Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team

The following responses were submitted via web form and email (policy-staff@icann.org) to ICANN in response to the Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team comment period ending December 21, 2018. In some cases, the original questions have been reformatted for ease of reading.

1. Email address *

lschulman@inta.org

2. Please provide your name: *

Lori Schulman
Senior Director, Internet Policy

3. Please provide your affiliation *

International Trademark Association (INTA)

4. Are you providing input on behalf of another group (e.g., organization, company, government)?

Yes

5. If yes, please explain:

The International Trademark Association (INTA) is a global association of brand owners, legal professionals, academics, civil society and trademark and domain industry service providers and others dedicated to defending trademarks and related intellectual property (IP) rights to foster consumer protection, economic growth and innovation. With more than 7,200 members in over 192 countries, one of INTA’s goals is the promotion and protection of trademarks as a primary means for consumers to make informed choices regarding the products and services they purchase. INTA members frequently rely on and use ownership information in the global WHOIS database to locate and contact the registrant behind web sites that infringe the
intellectual property rights of others, steal personal information, sell counterfeit goods, distribute malicious software and perpetuate fraud.

During the last two decades, INTA has been the leading voice of trademark owners within the Internet community, serving as a founding member of the Intellectual Property Constituency (IPC). INTA’s Internet Committee is a group of over 175 trademark owners and professionals from around the world charged with evaluating treaties, laws, regulations and procedures relating to domain name assignment, use of trademarks on the Internet, and unfair competition on the Internet, whose mission is to advance the balanced protection of trademarks on the Internet.

Section 3, Part 1: Purposes for Processing Registration Data

The EPDP team was tasked with determining whether the ICANN and Contracted Party Purposes for Processing Registration Data listed in the Temporary Specification are appropriate and if additional “Purposes” are required. The Team developed DNS requirements, the data requirements, and mapped data flows in order to identify these purposes.

Recommendation #1: Purposes for Processing Registration Data

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

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

PURPOSE 1 FOR PROCESSING REGISTRATION DATA:

AS SUBJECT TO REGISTRY AND REGISTRAR TERMS, CONDITIONS AND POLICIES, AND ICANN CONSENSUS POLICIES:

(I) TO ESTABLISH THE RIGHTS OF A REGISTERED NAME HOLDER IN A REGISTERED NAME;

(II) TO ENSURE THAT A REGISTERED NAME HOLDER MAY EXERCISE ITS RIGHTS IN THE USE AND DISPOSITION OF THE REGISTERED NAME; AND

(III) TO ACTIVATE A REGISTERED NAME AND ALLOCATE IT TO THE REGISTERED
NAME HOLDER

6. Please choose your level of support for Purpose 1:

Support Purpose intent with wording change

7. If your response requires an edit or deletion of Purpose #1, please indicate the revised wording here (keep in mind that "Purposes" must be GDPR compliant).

8. Please provide rationale for your recommendation.

INTA supports Purpose intent with a modification. The Purpose should be more accurately defined to refer to both the rights “and obligations” of the registered name holder, which reflects the practical and legal context in which a name is registered. For example, a registered name holder provides their contact details not only to establish their claim to a specific domain but also to put third parties on notice of that claim. The name holder also agrees to certain obligations in connection with their registration, and the provision of registration data is integral to establishing the identity of the name holder so that the registrar, registry operators and (potentially) third parties are able to identify the party which has undertaken such obligations. This goes beyond Purpose 3 (described below) which deals with communication.

PURPOSE 2 FOR PROCESSING REGISTRATION DATA

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

9. Choose your level of support of Purpose #2:

Support Purpose intent with wording change

10. If your response requires an edit or deletion of Purpose #2, please indicate the revised wording here (keep in mind that "Purposes" must be GDPR compliant).
ENSURING THE SECURITY, STABILITY, AND RESILIENCY OF THE DOMAIN NAME SYSTEM IN ACCORDANCE WITH ICANN'S MISSION, AS SET FORTH IN ICANN'S BYLAWS TOGETHER WITH ICANN'S COMMITMENTS AND CORE VALUES, THROUGH THE ENABLING OF LAWFUL ACCESS FOR LEGITIMATE THIRD-PARTY INTERESTS, SUCH AS LAW ENFORCEMENT, INTELLECTUAL PROPERTY RIGHTS HOLDERS AND CYBERSECURITY PROFESSIONALS, TO DATA ELEMENTS COLLECTED FOR THE OTHER PURPOSES IDENTIFIED HEREIN.

11. Please provide rationale for your recommendation.

As described in the Bylaws, ICANN’s mission is to “ensure” the security, stability and resiliency of the DNS, not merely “maintain” it. This underscores that ICANN’s policies in this regard are proactive. The scope of ICANN’s Mission was carefully clarified and described in its Bylaws, and this is what should guide the interpretation of this purpose. For clarity sake, reference to the definition in the Bylaws is important. Furthermore, in order to ensure that there are examples of what may constitute legitimate third party interests, INTA believes strongly that those of law enforcement, intellectual property owners, and cybersecurity professionals are recognized as stakeholders in this area. This has been historically true at ICANN and should remain so, and is consistent with ICANN’s obligation to uphold the broader public interest, in furtherance of fulfilling ICANN’s Mission, under its Bylaws.

PURPOSE 3 FOR PROCESSING REGISTRATION DATA

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

12. Choose your level of support of Purpose #3:

Support Purpose intent with wording change

13. If your response requires an edit or deletion of Purpose #3, please indicate the revised wording here (keep in mind that "Purposes" must be GDPR compliant).

ENABLE COMMUNICATION WITH AND/OR NOTIFICATION TO THE REGISTERED NAME HOLDER AND/OR THEIR DELEGATED AGENTS OF TECHNICAL, LEGAL, AND/OR ADMINISTRATIVE ISSUES WITH A REGISTERED NAME.

Please provide rationale for your recommendation.

