #17: Scope of application for Geographic Distinction and Natural vs. Legal**

Update to Recommendation #16:

- 1) The EPDP Team recommends that Registrars and Registry Operators are permitted to differentiate between registrants on a geographic basis, but are not obligated to do so.
- 2) The EPDP Team recommends that as soon as possible ICANN Org undertakes a study with respect to geographic distinctions, similar to the study already contemplated in Rec 17 below.
- 3) The EPDP Team will determine and resolve the issue of geographic distinction in Phase 2.

Update to Item 3 of Recommendation #17:

- 1) The EPDP Team recommends that the policy recommendations in this Final Report apply to all gTLD registrations, without requiring Registrars or registries to differentiate between registrations of legal and natural persons, although registrars and registries are permitted to make this distinction.
- 2) The EPDP Team recommends that as soon as possible ICANN Org undertakes a study, for which the terms of reference are developed in consultation with the community, that considers:
  - \_The feasibility and costs including both implementation and potential liability costs of differentiating between legal and natural persons;
  - \_Examples of industries or other organizations that have successfully differentiated between legal and natural persons;
  - \_Privacy risks to registered name holders of differentiating between legal and natural persons; and
  - \_Other potential risks (if any) to registrars and registries of not differentiating.
- 3) The EPDP Team will ~~discuss~~ determine and resolve the Legal vs. Natural issue in Phase 2. ~~Depending on the timing of the research, its discussions may inform the scope of research and/or use its findings.~~

### **Additional Concerns:**

We agree with concerns expressed by ALAC regarding Thick Whois. A middle ground may be to have currently-thick TLDs remain thick, and permit currently-thin gTLDs to stay thin.

There are no assurances of verification for data accuracy in non-redacted WHOIS fields, nor any requirement to respect a registrant's consent to publish his or her contact information.

## Annex G – EPDP Team Group Statements

SECURITY AND STABILITY ADVISORY COMMITTEE (SSAC)

AT-LARGE ADVISORY COMMITTEE (ALAC)

NON-COMMERCIAL STAKEHOLDER GROUP (NCSG)

REGISTRY STAKEHOLDER GROUP (RySG)

INTERNET SERVICE PROVIDERS AND CONNECTIVITY PROVIDERS CONSTITUENCY (ISPCP)

GOVERNMENTAL ADVISORY COMMITTEE

## SECURITY AND STABILITY ADVISORY COMMITTEE (SSAC)

Recommendation #3 (Formerly #2) - Commitment to consider a system for Standardized Access to non-public Registration Data and Purpose 2

SSAC supports the sentiment behind Recommendation 2, but not the language. The language is flawed and does not provide a clear and actionable recommendation to the GNSO Council and the ICANN Board. SSAC takes this opportunity to clarify intent and urge that the problems with the language be fixed.

SSAC believes that the ePDP team shared a common sentiment: that policy-making regarding lawful access of non-public data should definitely proceed now that the gating factors have been addressed. SSAC supports that sentiment.

There are three problems with Recommendation 2's language:

- A. It says the group makes a recommendation but then does not say what the recommendation is. It should clearly recommend that further policy development on the topic take place. The current ambiguity leaves open the prospect that the Recommendation will be misunderstood.
- B. Recommendation 2 says that "the EPDP team will consider amongst other issues, disclosure in the course of intellectual property infringement and DNS abuse cases." But that is technically not possible, because the current ePDP is expiring and this ePDP team cannot consider further issues. Council will need to authorize a new or add-on policy process to complete the unfinished work from the current ePDP.
- C. It does not address timing or urgency. The issues were included in the current ePDP's charter and were supposed to be addressed already but remain unfinished. The open issue is vital to security and stability, and in SAC104 the SSAC has urged the Council to adopt an ambitious deadline to complete this work.

We therefore suggest that the first part of the recommendation be something more clear and actionable, such as:

"The EPDP Team recommends that the Council immediately authorize an additional ePDP to consider a system for Standardized Access to non-public Registration Data (referred to in the Charter as 'Standardised Access'). This should be designed to fulfill undelivered work items contained in the present EPDP Team Charter. It will be in line with Purpose #2, and is possible to begin because the gating questions in the charter have been answered."<sup>81</sup>

---

<sup>81</sup> The above comments are based on statements endorsed by the entire SSAC, found in:

\* SAC101 Recommendation 1A: "ICANN policy-making should result in a domain registration data policy, including statements of purposes for the collection and publication of the data."

\* SAC101 Recommendation 1D: "The ICANN Board should support the creation of an accredited RDDS access program, with the ICANN Organization ensuring the creation, support of, and oversight of the supporting technical access mechanism. This program will identify qualified users, enable their access under appropriate data protection measures, and will allow RDDS server operators to manage those users' access accordingly. The technical access mechanism should include a credential management system so that users do not need to negotiate and set up access with RDDS operators individually."

\* SAC101 Recommendation 3: "The ICANN Board and EPDP policy-makers should ensure that security practitioners and law enforcement authorities have access to domain name contact data, via RDDS, to the full extent allowed by applicable law."

\* SAC104: "The SSAC urges the GNSO to begin planning further efforts now, to complete the policy-making that has been started. It is vital to keep momentum. Driven by the GDPR, the EPDP is finally addressing some long-delayed issues. It will not serve the Internet community, or ICANN as a multistakeholder organization, if the work is allowed to drift. We urge the GNSO to begin planning next steps, with specific deliverables and ambitious deadlines for completion." (Section 2.3)

Recommendation #4 (Formerly #3) - **Requirements related to accuracy – SSAC joins consensus with this Recommendation, but SSAC requests that the following statement be added to the Final Report for the GNSO Council to review:**

As explained in SAC104 Section 3.2: [FOOTNOTE

TO: <https://www.icann.org/en/system/files/files/sac-104-en.pdf> [icann.org]]

“Here the EPDP WP makes a recommendation about data accuracy, but so far the EPDP team has not fully explored the data accuracy requirements of the GDPR, and whether the procedures in the 2013 Registrar Accreditation Agreement (RAA) and the Temp Spec are GDPR-compliant. That needs to be done.

A vital ICANN policy is the accuracy complaint process, where third parties have the right to submit data accuracy complaints, and registrars and registrants must respond per the requirements. The accuracy complaint process has been a vital accountability and compliance mechanism that has helped stop and prevent numerous serious abuse and security issues. Historically, registration data inaccuracy complaints have come mainly from the public, who may have been directly or indirectly affected by abusive registrations and bad actors who provide bogus data. The inability of affected parties to see the data, and thus to make complaints, is an undesirable consequence under the Temp Spec. Accuracy requirements and procedures without the opportunity to effectively utilize them are worthless.

A balanced situation is needed. An accredited RDS access program will allow examination of the data and challenges by parties who are pre-qualified and responsible actors, and some better requirements around reasonable access would assist non-accredited parties and would also be part of a balanced solution.” SSAC recommends that an accredited RDS access program is essential and that it be discussed in Phase 2 “with specific deliverables and ambitious deadlines for completion.”

**Recommendation #5 (old #4) - Data elements to be collected by Registrars – SSAC concurs with the recommendation with the understanding that Registrars must support / process Tech Contact data if it is provided by the RNH**

**Explanation:**

There is some confusion whether Recommendation 5 requires registrars to offer the Tech Contact fields to their Registered Name Holders or not. This is because Recommendation 5's table marks the Tech Contact fields as mandatory to collect, but Recommendation 5 also says "if the Registrar provides this option".

SSAC understands that there are legal requirements for collecting and transferring the Tech Contact data which will need to be discussed in the implementation phase.

SSAC believes that the ePDP Team's discussion was: Registrars MUST offer the Registered Name Holder the opportunity to provide Technical Contact data. Technical Contact data should be optional for the Registered Name Holder to provide. If Technical Contact data is provided to the registrar, the data must be provisioned to the registry. If that is what Recommendation 5 delivers, SSAC can endorse Recommendation 5. If Recommendation 5 does not deliver that, SSAC cannot endorse Recommendation 5.