The existing wording is unduly narrow and fails to acknowledge that the relationship between the registrant and the registrar is a legal one, which includes obligations not only in relation to
the act of registering and technically maintaining the domain name, but other obligations pertaining to the terms of use which are included as part of the framework of agreements and obligations between ICANN, Registry Operators, Registrars and Registrants. These obligations are in accordance with ICANN’s Mission, as set forth in its Bylaws. Communication with the registrant when such terms are breached is a logical and proportionate purpose for data processing.

PURPOSE 4 FOR PROCESSING REGISTRATION DATA

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

14. Choose your level of support of Purpose #4:

Support Purpose as written

15. If your response requires an edit or deletion of Purpose #4, please indicate the revised wording here (keep in mind that "Purposes" must be GDPR compliant).

16. Please provide rationale for your recommendation.

PURPOSE 5 FOR PROCESSING REGISTRATION DATA

HANDLE CONTRACTUAL COMPLIANCE MONITORING REQUESTS, AUDITS, AND COMPLAINTS SUBMITTED BY REGISTRY OPERATORS, REGISTRARS, REGISTERED NAME HOLDERS, AND OTHER INTERNET USERS

Choose your level of support of Purpose #5:

Support Purpose as written

17. If your response requires an edit or deletion of Purpose #5, please indicate the revised wording here (keep in mind that "Purposes" must be GDPR compliant).

18. Please provide the rationale for your recommendation.

PURPOSE 6 FOR PROCESSING REGISTRATION DATA
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, RDRDP, AND FUTURE DEVELOPED DOMAIN NAME REGISTRATION RELATED DISPUTE PROCEDURES FOR WHICH IT IS ESTABLISHED THAT THE PROCESSING OF PERSONAL DATA IS NECESSARY.

19. Choose your level of support of Purpose #6:

Significant change required: changing intent and wording

20. If your response requires an edit or deletion of Purpose #6, please indicate the revised wording here (keep in mind that "Purposes" must be GDPR compliant).

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, BUT INCLUDING WHERE SUCH POLICIES TAKE INTO ACCOUNT USE OF THE DOMAIN NAMES), NAMELY, THE UDRP, URS, PDDRP, RDRDP, AND ANY FUTURE DEVELOPED DOMAIN NAME REGISTRATION-RELATED DISPUTE PROCEDURES FOR WHICH IT IS ESTABLISHED THAT THE PROCESSING OF PERSONAL DATA IS NECESSARY. THIS PURPOSE SHOULD NOT BE READ TO LIMIT ANY OTHER PURPOSE WHERE PROCESSING OF DATA HAS BEEN RECOGNIZED AS LEGITIMATE IN CONNECTION WITH FACILITATING INVESTIGATION AND ACTION CONCERNING ANY OTHER LEGAL ISSUES INVOLVING A DOMAIN NAME, INCLUDING HOW A DOMAIN NAME IS USED.

21. Please provide rationale for your recommendation.

INTA is concerned with the narrow and selective reference to the exclusion of processing for this purpose where it relates “use of domain names”, which ignores long standing ICANN policies applicable to domain name disputes. ICANN’s Bylaws specifically reference policies taking into account the use of domain names as part of ICANN’s mission, and in policy as well as practice, UDRP actions depend on a showing of bad faith relating to the use of a particular domain. The approach of the proposed language in the Initial Report may be seen as an attempt to undermine or alter the implementation of ICANN consensus policy in this area. It is therefore essential that this gross oversight be corrected through the inclusion of the language from the Bylaws. As a point of reference, INTA’s first proposed addition to the purpose statement quotes verbatim the language from the Bylaws.
PURPOSE 7 FOR PROCESSING REGISTRATION DATA

ENABLING VALIDATION TO CONFIRM THAT REGISTERED NAME HOLDER MEETS OPTIONAL GTLD REGISTRATION POLICY ELIGIBILITY CRITERIA VOLUNTARILY ADOPTED BY THE REGISTRY OPERATOR

22. Choose your level of support of Purpose #7:

Support Purpose as written

23. If your response requires an edit or deletion of Purpose #7, please indicate the revised wording here (keep in mind that "Purposes" must be GDPR compliant).

24. Please provide rationale for your recommendation

25. Enter additional comments to Recommendation #1.

Question #1 for Community Input: Purposes for Processing Registration Data

26. If you recommend additional purposes for processing registration data, please enumerate and write them here, keeping in mind compliance with GDPR.

Purposes should reference the need for processing for law enforcement, DNS abuse, IP infringement and consumer protection purposes. INTA also supports clarification of purposes to include research of DNS abuse since this falls squarely within ICANN’s mission and is one of the primary bases for the obligation of registrars to collect registrant data insofar as ICANN is concerned. If these purposes cannot be clarified within the framework of the existing purposes enumerated above, then it may be necessary to include additional purposes.

27. For each additional purpose identified above, please enumerate and provide rationale for each of them.

The list of purposes set forth above are integral to accomplishing ICANN’s mission, and ensuring the health and welfare of the DNS system, for the benefit of individual registrants, as well as the many stakeholders who have an interest in the DNS system.

Section 3, Part 1: Purposes for Processing Registration Data (Continued)

Recommendation #2: Standardized Access
Per the EPDP Team Charter, the EPDP Team is committed to considering a system for Standardized Access to non-public Registration Data once the gating questions in the charter have been answered. This will include addressing questions such as:

- 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, amongst others, disclosure in the course of intellectual property infringement and DNS abuse cases will be considered.

28. Choose your level of support of Recommendation #2:

Support intent of recommendation with edits

29. Do you recommend a change to the wording of Recommendation 2? If so, please indicate proposed edits here.

INTA requests that the general comment in Recommendation #2 be edited to read as follows:

“In this context, amongst others, the EPDP Team will develop a policy that prescribes the method for disclosing non-public registrant data to third parties that have established legitimate interest in viewing registrant data including intellectual property rights holders, cybersecurity firms, organizations that mitigate DNS abuse, and law enforcement agencies, among others.”