**Recommendation #16** – Geographic Basis – **SSAC cannot support the recommendation as written (See Below)**

**Recommendation #17** – Natural vs. legal – **SSAC cannot support the recommendation as written (See Below)**

**Reasoning:**

Recommendations 16 and 17 have a negative effect on security and legitimate contactability. Recommendation 16 allows significant over-redaction of data not required by GDPR (or other laws currently in place), and enables a race to the bottom, allowing venue-shopping without respect to the actual location of registrars or registrants. Recommendation 17 enables ongoing redaction of information about legal persons that do not have the rights of natural persons. These outcomes are not balanced, and are neither necessary nor desirable. We believe that better, more balanced solutions – are both legally and technically possible and should be discussed.

It is the SSAC's position that:

- Recommendation 16: Registrars and Registry Operators must be obligated to differentiate between registrants on a geographic -- i.e. legal jurisdiction basis, after a suitable implementation period.
- Recommendation 17: Registrars and Registry Operators must be obligated to differentiate between registrations of legal and natural persons, after a suitable implementation period.

Regarding Recommendation 17:

- The EPDP Team will discuss the Legal vs. Natural issue in Phase 2, and SSAC looks forward to participating in that discussion.

Should Recommendation 17 be adopted by Council, SSAC notes that the study criteria in section #2 are unbalanced and must be updated. They assume that the main decision-making criteria are the costs and risks to contracted parties. The list is missing consideration of how policy affects third parties with legitimate interests, and how the law imposes new responsibilities (and therefore costs) on the Contracted Parties . As SAC104 notes: "The GDPR imposes certain new obligations and therefore risk and costs on registrars and registry operators. It has also imposed risk and

costs on the parties who rely upon domain registration data for the wide array of legitimate purposes. The GDPR calls for balancing and the accommodation of legitimate security interests, explicitly called out in Recital 49. ICANN policy should also provide balanced solutions. In some cases the Initial [and now the Final] Report asks what costs will be borne by the Contracted Parties, but does not also evaluate the costs on all other parties, or the cost of not putting a balanced solution into place. Cost or risk to registrars or registry operators alone is not a persuasive argument against balanced solutions."

**Supporting Documentation:**

SAC104: <https://www.icann.org/en/system/files/files/sac-104-en.pdf>

SAC101v2: <https://www.icann.org/en/system/files/files/sac-101-v2-en.pdf>

As SSAC stated in SAC104:

"The GDPR states clearly that it 'does not cover processing of personal data which concerns legal persons.' We recommend that registrars be required to deploy mechanisms that ensure a reliable declaration or determination of natural or legal person status for new registrations going forward,

and to eventually obtain those declarations or determinations for existing registrations and their registrants.

"Contact data associated with natural persons should be published in RDS where such is not prohibited by local law. In SAC101, SSAC stated: 'The new policy [The Temporary Specification] allows RDDS operators complete freedom to choose when to redact domain contact data from publication, whether or not a domain contact is protected by GDPR or by any other local privacy law. The result has been blanket redactions, hiding more data than is legally called for. A more balanced and justified approach is needed.. access should not be less timely, more restricted, and less public than law requires....

We also note that as of this writing, most ccTLD operators in the European Union continue to publish some (and sometimes all) contact data fields for domains registered by legal persons. Some continue to publish some personal data for natural person registrants in public WHOIS output.'

"SAC101 also highlights RIPE-NCC's solution, which allows for the publication of data about natural persons contained in the contact data for legal persons. This process provides mechanisms that RIPE-NCC says were specifically designed to comply with GDPR. The RIPE-NCC solution seems to be balanced in that it provides contactability and does not overapply the law. SSAC believes that RIPE's model deserves a full examination and neutral legal evaluation.... We also recommend the following:

1. Introduction of a policy requiring registrants to make a legal or natural person declaration.
2. Obtaining declaration would be mandatory for registrars to implement within a reasonable time.
3. A declaration would only be required during registration events, i.e. when a new domain is registered, or when an existing domain is renewed or transferred (by gaining registrar). This would eventually "fill in" status data about existing/historical registrations.
4. Registrar may make declaration on behalf of registrant if the registrar has reasonable knowledge of registrant's status and the registrant has not made a declaration of its own. This would be applicable to registrars with specific business models, for instance when they only process registrations on behalf of organizations where it is clear that the registrant falls into a particular category based on their relationship with the registrar.
5. Registrant may change its declaration at any time.
6. The absence of a declaration results in assumption that the registrant is a natural person; i.e. a default redaction of data.
7. Inaccurate declarations will be subject to a revised WHOIS inaccuracy complaint process."

## AT-LARGE ADVISORY COMMITTEE (ALAC)

### ALAC Statement for EPDP Phase 1 Final Report

As demonstrated by the ALAC's long history of participating in GNSO and ICANN working groups and other processes, we strongly support and contribute to the bottom-up multistakeholder model. The ALAC participation and contributions to the EPDP further illustrate that. Moreover, the ALAC understands that any process such as this will require all parties to accept compromises.

Our support of the generic processes notwithstanding, the ALAC has significant concerns that the EPDP has not adequately addressed the issues that are most important to fulfilling critical ALAC targets in relation to the GDPR:

- \_Maximizing access to RDDS information for those involved with cybersecurity and consumer protection;
- \_Maximizing stability and resiliency of a trustworthy DNS;
- \_Protecting and supporting individual Internet users; and
- \_Protecting Registrants

There are a number of recommendations with which the ALAC has very strong concerns, and others that we find problematic. We note that some of the descriptions that follow include implementation methodologies. This is not to say that the EPDP should work at that level of detail, but to demonstrate that viable solutions do exist.

To be specific, the results with which the ALAC has very strong concern are:

- Recommendation #16: The report recommends that contracted parties will not need to perform any level of geographic differentiation due to the difficulty of determining the location of the registrant and the risk of improperly attributing a location. Given that contracted parties have claimed that accuracy of RDDS data is not an issue, the declared location of the registrant should not be questionable. And contracted parties should be able to determine where their data is being processed! Given that this issue was declared settled and not even deferred until Phase 2, the ALAC has difficulty supporting this. The ALAC is aware that there is an open question regarding whether ICANN may be considered "established" in the EU and the EPDP has requested a legal opinion. Ultimately the European Data Protection Board (EDPB) may rule and that may force the issue, but until that happens, we should not pre-judge the outcome.
- Recommendation #5: One of the original bases for WHOIS and among its current usage is to enable contact to address technical issues. The recommendation allows registrars at their option to not collect technical contact information making it difficult for registrants to identify agents to whom they delegate technical responsibility. This impacts a range of users from novices who wish to delegate their web hosting service to address technical issues to large corporations that want 24/7 coverage to address technical matters. Among the reasons for doing so is that they cannot rely on a registrants declaration that the technical contact will allow such publication, but that ignores that a) only an anonymized address or web form would be published, and b) anyone who signs up for a mailing list is familiar with the technology asking the person who "signed up" whether they really want to do so – the same technology could be used by a registrar in this case.
- Embedded throughout the report is the concept that we will abandon the concept of Thick WHOIS. ICANN and the volunteer community recently spent considerable time and effort on the Thick WHOIS PDP which determined that there were substantial benefits to using the Thick model. This was discarded by the EPDP without due consideration of whether these benefits could justify the incorporation of this model into the GDPR solution. It was simply deemed to



be “non-conforming” with GDPR without addressing the underlying rationales and alternatives.

Issues which raise considerable but somewhat lesser concern:

- All contact with registrants or their agents will be via anonymized e-mail or through web forms unless the registrant explicitly requests direct communications. This will be true in many cases even for legal persons, because the permission to redact is allowed for them (unless reversed in Phase 2). However, the sender typically gets no indication that a message is even sent, not to mention confirmation that it reached its target. It is understood that the registrar (or registry if applicable) relaying the message (relay agent) has no way of ensuring that the message is received. But in many cases, a failure is returned to the relay agent. Contracted parties must use current best practices for such actions such as copying the message originator (not displaying the actual recipient address), including a message ID that can later be used for referencing the message (including asking for confirmation of whether a bounce was received that can be identified with the sent message). The ALAC also notes that registrar/registry privacy policies must guarantee that the content of the messages it forwards will be subject to stringent privacy rules and will not be used in any way.
- Recommendations #24/25: The Inter-Registrar Transfer Policy has been very significantly weakened by the Temporary Specification and that will now continue based on the EPDP recommendations. The report does advise the GNSO to address this with “great urgency”, but realistically IF the GNSO decides to charter a PDP to look at this, it will likely be 2-3 years before a solution can be implemented. That is not an acceptable risk for registrants.
- The RDDS Organization field will be redacted or deleted until a registrant approves it being displayed. Although not optimal, that solution would be acceptable if there were a guaranteed timeline associated with it.
- Recommendation #15: Data is to be retained for a period of no more than one year (with an additional cushion of 6 months to effect the deletion). The one year was based on the Transfer Dispute Resolution Process (TDRP) which gives a registrant one year to file a claim. But as a result, it is possible that the data could be deleted effectively as the claim is being filed – no buffer was allowed for processing the claim and protecting the registrant’s rights. A period marginally longer than 1 year would address this, with a requirement to address TDRPs within this period.
- Recommendation #6: Registrants will be able to specify that they wish their actual contact information published, but there is no timeline for registrars to allow this, and the data may only be published by the sponsoring registrar and not by the registry (if they have the data).

On a more global level, the EPD has spent an untold amount of time discussing possible contracted party liabilities and risks associated with improperly disclosing personal information. Very little time has been spent trying to understand the risks to the DNS, the Internet and its users of NOT disclosing information in some cases. A classic example of this mindset is recommendation #17 which says that the decision on whether to differentiate legal vs natural persons should be based solely on contracted party costs and risks, and registrant privacy issues. It recommends that no consideration be given to the impact on lawful access by third parties. This lack of balance cannot produce good policy.

The term “consumer protection” occurs five times in the Temp Spec. It is not used in the present report. “DNS Abuse” and “cybercrime” are also mentioned in the Temp Spec. “Cybercrime” is not mentioned the report, and there is one reference to addressing “DNS abuse” in Phase 2, but there is also a statement “that it would be difficult to argue that processing to prevent DNS abuse is “necessary for the performance of a contract to which the data subject is party”.

This lack of concern for public interest issues makes it VERY difficult to have confidence that these and other issues will be properly dealt with in Phase 2.

In determining the ALAC position on this Phase 1 Final Report, the ALAC and the EPDP At-Large support group considered our concerns over the particular issues noted here, and the concerns over how Phase 2 will be address the deferred issues as well as the access issue. An option we seriously considered was withdrawing support for the entire report based on the concerns outlined above.

Ultimately we decided we would raise objections to a small number of critical issues but would still support the report in general. We did this to demonstrate that we do support the multistakeholder process and despite concerns, we hope that the overall EPDP will consider the needs of the entire Internet community and not just focus on the needs of contracted parties and privacy advocates. What comes out of this process must be GDPR compliant. There is no question about that. But the GDPR should not be over applied and it must also allow the DNS to continue to function and to allow addressing issues of DNS abuse, cybercrime and consumer protection in a timely and effective manner.

**NCSG Comments for the annex of the final EPDP report**

The comments that follow pertain only to recommendations where the NCSG strongly disagrees or has important warnings or qualifications. Additional objections to other elements appearing in the report have been withheld due to our desire to reach a consensus policy.

**Recommendation #1:**

**Purposes:**

- Purpose 2: Disclosure of data to third parties. NCSG continues to maintain that disclosure to third parties is not a valid ICANN purpose for processing domain name registrants' data. Further, defining disclosure as a purpose is not necessary to disclose redacted data to law enforcement and other third parties with legitimate interests. To achieve consensus on this report, we have accepted this as a "purpose," but warn that it could be overruled by law.
  - Consensus guidance: NCSG would like to record its concern. It does not object to this purpose.
  
- Purpose 7: Purpose 7 is not acceptable to NCSG because it would needlessly increase the number of data registration elements in the RDDS or Whois. Some of these data elements could be very sensitive and personally identifiable. Registries can validate eligibility independently, without use of ICANN's RDDS/Whois. We were assured by registry operators that such data elements would not go into the RDDS, but since this proceeding concerns RDDS/Whois we believe it is inevitable that the data will go into it.
  - Consensus guidance: NCSG dissents on this purpose.

**Recommendation #2: Research and OCTO**

- Recommendation 2 states that Phase 2 will consider whether additional purposes should be defined to facilitate carrying out the mission of ICANN's Office of the Chief Technology Officer (OCTO). Yet OCTO has clearly stated on multiple occasions that it does not need access to personal information of domain name registrants. While we favor seeking legal guidance on ICANN's ability to use Whois data for research, Rec 2 is too ambiguous and broad and could open the door to bulk access for many third parties (and is actually intended to do so)
  - Consensus guidance: NCSG dissents on this recommendation.

**Recommendation #7: Transfer of registration data elements**

- Recommendation 7 states "the specifically-identified data elements under "[t]ransmission of registration data from Registrar to Registry" ... must be transferred from registrar to registry provided an appropriate legal basis exists and data processing agreement is in place."
  - Consensus guidance: NCSG can accept this but wishes to emphasize that there may be no valid legal justification for transferring all of these data elements from registrars to registries and inclusion of this recommendation does not imply that there is one.

#### Recommendation #8: Transfer to Escrow

- As noted in our objection to Purpose 7, additional data elements identified by registries should not be added to escrow.
  - Consensus guidance: NCSG dissents from Purpose 7

#### Recommendation #16: Geographic differentiation

- The Recommendation says that Registrars and Registry Operators are *permitted* to differentiate between registrants on a geographic basis, but are not *obligated* to do so.
- NCSG does not recall the group settling on this position. NCSG believes that ICANN's rules should be uniformly applicable, therefore registries and registrars should be obliged NOT to differentiate.

#### Recommendation #18: Reasonable access, Timeline, and Criteria

NCSG accepts the recommendation and particularly emphasizes the importance of re-naming this to "Reasonable Requests for Lawful Disclosure of Non-Public Registration Data." We have the following observations:

- Logs of requests: Logs of requests should be provided only to ICANN upon request, on a case by case basis, as stated in purpose 13. The audit function, which has been added to the recommendation 18, is not acceptable.
- Logs of the request should only contain information about "confirmation that a relay of the communication between the requestor and the Registered Name Holder has occurred, not including the origin, recipient, or content of the message."
- The distinction between urgent and non-urgent requests and obliging contracted parties to treat requests differently is not acceptable.
- We recommend deleting recommendation 18 provisions about logs and responding to urgent requests

## REGISTRY STAKEHOLDER GROUP (RySG)

### EPDP FINAL REPORT DRAFT ISSUES AND COMMENTS

The RySG remains generally supportive of the Final Report and continues to voice its support for approval of the Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process. That being said, the RySG still retains some concerns with the drafting of the report, including a lack of clarity around some of its content, and wishes to formally raise these concerns on the record. The following comments detail the areas where:

- a) The language does not reflect consensus;
- b) The language requires clarification (i.e., where the RySG supports the spirit of the recommendation, but does not believe the language correctly captures the intent of the recommendation);
- c) The RySG does not agree to the language as written; and
- d) The RySG supports the language as written.

The RySG appreciates the work done in Phase 1 and looks forward to finalizing this Report and moving to the important work of Phase 2 of the EPDP, as outlined in the Charter.

#### **High-level Comments**

- 1) Annex D of the Draft Final Report contains the Workbooks created in the analysis phase of the EPDP's work to identify and scope the data processing activities associated with each of the Purposes. While the RySG acknowledges that the Workbooks have been a useful tool to understand the background and development of each Purpose, we wish to remind the drafters of the EPDP Team's agreement that the Workbooks would remain informational and would not be part of the Recommendations. To that end, the RySG highlights several instances in the Draft Final Report where the Workbooks are incorporated by reference. These references need to be removed. Where these references serve to incorporate agreed data sets or language, that information should be reflected in the body of that Recommendation as agreed-upon, standalone text.
- 2) The RySG remains of the opinion that the matters relating to Recommendation 2 have been adequately debated and are out of scope of this EPDP, as they relate to a future potential use, and not a current use of data. We expand on this point below.
- 3) The RySG does not believe Recommendation 27 reflects EPDP consensus and requires review and revision.

#### **Comments by Recommendation**

##### **Recommendation 1**

##### **Comments by Purpose:**

###### **1) Purposes 1a & 1b**

The RySG notes no issues with Purposes 1a & 1b and supports their inclusion in the Final Report without further comment.