30. Please include the rationale for your answers here.

INTA strongly supports this recommendation for the EPDP Team to develop a standardized, or “unified,” system for access to non-public registration data after the gating questions have been answered.

INTA proposes edits to this recommendation to ensure that the protection of intellectual property rights is expressly recognized as a legitimate interest under GDPR and therefore understood to be within scope of the final policy. The term “legitimate” implies that the interest is bolstered by recognition of a legal right, which in the case of intellectual property is the reason for its very existence. Intellectual property rights are regarded as third generation human rights and are duly recognized as human rights under Article 27 (2) of the Universal Declaration of Human Rights. The Article provides that ‘Everyone has the right to the protection of the moral
and material interests resulting from any scientific, literary or artistic production of which he is the author.’

In the Article 29 Working Party’s letter to ICANN dated April 11, 2018, the A29WP “welcome[d] the decision of ICANN to propose an interim model which involves layered access, as well as an “accreditation program” for access to non-public WHOIS data.” This communication signaled A29WP’s support for a standardized access program. This support is further echoed, in a May 27 communication to ICANN, in which the EPDB reiterated that it 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.”

With respect to the reference to “relevant stakeholders,” ICANN has identified “intellectual property rights holders” as being such stakeholders with a legitimate interest in having access to registrant data.

For the reasons expressed above and in deference to the statements provided, INTA recommends the edits provided above.

**Recommendation #3: Contractual Accuracy Requirements**

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.

31. Choose your level of support of Recommendation #3:

Intent and wording of this recommendation requires amendment

32. Do you recommend a change to Recommendation 3? If so, please indicate proposed edits here.

The accuracy requirements under the ICANN contracts and consensus policies need to be reflected in the EPDP recommendations, particularly because accuracy is itself a fundamental component of the GDPR. Greater accuracy will enhance the objectives of compliance with the GDPR while maintaining the WHOIS framework to the greatest extent possible, since accuracy is a common element of both sides of that equation. Therefore, the EPDP should consider requirements to include in its policy recommendations that will support maintaining and enhancing accuracy in the DNS, such as:

- Additional validation - currently only one field is validated as operational under the RAA
(email or telephone number). The EPDP should consider how to expand the validation requirements to include other fields.

- Enhanced compliance tools - ICANN should be given broader powers to investigate the steps taken by a registrar in response to a complaint of inaccuracy, and to require registrars with unacceptably low accuracy rates to submit remediation plans.
- Cross-field address validation - ICANN should implement this requirement under the 2013 RAA.
- Rectification - ICANN should ensure that there is a standard, robust process for data subjects to have their data corrected.
- Accuracy Reporting System -- ICANN should continue publishing its periodic Accuracy Reports, and the policy should allow ICANN the ability to access the full WHOIS records necessary to conduct this analysis.

33. Please include the rationale for your answers here.

GDPR Article 5 states that personal data shall be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay."

The ICO (Information Commissioner’s Office in the UK) points out in its “Principle (d): Accuracy” that one of the new features of GDPR as compared to the principles under its predecessor is that there is now a “clearer proactive obligation to take reasonable steps to delete or correct inaccurate personal data.” The ICO notes that “[i]n order to ensure that your records are not inaccurate or misleading in [the case of personal data someone else provides], you must:

- take reasonable steps in the circumstances to ensure the accuracy of the information; and
- carefully consider any challenges to the accuracy of the information."

The ICO goes on to say that “The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you are using the data to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy. This may mean you have to get independent confirmation that the data is accurate.” The accuracy of WHOIS significantly affects not just the registrant but those third parties that access WHOIS for legitimate purposes such as intellectual property infringement of all types.

The EPDP had been chartered to ensure that the new WHOIS policy complies with all of the principles of the GDPR. As a result, its work is not complete until it conducts a careful analysis.
of GDPR’s accuracy principles, and updates the WHOIS policy to address the unacceptably low levels of accuracy that exists today.

Section 3, Part 2: Required Data Processing Activities Recommendation #4: Data Elements

The EPDP Team recommends that the data elements defined 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 (or automatically generated):

Data Elements (Collected and Generated) Note, Data Elements indicated with ** are generated either by the Registrar or the Registry.

<table>
<thead>
<tr>
<th>Data Elements (Collected and Generated)</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name**</td>
<td></td>
</tr>
<tr>
<td>Registry Domain ID**</td>
<td></td>
</tr>
<tr>
<td>Registrar Whois Server**</td>
<td></td>
</tr>
<tr>
<td>Registrar URL**</td>
<td></td>
</tr>
<tr>
<td>Updated Date**</td>
<td></td>
</tr>
<tr>
<td>Creation Date**</td>
<td></td>
</tr>
<tr>
<td>Registry Expiry Date**</td>
<td></td>
</tr>
<tr>
<td>Registrar Registration Expiration Date**</td>
<td></td>
</tr>
<tr>
<td>Registrar**</td>
<td></td>
</tr>
<tr>
<td>Registrar IANA ID**</td>
<td></td>
</tr>
<tr>
<td>Registrar Abuse Contact Email**</td>
<td></td>
</tr>
<tr>
<td>Registrar Abuse Contact Phone**</td>
<td></td>
</tr>
<tr>
<td>Reseller**</td>
<td></td>
</tr>
<tr>
<td>Domain Status**</td>
<td></td>
</tr>
<tr>
<td>Registry Registrant ID**</td>
<td></td>
</tr>
</tbody>
</table>

Registrant Fields:

- Name
- Organization (optional)
Street
City
State/province
Postal code
Country
Phone
Phone ext (optional)
Fax (optional)
Fax ext (optional)
Email
Tech ID

(optional)

Tech Fields:

• Name (optional)
• Phone (optional)
• Email (optional)
• Name Server
• DNSSEC

(optional)

Name Server IP Address**

Last Update of Whois Database**

Additional optional 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].

Question #2 for Community Input

34. Do you agree that all these data elements should be collected / generated to achieve the Purposes identified in the Initial Report?

Yes

35. If your answer is ‘no’, please enumerate which data elements should not be collected / generated.
36. Please provide the rationale for your answer.

INTA strongly supports the proposition that all data elements should continue to be collected/generated and that they should continue to be made freely available to the greatest extent possible while remaining GDPR compliant. In addition to supporting the various Purposes identified in the Initial Report, collection and access to these data elements support various other important public interests, including (a) consumer protection against counterfeits, fraud, phishing schemes etc., (b) the ability of law enforcement to efficiently respond to online criminal activity, and (c) efforts by brand owners to protect their brands online. Additionally, it is critically important to note that domain names commonly trade on the private market for millions of dollars. It has become commonplace for domain names to be worth more than most homes around the world. Accordingly, it is an unreasonable burden to place on the buyers in these transactions to mask the identity of the sellers, and thereby frustrate the ability to conduct diligence on the provenance of the domain. Like with any other financial transaction of this size, Buyers need to be afforded the protection of knowing the seller’s identity so that they can conduct the necessary due diligence and ensure that, for example, they are not dealing with a foreign government, funding any illicit activity, or even purchasing the domain from one of their employees.

37. If you believe additional data elements should be collected / generated, please enumerate which additional elements should be collected / generated.

38. Please provide the rationale for your answer.

Recommendation #4 Continued: Optional Data Elements

The EPDP Team recommends that the following data elements are optional for the Registered Name Holder (RNH) to provide:

- technical contact name
- technical contact email and
- technical contact phone number

The EPDP Team has discussed two definitions of the term “optional” as used in this recommendation:

(1) registrars must offer the data field and registrants can decide whether to fill in the field or leave in blank (in which case the query would return the registered name hold data; OR

(2) registrars can offer this field at their option.
39. Should the technical contact fields be optional or mandatory (where mandatory means the registrar must offer the fields AND the RNH must fill in information)?

Optional

40. Please provide the rationale for your answer.

INTA does not believe that collection of Technical Contact information should be “Mandatory”, however, the OPTION to provide this information should be required as some Registrants may wish to provide this information in order to route the appropriate communications within their organization. Therefore, INTA believes that Registrars should be **required** to provide Registrants with the “OPTION” to provide Technical Contact information, although provision of this information by registrants should not be mandatory.

41. If your answer is 'optional', should registrars be required to offer these technical contact fields?

Yes

42. Please provide the rationale for your answer.

INTA does not believe that collection of Technical Contact information should be mandatory. However, the option to provide this information should be required as some Registrants may wish to provide this information in order to route the appropriate communications within their organization. Therefore, INTA believes that Registrars should be **required** to provide Registrants with the “OPTION” to provide Technical Contact information, although provision of this information by registrants should not be mandatory.

43. The EPDP team recommends that contact information for billing and administrative contacts should not be collected. Do you agree that this information should not be collected?

No

44. Please provide the rationale for your answer.

INTA does not believe that collection of Billing and Administrative Contact information should be mandatory. However, the option to provide this information should be required as some Registrants may wish to provide this information in order to route the appropriate
communications within their organization. Therefore, INTA believes that Registrars should be **required** to provide registrants with the “OPTION” to provide Billing and Administrative Contact information, although provision of this information should not be mandatory.

**Recommendation #5: Transmission of Data from Registrar to Registry**

The EPDP Team recommends that the specifically identified data elements under “[t]ransmission of registration data from Registrar to Registry” within the data elements workbooks must be transferred from Registrar to Registry. In the aggregate, these data elements are the same as those in Recommendation #4 for the reasons stated in the Data Workbooks found in Annex D of the Initial Report.

**45. Do you agree that all these data elements should be transferred from the registrar to the registry?**

INTENTIONALLY OMITTED

**Recommendation #6: Transmission of Data to Data Escrow Providers**

1. The EPDP Team recommends that ICANN Org enter into legally compliant data processing 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 workbooks that analyze the purpose to provide mechanisms for safeguarding Registered Name Holders’ Registration Data.

3. The data elements workbook that analyzes the purpose to provide mechanisms for safeguarding Registered Name Holders’ Registration Data contains the specifically identified data elements the EPDP Team recommends be transferred by Registries and Registrars to data escrow providers (see Annex D, Workbook 4).

**46. Choose your level of support of Recommendation #6:**

INTENTIONALLY OMITTED

**Recommendation #7: Transmission of Data from Registries/Registrars to ICANN Compliance**

1. The EPDP Team recommends that updates are made to the contractual requirements for registries and registrars to transfer to ICANN Compliance the domain name registration data that they process when required/requested, consistent with the data elements workbook that analyzes the purpose to handle contractual compliance monitoring requests, audits, and complaints submitted by Registry Operators, Registrars, Registered Name Holders, and other
2. The data elements workbook that analyzes the purpose to handle contractual compliance monitoring requests, audits, and complaints submitted by Registry Operators, Registrars, Registered Name Holders, and other Internet users contains the specifically-identified data elements the EPDP Team recommends be transferred from registries and registrars to ICANN Compliance (see Annex D, Workbook 5).

47. Choose your level of support of Recommendation #7:

Support recommendation as written

48. Do you agree that all of these data elements should be transferred from the registrar to ICANN?

Yes

49. If your answer is ‘no’, please enumerate which data elements should not be transferred from the registrar to ICANN.

50. Please provide the rationale for your answer.

51. Enter additional comments for Recommendation #7 here.

INTA supports compliance having all the data it needs to efficiently carry out its vital function to ensure that contractual obligations are being met, and issues are resolved as quickly as possible. This is particularly vital in the context of ICANN Compliance activities to support the combat of DNS abuse.

**Recommendation #8: Data Redaction**

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 in a freely accessible directory.