## **2) Purpose 2**

The RySG supports the inclusion of Purpose 2 in the Final Report.

However, the RySG notes that it expresses such support with the understanding, and continued reminder to the EPDP Team, that Purpose 2 does not qualify as a legal “Purpose” as defined in the GDPR. We also remind the EPDP Team of the advice of the European Data Protection Board<sup>82</sup>, which cautions against conflating ICANN’s purposes with those of third parties. The RySG believes this conflation continues to be at the root of the confusion regarding Purpose 2.

Along with the above statement, we make the following observations:

- The RySG accepts the current Purpose 2 is a placeholder statement that may be impacted by additional analysis conducted during Phase 2.
- The RySG concurrently accepts that, regardless of the inclusion of Purpose 2, requests for disclosure may legally be made to all contracted parties under the terms of GDPR (Art 6(1)). We restate that such disclosure requests do not require a ‘Purpose’ for disclosure.
- We also accept that, in line with the GDPR, disclosure of data may only be granted where a requester establishes a valid legal basis, demonstrates sufficient necessity and, where applicable, that the balance of the data subject’s rights has been duly considered. Such a decision to disclose MUST lie solely with the Contracted Party of whom the request has been made.

Therefore, noting the above, the spirit of Purpose 2 remains agreeable to the RySG, and as such, we shall not seek to object to its publication in the final report.

## **3) Purpose 3**

The RySG notes no issues with Purpose 3 and supports its inclusion in the Final Report without further comment.

## **4) Purpose 4**

The RySG notes no issues with Purpose 4 and supports its inclusion in the Final Report without further comment.

## **5) Purpose 5**

The RySG supports the inclusion of Purpose 5 in the Final Report.

However, we must note on the record that we believe that the inclusion of Purpose 5, in fact, creates further confusion, and we do not believe that it is a strictly necessary to include this Purpose.

Rather, Purpose 5 would, in our estimation, more appropriately be considered to be a secondary purpose, compatible with Purpose 1(b), as that Purpose relates to the processing of personal data to allow for the application of the relevant contracted party’s

---

<sup>82</sup> Letter from jelinek to marby, 5th July, 2018 - <https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf>

terms, conditions, policies, and various contractual obligations including Consensus Policies; this necessarily includes the work of contractual compliance.

Inclusion of this as a “Primary” Purpose results in increased obligations in terms of notification and Privacy Policy inclusions for both Registries and Registrars in the data processing chain. On a more immediate note, Purpose 5 has created conceptual difficulty in the completion of its associated Workbook (namely, around whether it necessitates separate collection, transfer, retention, etc.), not to mention has caused some consternation to ICANN Compliance, as it struggles to understand its place in the data processing ecosystem.

#### **6) Purpose 6:**

The RySG supports the inclusion of Purpose 6 in the Final Report.

We do note however, similarly to Purpose 5 above, it is not strictly necessary to include Purpose 6 as a standalone or “Primary” Purpose. It would more appropriately be considered as a secondary purpose compatible with Purpose 1(b) and Purpose 3, as they relate to:

- a) the application of terms, conditions, policies, and various contractual obligations including Consensus Policies; and
- b) enabling communication with the registered name holder regarding issues with the domain.

Inclusion of Purpose 6 as a “Primary” Purpose also results in increased obligations in terms of notification and Privacy Policy inclusions for both Registries and Registrars in the data processing chain. Additionally, Purpose 6 has created conceptual difficulty in the completion of its associated Workbook (namely, around whether it necessitates separate collection, transfer, retention, etc.)

As with Purpose 5, the RySG is not opposed to the attempts at clarity provided by the inclusion of Purpose 6; however, we must note on the record that we do not believe that it is a strictly necessary inclusion.

#### **7) Purpose 7:**

The RySG notes no issues with Purpose 7 and supports its inclusion in the Final Report without further comment.

### **Recommendation 2**

The RySG **does not agree to** Recommendation 2 and we continue to have concerns regarding its inclusion, both in content and in the procedure that led to its inclusion (pg. 37 - 39). The RySG believes that Recommendation #2 should be removed.

The RySG does not believe that Recommendation #2 reflects consensus among the EPDP Team. The inclusion of a Recommendation specifically to address an ICANN action, in the form of “research” by ICANN’s Office of the Chief Technology Officer (OCTO), was introduced very late in the drafting period and although discussed, was in no way agreed to by the full Team.

OCTO is a wholly inappropriate inclusion in the Draft Final Report for several reasons:

- ICANN itself stated that at present, OCTO does not require, or use, personal data in its research activities;

- A recommendation from the EPDP Team to consider or identify a Purpose for potential future uses of personal data by OCTO, directly contradicts GDPR requirements that Purposes not be speculative;
- Further, the inclusion of a Purpose for OCTO is outside of the scope of the EPDP’s work. The EPDP is chartered to accept, reject, or refine the Temporary Specification. The Temporary Specification provides baseline policy addressing the requirements outlined in Registry Agreements and Registrar Accreditation Agreements, with regard to the use of personal data. It’s been made clear that the use of any personal data by a Contracted Party that is not covered by the relevant RA or RAAs is the responsibility of the contracted party. For example, if a contracted party wanted to provide a service to customers that was outside the requirements of the base contract, that contracted party must create a justification for the use of that personal data in addition to the primary Purposes defined in the Draft Final Report. ICANN’s use of data via OCTO is exactly the same. If ICANN wishes to incorporate the use of personal data into its research efforts, it must develop a GDPR-compliant justification for that use;
- Finally, the background discussion in the Draft Final Report notes that the group did not reach consensus on including Recommendation #2 and that this issue would require further work. It is therefore not appropriate to include Recommendation #2 as a Recommendation. We believe the inclusion of the background text and minority statement addressing OCTO is unnecessary (p. 37 of the redline). We cannot see how this inclusion impacts the actual Purpose or Recommendation, and if anything, it only lends itself to further confusion and should be removed.

### **Recommendation 3**

The RySG has no issue as with the inclusion of this language in the Final Report, but urges the EPDP Team to consider placing the statement under an appropriate heading, so as to avoid confusion at implementation.

The RySG does not believe that Recommendation #3 is, in reality, a “recommendation.” The language used identifies this more as a statement of intention, without serving a particular substantive purpose for implementation.

### **Recommendation 4**

The RySG supports the inclusion of Recommendation #4 in the Final Report in light of the analysis and recommendation provided to the EPDP by outside counsel, Bird & Bird:

*“In sum, because compliance with the Accuracy Principle is based on a reasonableness standard, ICANN and the relevant parties will be better placed to evaluate whether these procedures are sufficient. From our vantage point, as the procedures do require affirmative steps that will help confirm accuracy, unless there is reason to believe these are insufficient, we see no clear requirement to review them.”*

### **Recommendation 5**

The RySG notes that the wording of this Recommendation is unclear. The text of the Recommendation notes that the provision of technical contact name, email, and phone number should be optional for the Registered Name holder to provide. The supporting text in the Draft Final Report then notes that there was not consensus on making it mandatory for Registrars to provide the option to the Registered Name Holder to provide the technical contact data. The Recommendation should include only the agreed text. Discussion of alternate options is not only



confusing but unnecessary to a Final Report intended to provide consensus policy Recommendations.