NOT REDACTED
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Registrar Whois</th>
<th>Server Registrar</th>
<th>URL Updated Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation Date</td>
<td>Registry Expiry</td>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>Registrar Registration Expiration</td>
<td>Date Registrar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registrar IANA ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registrar Abuse Contact</td>
<td>Email Registrar Abuse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact Phone Reseller</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domain Status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registrant Fields</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• State/province</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Country</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Anonymized email / link to web form</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tech Fields</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Anonymized email / link to web form</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NameServer(s) DNSSEC No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name Server IP Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Update of Whois Database</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REDACTED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Registrant Fields</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Street</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• City</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Postal code</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Phone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Email</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Tech Fields

- Name
- Phone
- Email

UNDECIDED (REDACTED/ NOT REDACTED)

- Organization (opt.)


52. Do you agree that all of these data elements should be redacted?

No

53. If your answer is ‘no’, please enumerate the data elements that should not be redacted.

INTA supports publication of Registrant Email, Organization, and Registrant City. None of these data elements should be redacted.

54. Please provide the rationale for your answer.

In order to minimize consumer harm, it is important that swift action is taken in instances of suspected malicious activity. Malicious sites support a range of harmful bad practices including offering counterfeit goods or services, infringing trademarks or supporting some other illegal purpose like the support of malware. Typically, when a rights holders begins an investigation into whether a website is malicious, the email address is the first line of inquiry. Knowing the Registrant's city is another data point used to determine whether the site may be controlled by a bad actor or, instead, a business partner or other friendly entity. As important as it is to find bad actors, it is equally important to identify authorized users and avoid unnecessary enforcement actions including UDRP filings or other means of enforcement. Access to accurate and timely information can help rights holders avoid bringing registrants into the UDRP process unnecessarily.

From a privacy perspective, oftentimes a Registrant’s Email address will not have sufficient identifying information to be able to decipher personal information, while still giving others an opportunity to correspond directly with the Registrant. Practically speaking, Registrants may provide email addresses without any personally identifying information. The implications of
using email with personally identifiable information could be explained to Registrants during the domain name registration process. Therefore, Registrants will have full notice as to the accessibility of the email address and the ability to provide an email address with non personally identifying information. The legal basis of GDPR Article 6.1 (f) and corresponding balancing tests support the exercise of rights and furtherance of interests of third parties including law enforcement and intellectual property rights holders. The risk of the Registrant receiving unsolicited emails must be weighed against the risk of perpetuating online abuse and consumer fraud.

As explained in INTA’s response to Purpose 1 above, Registrants have rights and obligations within the domain name system. The risk of the Registrant receiving unsolicited communication cannot outweigh the accountability and transparency necessary when operating a website or email address related to a domain name. Alternatives like communicating through an anonymized email address or web form are not sufficient to overcome the challenges of redacted email. This is because communications from anonymized email addresses or web forms may either be marked as spam or never be properly forwarded. The net effect is that a third party attempting to get in contact with a Registrant would not be able to know if the email failed or if the Registrant is simply not responsive.

Redacting or masking the email address of Registrants unduly restricts law enforcement, enforcement of intellectual property rights and consumer protection. It also prevents parties from amicably settling disputes related to potential online infringements and may trigger unnecessary legal actions based on the failure to properly identify a party prior to a legal filing. Many of these harms are rightfully avoided by publishing an accurate, contactable email address.

The rationale for publishing organization information is more thoroughly explained below.

55. The EPDP Team is of divided opinion as to whether “Organization” should be redacted for reasons stated in the Initial Report. Please see the Initial Report, beginning on p. 42. Should the “Organization” field be redacted?

No

Please provide rationale for your answer above.

The Organization field is critical for being able to determine additional non-private information about a particular Registrant. If a registrant is associated with a rights holder or their partner, the rights holder will be able to identify that perhaps only if the Organization field is not redacted. Being able to see this information can offer rights holders an opportunity to identify and work
with registrants outside of the UDRP or other dispute resolution system and make more educated decisions about whether or not a given domain name is malicious or not. As explained more thoroughly below, appropriate instructions can be given so as to avoid the Organization field containing personal identifying information.

56. Enter additional comments for Recommendation #8.

N/A

Recommendation #9: Organization Field

The EPDP Team recommends that registrars provide further guidance to a Registered Name Holder concerning the information that is to be provided within the Organization field. (For further information, please refer to the Initial Report discussion, beginning on p. 42).

57. Choose your level of support of Recommendation #9:

Support recommendation as written

58. If your response requires an edit or deletion of Recommendation #9, please indicate the revised wording here.

59. Please provide the rationale for your answer.

As discussed fully in the answer to Recommendation #11 below, any ICANN Consensus Policy for generic top-level domain Registration Data should include a clear distinction between the treatment of data belonging to natural persons and data belonging to legal persons. Clear registrar guidance explaining to Registered Name Holders what information should and should not be included in the Organization field would help ensure that this distinction is clearly delineated, easy to follow, and consistent with the requirements of the GDRP while at the same time supporting accurate, reliable, and uniform Registration Data and preserving an ability to address law enforcement needs, intellectual property protection, consumer protection issues, and DNS abuse.

Specifically, the very act of informing the public that the Organization field is reserved for Registered Name Holders that are legal persons should significantly reduce the likelihood that personal information is inadvertently entered into the Organization field. Additionally, providing further guidance about the Organization field to Registered Name Holders can help address concerns specific to certain types of businesses. For example, Registered Name Holders that are sole proprietors can be instructed to only fill out the Organization field if they do business...
under a fictitious name. Similarly, legal entities with names that include the personal name of an affiliated person can be instructed to either use a d/b/a in the Organization field or forego filling out the Organization field entirely.

60. Additional comments for Recommendation #9.

Recommendation #10: Provision of Email Address/Web Form

In relation to facilitating email communication between third parties and the registrant, the EPDP Team recommends that current requirements in the Temporary Specification that specify that a 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, remain in place.