Further, the citation of the Workbooks in Recommendation #5 should be removed. The agreed aggregate data set is presented in the text of the Recommendation as that was the agreed-upon text. **The Workbooks are informational and should not be incorporated by reference.**

In light of the inaccuracies in the draft language and some lack of clarity noted above with the report we **suggest the following modifications** to the Recommendation and accompanying chart for clarity:

*The EPDP Team recommends that the data elements, representing the Aggregate Minimum Data Set, listed below are required to be collected by registrars, noting that the collection of some data elements is optional.*

<b>Data Elements Collected and Generated by Registrar</b>	
Domain Name	REQUIRED to be collected from RNH
Registrar Whois Server	REQUIRED to be generated by Registrar
Registrar URL	REQUIRED to be generated by Registrar
Updated Date	REQUIRED to be generated by Registrar
Registrar Registration Expiration Date	REQUIRED to be generated by Registrar
Registrar	REQUIRED to be generated by Registrar
Registrar IANA ID	REQUIRED to be generated by Registrar
Registrar Abuse Contact Email	REQUIRED to be generated by Registrar
Registrar Abuse Contact Phone	REQUIRED to be generated by Registrar
Reseller	REQUIRED to be generated by Registrar IF applicable
Domain Status(es)	REQUIRED to be generated by Registrar
Registrant Fields	
· Name	REQUIRED to be collected from RNH

· Organization	OPTIONAL for RNH to provide and optional for Registrar to collect (as per recommendation 12)
· Street	REQUIRED to be collected from RNH
· City	REQUIRED to be collected from RNH
· State/province	REQUIRED to be collected from RNH
· Postal code	REQUIRED to be collected from RNH
· Country	REQUIRED to be collected from RNH
· Phone	REQUIRED to be collected from RNH
· Phone ext	OPTIONAL for RNH to provide, REQUIRED to be collected by Registrar IF provided
· Fax	OPTIONAL for RNH to provide, REQUIRED to be collected by Registrar IF provided
· Fax ext	OPTIONAL for RNH to provide, REQUIRED to be collected by Registrar IF provided
· Email	REQUIRED to be collected from RNH
Tech Fields	
· Name	OPTIONAL for Registrar to support AND OPTIONAL for RNH to provide <sup>83</sup>
· Phone	OPTIONAL for Registrar to support AND OPTIONAL for RNH to provide
· Email	OPTIONAL for Registrar to support AND OPTIONAL for RNH to provide
Name Server	OPTIONAL for RNH to provide, REQUIRED to be collected by Registrar IF provided

<sup>83</sup> As per <https://mm.icann.org/pipermail/gnso-epdp-team/2019-February/001662.html>

DNSSEC	OPTIONAL for RNH to provide, REQUIRED to be collected by Registrar if provided
Name Server IP Address	OPTIONAL for RNH to provide, REQUIRED to be collected by Registrar if provided
Additional data elements as identified by Registry Operator in its registration policy	REQUIRED to be collected by Registrar IF applicable

*For the purpose of the Technical contact, which is optional for the Registered Name Holder to provide (and if the Registrar provides this option), Registrars are to advise the Registered Name Holder at the time of registration that the Registered Name Holder is free to (1) designate the same person as the registrant (or its representative) as the technical contact; or (2) provide contact information which does not directly identify the technical contact person concerned.*

**Recommendation 6**

The RySG supports the inclusion of Recommendation #6 in the Final Report without further comment.

**Recommendation 7**

The RySG notes that there were some inaccuracies and missing fields in the table and therefore this Recommendation does not reflect the consensus of the EPDP Team. The inclusion of the language “*Provided an appropriate legal basis exists*” in this recommendation is inconsistent with Purpose 1a and 1b, which in fact provide the legal basis for processing the aggregate minimum data set. This statement could be interpreted as meaning that each Contracted Party is required to then develop a new/separate legal basis apart from what is provided by Purpose 1a and 1b, which is not the case.

Further, the citation of the Workbooks in Recommendation #7 should be removed. The agreed aggregate data set is presented in the text of the Recommendation as that was the agreed-upon text. **The Workbooks are informational and should not be incorporated by reference.**

In light of the inaccuracies in the draft language and some lack of clarity noted above with the report we **suggest the following modifications** to the Recommendation and accompanying chart for clarity:

*“The EPDP Team recommends that registrars are required to transfer the data elements listed below to the registry.*

<b>Data Elements Transferred from Registrar to Registry</b>	
Domain Name	REQUIRED to be transferred from Registrar to Registry

Registrar Whois Server	REQUIRED to be transferred from Registrar to Registry
Registrar URL	REQUIRED to be transferred from Registrar to Registry
Updated Date	REQUIRED to be transferred from Registrar to Registry
Registrar Registration Expiration Date	OPTIONAL to be transferred based on Registry policies
Registrar	REQUIRED to be transferred from Registrar to Registry
Registrar IANA ID	REQUIRED to be transferred from Registrar to Registry
Registrar Abuse Contact Email	REQUIRED to be transferred from Registrar to Registry
Registrar Abuse Contact Phone	REQUIRED to be transferred from Registrar to Registry
Reseller	OPTIONAL to be transferred based on Registry policies
Domain Status(es)	REQUIRED to be transferred from Registrar to Registry
Registrant Fields	
· Name	REQUIRED to be transferred from Registrar to Registry IF Registry terms/conditions/policies require this data element
· Organization	OPTIONAL for RNH to provide, REQUIRED to be transferred from Registrar to Registry IF provided and IF Registry terms/conditions/policies require this data element

· Street	REQUIRED to be transferred from Registrar to Registry IF Registry terms/conditions/policies require this data element
· City	REQUIRED to be transferred from Registrar to Registry IF Registry terms/conditions/policies require this data element
· State/province	REQUIRED to be transferred from Registrar to Registry IF Registry terms/conditions/policies require this data element
· Postal code	REQUIRED to be transferred from Registrar to Registry IF Registry terms/conditions/policies require this data element
· Country	REQUIRED to be transferred from Registrar to Registry IF Registry terms/conditions/policies require this data element
· Phone	REQUIRED to be transferred from Registrar to Registry IF Registry terms/conditions/policies require this data element
· Phone ext	OPTIONAL for RNH to provide, REQUIRED to be transferred from Registrar to Registry IF provided and IF Registry terms/conditions/policies require this data element
· Fax	OPTIONAL for RNH to provide, REQUIRED to be transferred from Registrar to Registry IF provided and IF Registry terms/conditions/policies require this data element
· Fax ext	OPTIONAL for RNH to provide, REQUIRED to be transferred from Registrar to Registry IF provided and IF Registry terms/conditions/policies require this data element
· Email	Required to be transferred from Registrar to Registry IF Registry terms/conditions/policies require this data element
Tech Fields	

· Name	OPTIONAL for RNH to provide, REQUIRED to be transferred from Registrar to Registry IF provided and IF Registry terms/conditions/policies require this data element
· Phone	OPTIONAL for RNH to provide, REQUIRED to be transferred from Registrar to Registry IF provided and IF Registry terms/conditions/policies require this data element
· Email	OPTIONAL for RNH to provide, REQUIRED to be transferred from Registrar to Registry IF provided and IF Registry terms/conditions/policies require this data element
Name Server	OPTIONAL for RNH to provide, REQUIRED to be transferred from Registrar to Registry IF provided
DNSSEC	OPTIONAL for RNH to provide, REQUIRED to be transferred from Registrar to Registry IF provided
Name Server IP Address	OPTIONAL for RNH to provide, REQUIRED to be transferred from Registrar to Registry IF provided
· Additional data elements as identified by Registry Operator in its registration policy, such as (i) status as Registry Operator Affiliate or Trademark Licensee [.MICROSOFT]; (ii) membership in community [.ECO]; (iii) licensing, registration or appropriate permits (.PHARMACY, .LAW] place of domicile [.NYC]; (iv) business entity or activity [.BANK, .BOT]	REQUIRED to be transferred from Registrar to Registry IF Registry terms/conditions/policies require these data elements

### Recommendation 8

The RySG notes a number of concerns with Recommendation #8, as follows:

**Bullet One:**

The RySG notes that the language has changed from “develop” to “enter into.” This change was not agreed within the EPDP Team. The text should maintain the agreed-upon EPDP position of “enter into.” The EPDP Team’s direction to enter into required Data Processing Agreements with the escrow providers, and not just to develop them, is absolutely necessary for compliance with the requirements of the GDPR.

**Bullet Two:**

The citation of the Workbooks in Recommendation #8 should be removed. The agreed aggregate data set is presented in the text of the Recommendation as that was the agreed-upon text. **The Workbooks are informational and should not be incorporated by reference.**

Further, Bullet Two is overly complicated and should merely reference the Aggregate Minimum Data Set (i.e., that which the EPDP Team has agreed is necessary for the purpose of escrow / recovery of the Zone in the event of a triggering event). The current phrasing is incredibly complicated and will require extra focus at implementation, especially vis-a-vis ICANN's role as Controller.

**Bullet Three:**

Given the work of the EPDP Team, the RySG would note that escrow deposits should be limited to the Minimum Data Set (as defined by the EPDP Team). This Minimum Data Set is comprised of those data elements that are considered to be necessary for the registration of a Domain and as such for the reconstitution of the zone should an Escrow triggering event occur.

We note that any further changes that, may be considered necessary, should be deferred and tabled for review, and may be achieved, either by the contracted parties as per the envisaged agreements of Recommendation 19, or at the direction of the GNSO, as per Recommendation 27.

**Recommendation 9**

**The RySG does not object to the intent of Recommendation 9.**

**We do however note that the recommendation does not reflect discussions surrounding the grounding reason for this recommendation. This was not meant to address Contractual Compliance scope / actions, it was meant to address conformity of existing contractual agreements with the recommendations contained within the intended consensus policy.**

**So we urge the ePDP team to ensure that our recommendation is properly framed to achieve that which was scoped.**

- The RySG believes that this Recommendation is unclear. We are unsure how this relates to the specific question as posed in Charter question **(e1)**.
- The RySG clarifies that the current language within the Contracts already provides the appropriate scope for contractual compliance requests and subsequent transfer (E.g. Art 2.11 new GTLD Base Registry Agreement) .
- The only change required and thus the original concept and necessity grounding Recommendation 9 should be limited only to the ensuring that there are no unexpected incompatibilities with this intended consensus policy, that allow ICANN compliance to continue to perform their functions. The RySG does remind the ePDP that such matters will be reviewed and discerned as part of the negotiation and execution of the necessary legally binding data protection agreements between ICANN and CPs, which are already envisaged in Recommendation #19.

- Part 2 of the recommendation as written and the subsequent table creates confusion and is unnecessary considering the point raised above. The RySG therefore recommends the removal of Part 2.

**The RySG will note however, by way of notice to ICANN Compliance,** the Compliance Summary of Contractual Compliance Team Data Processing Activities document, as is currently referenced, does tend to be remain unclear as to the data elements required, and for what specific reasons. We would be supportive of the recommendation that the Compliance dept. create a more in-depth, and point-in-time assessment / data map? This is to ensure clarity for the CPs and Compliance and to prevent any Data Privacy barriers in their carrying out of their function.

Considering that there remain a lack of agreement regarding Tech Contact fields, the RySG notes that their continued inclusion in the tables, without clear qualifying language, is confusing and will likely cause issues at implementation.

#### **Recommendation 10**

The RySG notes no major issues with Recommendation #10 and supports its inclusion in the Final Report without further comment.

#### **Recommendation 11**

**The RySG supports redaction of the 'CITY' field.**

This statement is predicated on the Legal Memo from Bird & Bird<sup>84</sup>. Although we appreciate the ultimate conclusion of the memorandum was to suggest further review, specific to the context of the DNS was necessary, noting our considerations should be based on civil standards of liability (balance of probabilities), the memorandum does conclude that an enhanced risk to the privacy of the registered name holder does likely exist should the 'City' field be published. The lack of conclusion was in relation to the severity of the increased risk and thus is not determinative as to the presence of an increased risk or not.

Fundamentally the EPDP team should NOT create policy where such a policy knowingly increases the legal risk and financial to the Contracted Parties (and thus increasing the SSR risk generally) therefore, the 'CITY' field must be redacted.

The RySG, noting the above does believe that Recommendation 10 and 11 should be merged, with relevant footnotes as necessary.

#### **Recommendation 12**

The RySG notes minor issues with Recommendation #12 and supports its inclusion in the Final Report.

In addition, we suggest the the implementation notes be updated to clarify that this is a Registrar obligation. For a Registry the obligation to publish is optional. Further, the final paragraph in the implementation advice does not distinguish Registry and Registrar and should make clear it is optional for Registry.

---

<sup>84</sup> <https://community.icann.org/download/attachments/102138857/ICANN%20-%20Memo%20on%20publication%20of%20the%20City%20field%20%28130219%29.docx?version=1&modificationDate=1550152144000&api=v2>



### **Recommendation 13**

The RySG notes no major issues with Recommendation #13 and supports its inclusion in the Final Report without further comment.

### **Recommendation 14**

The Registries have no issue with Recommendation #14, **so long as it is clear that the permissive language that applies to Registrars, applies equally and independently to Registry Operators.**

Meaning, Registries may choose to not display or return privacy/proxy data as transferred to them from Registrars in response to an RDDS query.

### **Recommendation 15**

The RySG notes no major issues with Recommendation #15 and supports its inclusion in the Final Report without further comment.

### **Recommendation 16**

The RySG notes no major issues with Recommendation #16 and supports its inclusion in the Final Report without further comment.

### **Recommendation 17**

Although the RySG supports the language in Recommendation #17, we do submit that it is confusing, and in the interests of clarity, simplicity and consistency, it should simply mirror the language of Recommendation #16. As such, we **suggest the following modifications:**

*The EPDP Team recommends that Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so.*

### **Recommendation 18**

Although the RySG supports Recommendation #18, we do not believe that the task of addressing the timeline to respond to disclosure requests should be deferred to the implementation phase. This does not reflect the consensus of the EPDP Team. We therefore suggest the removal of that suggestion from Recommendation #18.

The timeframe for responding to requests for disclosure should not be set during the implementation phase because it is a legal obligation of the Contracted Parties. ICANN should not be put in a position to enforce any such time limits, which are in effect, solely related to the disclosure request. A non-data subject disclosure request can vary greatly in complexity and require several procedural steps and substantive review and analysis under GDPR (i.e., legal advices, circumstances, balancing tests, etc.).

The RySG recalls that this question was to be flagged for further discussion of this matter to Phase 2, and does not support deferring this task to the implementation phase.

### **Recommendation 19**

The RySG notes no major issues with Recommendation #19 and supports its inclusion in the Final Report without further comment.

### **Recommendation 20**

The RySG notes no major issues with Recommendation #20 and supports its inclusion in the Final Report.

The RySG does, however, note that the roles and responsibilities outlined in the body of this Recommendation are not final and are subject to revision following the analysis required to establish the appropriate agreements per Recommendation #19.

#### **Recommendation 21**

The RySG does not object to Recommendation #21 and but notes some issues.

First, Recommendation #21 lacks a requirement to establish the appropriate agreements (i.e. legally binding data protection agreement) between URS provider and ICANN Org. In addition to the issues noted above at Recommendation #1 / Purpose 6, the RySG notes that this Recommendation really establishes a secondary purpose for those Registry Operators that participate in the URS in line with their agreements. This does not create a mandatory transfer of data Registries. It is understood that this Recommendation does not create a requirement by itself to transfer data from Registrar to Registry. If the data exists at the Registry, it would be provided per section 1, if it does not, the URS provider would go to the Registrar per section 2.

As explained below, Recommendation #21 should be moved in the order of recommendation to appear after the current Recommendation #23, as this recommendation is dependent on Recommendation #23.

#### **Recommendation 22**

The RySG notes no major issues with Recommendation #22 and supports its inclusion in the Final Report without further comment.

#### **Recommendation 23**

The RySG notes no major issues with Recommendation #23 and supports its inclusion in the Final Report, but stresses that Recommendation #23 should rank in priority to Recommendation #21. The order of the Recommendations should be changed to make #21 dependent upon current #23.

#### **Recommendation 24**

The RySG notes no major issues with Recommendation #24 and supports its inclusion in the Final Report without further comment.

#### **Recommendation 25**

The RySG note that, as written, Recommendation #25 seems completely redundant to Recommendation #24.

#### **Recommendation 26**

The RySG notes no major issues with Recommendation #26 and supports its inclusion in the Final Report without further comment.

#### **Recommendation 27**

The RySG does not believe Recommendation #27 reflects consensus of the EPDP Team. This recommendation should be for the GNSO Council to undertake a review of these policies. As worded it directs ICANN to make these changes which is inappropriate and out of ICANN's mandate.

**For clarification, we suggest the following modifications:**

*“The EPDP Team recommends that the GNSO undertake a review of the below policies, and makes updates to the following existing policies / procedures, and any others that may have been omitted, to ensure consistency with these policy recommendations as, for example, a number of these refer to administrative and/or technical contact which will no longer be required data elements.”....*

**Recommendation 28:**

The RySG notes no major issues with Recommendation #28 and supports its inclusion in the Final Report; however, the RySG notes that it is important that the GNSO Council determine what processes are appropriate within its scope and mandate.