61. Choose your level of support of Recommendation #10:

Delete recommendation

62. If you believe edits are needed for Recommendation #10, please propose edits here.

INTA supports deleting this recommendation, as explained further below. In the alternative, INTA supports amending the recommendation to read: “In relation to facilitating email communication between third parties and the registrant, the EPDP Team recommends that current requirements in the Temporary Specification that specify that a 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, remain in place. HOWEVER, a Registrar MUST ensure that the email or web form is delivered to the registrant, and if it is not must inform the party seeking contact that the communication cannot be delivered to the registrant as the registrant has provided inaccurate contact information. A Registrar MUST then promptly take steps to secure accurate contact information.”

63. Please provide the rationale for your answer.

As explained more thoroughly in the response to Recommendation 8, INTA supports publication of the Registrant’s email address so that third parties may more easily identify and contact the Registrant directly. However, if the consensus of the EPDP working group is that such information should remain redacted, INTA requests that Registrars be required to ensure that the anonymized email address or web form contact, in fact, reaches the Registrant. Third parties looking to reach a Registrant often do not know if an anonymized email or web form reached the Registrant, or if the Registrant is simply ignoring the communication. If Registrars were
required to not only ensure the accuracy of registrant contact information, but also notify a party seeking contact that the information did not reach its destination, then it may be possible to rely on anonymized email or web form only.

64. Additional comments for Recommendation #10.

N/A

Recommendation #11: Data Retention

The EPDP Team recommends that Registrars are required to retain the herein-specified data elements for a period of one year following the life of the registration. This retention period conforms to the specific statute of limitations within the Transfer Dispute Resolution Policy (“TDRP”).

65. Choose your level of support of Recommendation #11:

INTENTIONALLY OMITTED

Question 3 for Community Input: Differentiating Registrants: Legal v. Natural Persons; and Effects of Geographic Location

66. 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? (For more information, please refer to the Initial Report, beginning on p. 47.

As INTA has noted previously, it shares ICANN’s objective to “identify the appropriate balance for a path forward to ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible.” In other words: whatever Consensus Policy emerges from the EPDP should be “calibrated” as much as possible – so as not to over-comply with the GDPR. INTA thus agrees with the reasoning of the BC and IPC, as articulated in the Initial Report, that Contracted Parties should be required (not merely permitted) to make differentiations (for example, in what gTLD registration data should be redacted vs. published in the public WHOIS) that are consistent with the territorial scope of the GDPR. At the least, INTA suggests that the EPDP consider other factors on this “permitted vs. required” distinction, such as: (a) the risk of fragmentation from a non-mandatory, permissive regime; and (b) whether existing examples where registries and registrars are already making similar kinds of differentiations may shed any light on the feasibility of how to do so at scale.
That said, for the reasons outlined below, INTA does not necessarily agree with the premise of this question that the differentiation that Contracted Parties should be required (not merely permitted) to make will always necessarily be “on a geographic basis”. As the Initial Report notes, the actual location of the registrant is not always dispositive as to whether GDPR applies. Fortunately, the EDPB has recently issued Guidelines on this exact question – the territorial scope of the GDPR – that are illustrative in this regard.[5] For that reason, INTA also respectfully suggests that the EPDP consider (c) the recent guidance on the territorial scope of the GDPR from the EDPB.

67. Please provide the rationale for your above answer.

a) **Fragmentation.**

As noted in Section (e) of the EPDP Initiation Request, fragmentation of the WHOIS system is a policy outcome to be avoided – at least in part because it could jeopardize the security and stability of the Internet. INTA agrees with this. And so too, apparently, do those members of the EPDP (specifically, the Contracted Parties and the NCSG) who oppose requiring differentiation between registrants consistent with the territorial scope of the GDPR. As they have argued in the Initial Report: “Not having a common approach for all registrants could lead to two classes of registrants, which may result in competitive advantages to certain registrars/registries (due to their establishment in jurisdictions with privacy protection), fragmentation in the marketplace and interoperability issues.” See: Initial Report at 48.

In that sense, INTA and the Contracted Parties/NCSG appear to agree on the overarching policy objective – that “RDS policies should be as unified as possible”, and that fragmentation is problematic. They just disagree on how to get there – specifically, on whether a “permissive” or “mandatory” policy is most likely to do so.

On that specific disagreement, INTA does not understand how permitting but not requiring differentiation is somehow going to result in *less* (not more) fragmentation. The whole point of a “permissive” regime (as opposed to a mandatory one) is to allow each Contracted Party to make decisions as to differentiations on their own. The Contracted Parties/NCSG admit as much when they state:

> There are significant liability implications for Contracted Parties if they are incorrect in applying the appropriate data protection rules. Contracted parties should be free to choose whether or not to take that risk as a business decision rather than a contractual requirement.

Whatever the merits of that argument on its own terms, it is clearly contrary to the reasoning of the EPDP Initiation Request, which cautioned *against* an outcome in which “each registry
operator and registrar might make their own determination regarding what gTLD registration data should be collected, transferred and published, leading to a fragmentation of the globally distributed WHOIS system and the handling of gTLD registration data.” (emphasis added). Obviously, different Contracted Parties are going to have different risk tolerances – and thus are going to answer this question, and others, differently. The whole point of a consensus policy is to avoid that kind of fragmented decision-making. INTA does not understand – and the Initial Report does not make clear – why this differentiation question is somehow special, such that it would warrant an exception to the general preference that RDS policies be as unified as possible.

b) Existing examples.