**Recommendation 29:**

The RySG notes no major issues with Recommendation #29 and supports its inclusion in the Final Report.

The RySG also notes that the “Implementation Guidance” text is not part of the Recommendation as agreed. Its inclusion provides ambiguity and lacks clarity. The RySG recommends it be removed.

## **INTERNET SERVICE PROVIDERS AND CONNECTIVITY PROVIDERS CONSTITUENCY (ISPCP)**

### **Consensus Call #1**

On behalf of the ISPCP I would like to confirm that we support the consensus positions in the first bucket of the consensus call. This support is conditional to no changes being made to the language, in which case we would need to reconsider.

### **Consensus Call #2**

I am happy to confirm the ISPCP's support for the second batch of the consensus call. As mentioned for the first batch, this is conditional to the wording remaining unaltered. In case there are changes, Fiona and I would need to take the new language back to the ISPCP.

I also add - again - a caveat for the last recommendation on "consent to publish additional information", which I shared on the list earlier:

Let me just to on the record (again) that - whilst I do support that an opportunity for consent must be given at some point - we need to make sure this is done in a compliant fashion. As stated previously, I do not think we have the technical and organizational means in place so that the controller(s) can demonstrate that the consent (and the contents thereof) have been given, see Art. 7 | GDPR. This is not impossible to do, but I think the gTLD ecosystem is not yet ready for handling consent and make it travel with the registration data to all players. I think some in our team think that we are operationally and legally ready to do that in a compliant fashion, in which case we should probably link to related documentation or write a few lines on how this can be done. In sum, I do not think it is just a matter of commercial factors.

### **Consensus Call #3 / draft final report**

Please find below the statement on the draft final report from the ISPCP in addition to the input already provided on the first and second batch of the consensus call.

Recommendation 5 - optional Tech-C:

Whilst not opposing recommendation 5, we would like our concern to be noted that our goal should be to have one system that works globally for gTLDs to avoid fragmentation. Therefore, we recommend to amend this recommendation so that

- the registrar **MUST** offer the option to provide data for the tech-c and
- the provision of data for a tech-c is optional

Users should get the same experience and options regardless of what registrar they choose to work with.

Recommendations 10 / 16 and 17:

We think that more work needs to be done in order to provide for a system that is globally applicable to avoid fragmentation in terms of RNH rights and user experience.

Recommendation 18:

We suggest to include the timelines / procedure as laid down in Art. 15 III GDPR so that there is transparency regarding response times:

The clause reads:

1The controller shall provide information on action taken on a request under [Articles 15 \[gdpr-info.eu\]](#) to [22 \[gdpr-info.eu\]](#)to the data subject without undue delay and in any event within one month of receipt of the request. 2That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. 3The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. 4Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Additionally, we suggest to include a requirement for contracted parties to publish data on how many disclosure requests they get. That helps the community understand whether response times are corresponding with work load.

Recommendation 19:

The EPDP Team chose to dilute the language of this recommendation not to make reference to a specific legal vehicle. As a matter of compromise, reference to the analysis in the report was agreed to be made to inform the implementation and decision on what legal vehicle to use. The report now includes amended language as prepared by ICANN representatives. These changes were not discussed by the EDPDP team and we ask to reinstate the original language of the report to inform the decision-making during the implementation of the recommendation.

Recommendation 27:

We support the recommendation as long as it is ensured that

- the community is part of the implementation team
- the GNSO Council as the policy manager has the last saying on any policy amendments according to its PDP rules

## Governmental Advisory Committee<sup>85</sup> Input on the Draft Final Report of the Expedited Policy Development Process (EPDP) on gTLD Registration Data

---

### 1. General Concern that Draft Final Report does not Sufficiently Recognize the Benefits of the Whois database

The GAC commends the considerable efforts put forth by the EPDP members, observers, leadership and support staff to produce this Draft Final report. The complex subject matter and swift timeframes challenged all those involved to determine the best path forward to comply with the EU's General Data Protection Regulation (GDPR) and take into account the sometimes competing interests of the public, including intellectual property protection, cybersecurity, and those public authorities charged with protecting against deceptive or malicious conduct involving the domain name system (DNS). Nevertheless, the draft final report does not sufficiently recognize or incorporate recommendations in the public interest.

As set forth by the GAC in its 2007 Principles regarding gTLD WHOIS Services, as the Internet evolved, the WHOIS became a tool relied upon by various stakeholders for a number of legitimate activities, including *inter alia*, 1) supporting the security and stability of the Internet; 2) assisting law enforcement authorities in their national and international investigations; 3) assisting businesses, organizations and users in combatting fraud and 4) contributing to user confidence in the Internet.<sup>86</sup> The GAC also highlighted the importance of "sufficient and accurate data" about domain name registrations and registrants, subject to privacy safeguards. The GAC also recognized the legitimate concerns about misuse of WHOIS data and conflicts with applicable privacy and data protection laws. Hence the GAC concluded that operation of gTLD WHOIS services should take into account and respect these different interests. The 2007 GAC Principles therefore urge not only compliance with applicable laws but also WHOIS services that support "the stability, reliability, security, and global interoperability of the Internet from both a technical and public trust perspective." The current draft Final Report lacks this recognition and hence risks creating a new registration directory service that does not collect, publish, nor allow for lawful disclosure of sufficient information and provide adequate procedures necessary for promoting 1) the security and stability of the DNS, 2) user confidence in the Internet, and 3) quick and efficient mitigation of malicious conduct. The GAC concerns regarding specific recommendations, the importance of starting and concluding Phase 2 discussions as soon as possible, and suggestions to improve procedures for the next phase of the EPDP are set forth below.

---

<sup>85</sup> Submitted by GAC members of the EPDP, based on previous input of the GAC, which could not be consulted in the time allowed for submission.

<sup>86</sup> These interests are also reflected in ICANN's current Bylaws which commit to "[p]reserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet." The Bylaws also mandate specified reviews to assess the effectiveness of *inter alia*, "the security efforts to deal with actual and potential challenges and threats to the security and stability of the DNS"; the effectiveness of the then current gTLD registry directory service and whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust and safeguarding registrant data" and address issues of "consumer protection..., malicious abuse issues ..., and rights protection." See ICANN Bylaws Section 1.2 (a) Commitments and Section 4.6 (c)(d) and (e) Required Reviews.

## Input on Specific Recommendations

**Recommendation 1, paragraph 2** in the EPDP Initial Report, which states:

*2. Contributing to the maintenance of the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission through enabling responses to lawful data disclosure requests.*

The GAC believes that this purpose would be strengthened by referencing ICANN's *Commitments* and *Core Values* which are also integral to ICANN's Bylaws.

**Recommendation 2** which states:

*The EPDP Team commits to considering in Phase 2 of its work whether additional purposes should be considered to facilitate ICANN's Office of the Chief Technology Officer (OCTO) to carry out its mission (see <https://www.icann.org/octo>). This consideration should be informed by legal guidance on if/how provisions in the GDPR concerning research apply to ICANN Org and the expression for the need of such pseudonymized data by ICANN*

The GAC supports the intent of this Recommendation and urges its continued consideration in Phase 2. The GAC believes that the final version of this purpose should include ICANN's purpose to process information associated with its registration data Accuracy Reporting System.

**Recommendation 4** which states:

*The EPDP Team recommends that requirements related to the accuracy of registration data under the current ICANN contracts and consensus policies shall not be affected by this policy.*

Consistent with Article 5.1.d of the GDPR, every reasonable step must be taken to ensure the accuracy of personal data, in this case, including data provided by registrants. Article 5 of the GDPR also extends beyond the right of a data subject, "having regard to the purposes for which [the data] are processed". Current ICANN contracts (in particular in the 2013 [Registrar Accreditation Agreement](#), Sections 3.2.2, 3.7.7.2 and 3.7.8) are consistent with this aspect of the GDPR and obligate registrars to take steps to respond to and correct reports of inaccurate WHOIS data.

Therefore, the GAC believes that Recommendation 4 should more explicitly recognize the importance of ensuring information accuracy consistent with GDPR article 5.1(d). This recognition would underscore the data subjects (registrants) rights to the accuracy of their

data while also addressing concerns of those who rely on WHOIS information for legitimate purposes (such as maintaining the security and stability of the DNS).