Unlike Question 90 below, which asks for “existing examples where a legal/natural differentiation is already made”, for some reason the questions from the EPDP do not ask for existing examples where differentiations based on geography are already made. In that sense, the questions from the EPDP appear to take at face value (or at least, do not solicit any input from public comments that may be contrary to) the claims from the Contracted Parties/NCSG that: 1) “It is often difficult to identify a registrant's applicable jurisdiction with sufficient certainty to apply appropriate data protection rules”; and 2) that “Any consensus policy needs to be commercially reasonable and implementable, and in the current market place, differentiation based on geographic location will be difficult to scale, costly, and, accordingly, neither commercially reasonable nor implementable.”[4] It is unfortunate that the EPDP did not ask for any input testing or challenging those assumptions – because the claim that geographic differentiation is somehow commercially unreasonable is inconsistent with numerous examples from the current marketplace that specifically differentiate between registrants on a geographic basis. Most obviously, various ccTLDs restrict registration to registrants with a nexus to a particular geographic region. (See, e.g., https://eurid.eu/d/205796/Registration_Policy_EN.PDF (outlining eligibility criteria for the .eu ccTLD); https://www.about.us/policies/ustld-nexus-requirements (outlining the United States nexus requirement for the .us ccTLD); https://cira.ca/sites/default/files/public/policy/cprregistrants-en.pdf (outlining the Canadian presence requirements for the .ca ccTLD).

Likewise, various “geographic” gTLDs also restrict registration to registrants with a nexus to a particular geographic region. (See, e.g., https://www.ownit.nyc/policies/nyc-nexus-policy (“Registrants in .nyc must be either: a natural person whose primary place of domicile is a valid physical address in the City of New York . . . ; or an entity or organization that has a physical street address in the City of New York . . . ”).) In addition, it appears that at least some registrars (such as GoDaddy) are already making geographic differentiations for purposes of providing various privacy-related account-management services to their customers.
These examples belie the claim that differentiation based on geography is neither commercially reasonable nor implementable. At the least, they suggest that the EPDP should consider as an additional factor how the registries and registrars that are already making such differentiations have been able to do so.

c) **EDPB Guidelines.**

For the foregoing reasons, INTA sees no credible argument that differentiation should be permitted but not required (at least if uniformity is to be preferred over fragmentation). But INTA does agree with the point raised in the Initial Report that the actual location of the registrant may not always be dispositive as to whether the GDPR will apply. Fortunately, the EDPB has recently issued helpful Guidelines on that exact question – the territorial scope of the GDPR. INTA will not attempt in this Comment to exhaustively summarize those Guidelines. But in general terms, they do support a potential Consensus Policy that would require Contracted Parties to, for example, only redact gTLD registration data when: 1) the Contracted Party is collecting such data within the context of the activities of “an establishment in the EU” (as that term is defined in the EDPB Guidelines); or 2) when the Contracted Party is “targeting” domain-name registration services to individuals in the EU (as that term is also defined in the EDPB Guidelines). At a minimum, INTA suggests that the EPDP consider the recent EDPB Guidelines as an additional factor on this issue.

68. Are there any other risks associated with differentiation of registrants on a geographic basis? If so, please identify those factors and/or risks and how they would affect possible recommendations, keeping in mind compliance with the GDPR.

The question assumes the conclusion – that there are some risks associated with differentiation. And it does not ask the converse question: whether there are any risks associated with **not** requiring (but merely permitting) differentiation – such as the substantial risk of fragmentation that will result if each Contracted Party is permitted to make its own determination on the basis of its own unique risk tolerance.

69. What other factors should the EPDP team consider about whether Contracted Parties should be permitted or required to differentiate between natural and legal persons?
Considering the risk of fragmentation from a permissive regime and existing examples where a legal/natural differentiation is already made, INTA is of the view that this distinction is necessary and practicably achievable.

The solution that the Contracted Parties/NCSG have proposed (namely, that differentiation between natural and legal persons should be permitted, but not required) appears to suit the conveniences of those parties, but is an incongruous means of addressing the purported risk of possible inadvertent disclosure of personal data relating to natural persons who work for or represent a legal person – such as natural persons who manage administrative or technical issues on behalf of a legal person registrant. The EPDP should not ignore that if policy makers and legislators had intended the GDPR to cover a broader group of data subjects, they would have specifically said so. While implementation may be a challenge, ICANN should not through its policies effectively extend the reach of the GDPR to an entirely separate class of data subject.

70. Please provide the rationale for your above answer.

a) **Fragmentation**

INTA has provided its rationale as to “fragmentation” in its Response to the question above.

b) **Existing examples**

INTA has provided its rationale as to “existing examples” in its Response to the question above and has provided existing examples for the “legal vs. natural person” distinction in its Response to the question below.

c) **Fit**

INTA agrees with the Initial Report that there may be some risk that stems from the fact that natural persons employed by a legal person (and who may be designated as the registrant, admin, or technical contact for that legal person) still enjoy rights and protections under the GDPR – even if their employer does not.[1] INTA is concerned that the Initial Report does not explain why the EPDP thinks the best way to address that risk is to permit Contracted Parties to make their own determination as to whether (and how) to differentiate between legal and natural persons. INTA respectfully suggests that a permissive regime would more likely exacerbate that risk (given the lack of uniformity for registrants across different Contracted Parties) than ameliorate it.

INTA supports the alternative proposal referenced in the Initial Report namely, that the risk of inadvertent disclosure “may be minimized through clear explanatory language beneath each field when filling in data fields within domain name registrations”. This solution is far more likely
to address the potential risk identified. INTA does not share the concern that such explanatory language may be somehow inconsistent with the concept of “privacy by design.” This solution seems tailored for privacy by design. It stands to reason that a policy that leaves the decision of how to handle the legal vs. natural person distinction to each Contracted Party to implement different safeguards on their own will be riddled with inconsistencies. On the other hand, a policy that implements, by design, a consistent explanatory language beneath each data field minimizes the risk of inadvertent disclosure for all registrants across all registries and registrars. Registrants are, therefore, offered informed choice rather than arbitrary decision making by a third party. This outcome is consistent of GDPR principles that keep control of the data with the data subject.

71. Should there be further study as to 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? Please provide a rationale.