### **Recommendations 5 and 7 (data elements required to be collected)**

The GAC remains concerned that the “technical contact” field is currently considered optional to be collected by the registrar. A primary purpose for WHOIS is to provide contact points for network operators, computer incident response teams, and others who need to contact those responsible for a domain and its associated web sites in the event of a problem. Often a registrant has specific/distinct contacts responsible for acquiring/maintaining registration and other contacts responsible for ensuring the security of the domain. Being able to reach the informed technical contact responsible for security issues directly and quickly to respond to issues such as the domain being under control of a botnet, may be a matter of urgency. Making collection of this information optional for registrars eliminates this important safety net. Moreover, the GAC does not think it is appropriate for registrars to unilaterally decide for registrants that they do not need to identify a technical contact. Registrants may see value in providing a technical contact to resolve issues with their domain in a timely and most direct manner, among other reasons. The provision (and therefore collection) of a technical contact should remain an option for the registrant.

Further, the GAC is concerned that language in the recommendation leaves it completely optional for the registrant to decide whether or not to provide information in the “organization” field. The basis of this concern is that those registrants who are in fact organizations may not enter their organization’s name into this field if they are not required that they do so. The GAC is of the view that it is vital for members of the public to know if a domain is registered by an organization and if so, the name of that organization so that they may conduct due diligence as they decide what websites to trust with their communications and transactions or what entity to contact to seek resolution of complaints. Hence, the GAC is of the strong view that the organizational field should be required to be provided by a registrant that is in fact an organization and would recommend that this matter be considered during Phase II and/or implementation.

### **Recommendations 10 and 11 (redaction of data elements).**

#### *Organization*

The Organization field should not be redacted as this is clearly a field whereby any personal data contained within the entry would fall under that of a legal person as defined within GDPR Recital 14A. If registrants incorrectly provide personal information, this could be rectified by a number of means, including first, by providing registrants with clear guidance on what this field is for and the implications of entering data into the field. Second, by



providing the registrant with the ability to rectify this field if it is not correctly filled out and by confirmation at renewal point.

It should be noted that in GAC's previous input, there are many European countries who publicly publish business details (including organization name) and even a network of these national registers (European Business Registrar). Also the European Directive 2000/31/EC states "Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information:

- (a) the name of the service provider;
- (b) the geographic address at which the service provider is established;
- (c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;"

#### *City*

The City field should not be redacted as an individual is unlikely to be identified either directly or indirectly from this identifier or with all the identifiers otherwise non-redacted.

#### **Recommendation 12 (Publication of Organization field).**

The GAC is pleased that the EPDP was able to reach agreement in recommending that the Organization field be published under the conditions outlined in the report. That being said, the GAC is of the view that there should be more accountability to be applied to the Contracted Parties in implementing this. Specifically, the time frame for registrars to develop procedures to deal with existing registrations. The GAC would like this time frame to be time bound and correspond with the first renewal period after implementation of the new policy.

#### **Recommendation 13 (email address and web form to facilitate email communication).**

- 1) The EPDP Team recommends that the Registrar MUST provide an email address or a web form to facilitate email communication with the relevant contact, but MUST NOT identify the contact email address or the contact itself, unless as per Recommendation X, the Registered Name Holder has provided consent for the publication of its email address.
- 2) The EPDP Team recommends Registrars MUST maintain Log Files, which shall not contain any Personal Information, and which shall contain confirmation that a relay of the communication between the requestor and the Registered Name Holder has occurred, not including the origin, recipient, or content of the message. Such records will be available to ICANN for compliance purposes, upon

request. Nothing in this recommendation should be construed to prevent the registrar from taking reasonable and appropriate action to prevent the abuse of the registrar contact process.

The GAC is concerned that this recommendation does not provide sufficient accountability with regard to instances if emails bounce back or are ignored (for example: providing notification to the sender that the email has been received and read).

### **Recommendation 17 (Differentiation of Legal and Natural Persons)**

- 1) The EPDP Team recommends that the policy recommendations in this Final Report apply to all gTLD registrations, without requiring Registrars or registries to differentiate between registrations of legal and natural persons, although registrars and registries are permitted to make this distinction.
- 2) *The EPDP Team recommends that as soon as possible ICANN Org undertakes a study, for which the terms of reference are developed in consultation with the community, that considers:*
  - *The feasibility and costs including both implementation and potential liability costs of differentiating between legal and natural persons;*
  - *Examples of industries or other organizations that have successfully differentiated between legal and natural persons;*
  - *Privacy risks to registered name holders of differentiating between legal and natural persons; and*
  - *Other potential risks (if any) to registrars and registries of not differentiating.*
- 3) *The EPDP Team will discuss the Legal vs. Natural issue in Phase 2. Depending on the timing of the research, its discussions may inform the scope of research and/or use its findings.*

The GAC would recommend that the temporary specification require contracted parties to treat legal and natural persons differently because, the GDPR “does not cover processing of personal data which concerns legal persons.” (Recital 14). Hence, as the GAC recognized in its San Juan Communique advice, the personal information of legal persons should be part of the publicly available WHOIS data. Hence, the GAC support this recommendation in that it provides for further study of this topic in Phase II. However, the GAC notes that the Recommendation discusses only the risks and costs of this differentiation but does not mention the benefits of this distinction. Hence the GAC recommends that the study include an examination of the benefits of providing this information to the public.

## **Recommendation 18 (reasonable requests for Lawful Disclosure of Nonpublic Data)**

The GAC believes the recommendation provides much greater clarity around the matter of requesting disclosure of redacted information, for both the requester of the information and the contracted parties. The GAC looks forward to progressing this discussion to a unified access model in Phase II.

### **European Data Protection Board Guidance**

The GAC recognizes the considerable effort and time taken by the EPDP in developing the Phase I Final Report. The GAC asks that a legal review be undertaken to ensure that the purposes referenced in the Phase 1 Final Report take into account previous guidance provided by the European Data Protection Board (EDPB) and Article 29 Working Group (WP29). Specifically, that ICANN:

- explicitly define legitimate purposes in a way which comports with the requirements of GDPR<sup>87</sup>
- take care in defining purposes in a manner which corresponds to its own organizational mission and mandate / do not conflate purpose<sup>88</sup>
- that purposes be detailed enough<sup>89</sup>

### **Importance of Quickly Starting Phase 2 Deliberations**

The GAC urges the prompt start to Phase 2 deliberations which contains a number of crucial issues including the procedures, criteria, and parameters of how to access non-public registration directory information.

### **Improvements for Future Work**

---

<sup>87</sup> In its [11 April 2018 letter](#), WP29 stressed: “the importance of explicitly defining legitimate purposes in a way which comports with the requirements of the GDPR. It therefore urges ICANN to revisit its current definition of “purposes” in light of these requirements. Use of the word “include” suggests that not all purposes are made explicit, which would also be incompatible with article 5(1)b GDPR.”

<sup>88</sup> In its [11 April 2018 letter](#), WP29 stated: “ICANN should take care in defining purposes in a manner which corresponds to its own organisational mission and mandate, which is to coordinate the stable operation of the Internet’s unique identifier systems. Purposes pursued by other interested third parties should not determine the purposes pursued by ICANN. The WP29 cautions ICANN not to conflate its own purposes with the interests of third parties, nor with the lawful grounds of processing which may be applicable in a particular case.” In its [5 July 2018 letter](#), the EDPB stated: “the EDPB considers it essential that a clear distinction be maintained between the different processing activities that take place in the context of WHOIS and the respective purposes pursued by the various stakeholders involved.”

<sup>89</sup> In its [11 April 2018 letter](#), WP29 clarified: “that purposes specified by the controller must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied.”

While the GAC appreciates the work of the first ever EPDP, nevertheless certain changes would improve the efficiency of future work. First, there should be sufficient time to review and consider proposed text and edits prior to consensus calls. Second, there should be deadlines for changes to avoid “re-litigating” previously agreed upon positions. Third, when necessary, interventions should be limited to an agreed upon amount of time. Finally, the GNSO is urged to permit EPDP working group observers to have access to the fully functioning adobe connect room so that they can scroll through comments in the chat and confer with their counterparts in real-time. The current separate room does not permit any scrolling to review past remarks or permit private chats.