INTA would welcome further study on procedures that could improve the means to distinguish between different registrants for the purposes of more accurately and precisely applying the GDPR. However, INTA would also wish to note that the Guidelines on the territorial scope of the GDPR that were recently issued by the EDPB shed a great deal more light on what factors need to be taken into account, and should be considered along with additional data about how the registries and registrars that are already making these types of differentiations (namely, geographic differentiations; or legal person vs. natural person differentiations) have already been able to do so.

72. Are you aware of existing examples where a legal/natural differentiation is already made and could it apply at a global scale for purposes of registration data? If yes, please provide additional information.

Yes. The registry that operates the .TEL gTLD makes this differentiation. So does the .eu ccTLD. See https://www.do.tel/wp-content/uploads/2017/05/Whois_Policy.pdf ("With respect to the amount and type of domain name registrant data provided in response to queries of the WHOIS service by the general public, the WHOIS service will distinguish between domain name registrants that are companies, businesses, partnerships, non-profit entities, associations, or other types of legal constructs (‘Legal Persons’), and domain name registrants that are human beings, perceptible through the senses and subject to physical laws (‘Natural Persons’). Domain name registrants will be required to specify whether they qualify as Legal Persons or Natural Persons by clicking the appropriate box during the registration process.").

See also https://eurid.eu/d/205797/whois_policy_en.pdf.
Recommendation #12: Reasonable Access

The EPDP Team recommends that the current requirements in the Temporary Specification in relation to reasonable access remain in place until work on a system for Standardized Access to Non-Public Registration Data has been completed, noting that the term should be modified to refer to “parameters for responding to lawful disclosure requests.” Furthermore, the EPDP Team recommends that criteria around the term “reasonable” are further explored as part of the implementation of these policy recommendations addressing:

- [Practicable]* timelines criteria for responses to be provided by Contracted Parties;
- Format by which requests should be made and responses are provided;
- Communication/Instructions around how and where requests should be submitted;
- Requirements for what information responses should include (for example, auto-acknowledgement of requests and rationale for rejection of request);
- Logging of requests.

[*Some concern expressed that timeliness that should not be translated into requirements that are impractical for contracted parties].

73. Choose your level of support of Recommendation #12:

Support intent of recommendation with edits

If you believe edits are needed for Recommendation #12, please propose them here.

INTA recommends that the clause:

“Furthermore, the EPDP Team recommends that criteria around the term “reasonable” are further explored as part of the implementation of these policy recommendations addressing:”

Be amended to read:

“Furthermore, the EPDP Team recommends that definitions, criteria and processes around the term "reasonable access" will be determined as part of the final policy including how to address:”

74. Please provide the rationale for your answer.

Third parties that currently have a legitimate interest and lawful purpose for gaining access to non-public registrant data face a confusing array of different registrar and registry requirements and processes to access this data making such access extremely difficult, inefficient and, in many cases, non-existent.
Third parties that currently have a legitimate interest and lawful purpose for gaining access to non-public registrant data face a confusing array of different Registrar and Registry requirements and processes to access this data making such access extremely difficult, inefficient and, in many cases, non-existent.

INTA members, through responses submitted to INTA’s WHOISchallenges.org mailbox, report that ICANN’s implementation of the Temporary Specification has adversely affected access and usage of domain name registration information and the ability to address infringing activity and to mitigate abuse. With only a small percentage of Registrars returning complete WHOIS records, the impact felt by the absence of Registrant data is pervasive. Data recently published by MarkMonitor, an INTA member, revealed that nearly 80% of the requests for registrant data made to Registrars have been either ignored or denied. While the EPDP Team works on a future policy regarding standardized access as referenced in Recommendation #2, the EPDP Team should now also define and develop simple processes around “reasonable access” and make sure that implementation details of these processes are completed within this EPDP and not delayed until future discussions regarding implementation.

Recommendation #13: Joint Controller Agreements

Based on the information and the deliberations the EPDP Team had on this topic and pending further input and legal advice, the EPDP Team recommends that ICANN Org negotiates and enters into a Joint Controller Agreement (JCA) with the Contracted Parties.

In addition to the legally required components of such agreement, the JCA shall specify the responsibilities of the respective parties for the processing activities as described below. Indemnification clauses shall ensure that the risk for certain data processing is borne by either one or multiple parties that have the primary interest in the processing.

75. Choose your level of support of Recommendation #13:

INTENTIONALLY OMITTED

Section 3, Part 3: Data Processing Terms

Recommendation #14: Data Processing Roles & Responsibilities

The EPDP Team recommends that the policy includes the following data processing activities as well as responsible parties. Please reference the Initial Report, beginning on p. 63 for further details.
76. Choose your level of support of Recommendation #14:

INTENTIONALLY OMITTED

Recommendation #15: Uniform Rapid Suspension/Uniform Domain Name Dispute Resolution Policy Requirements

The EPDP Team recommends that for the new policy on gTLD registration data, the requirements of the Temporary Specification are maintained in relation to URS and UDRP until such time as these are superseded by recommendations from the RPMs PDP WG (if any).

77. Choose your level of support of Recommendation #15:

Support recommendation as written

78. Additional comments for Recommendation #15.

The lack of WHOIS information available to a complainant before filing a complaint is so limited that proving bad faith in an initial complaint is very difficult when the identity of the registrant is not known. For example, a complainant cannot know if the registrant has engaged in a pattern of cybersquatting. The complainant cannot know if the registrant has a legitimate interest in the domain without knowing the registrant’s identity. The UDRP Rules should include a rule specifically:

1) permitting complainants sufficient time to investigate and amend a complaint upon learning the identity of the registrant, and 2) requiring registrars to provide the complainant with a full list of all other domains owned by the registrant through the registrar.

Recommendation #16: Instruction to GNSO and Rights Protection Mechanisms Policy Development Working Group

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.

79. Choose your level of support of Recommendation #16:
Support recommendation as written

80. **Provide additional comments for Recommendation #16 here.**

While complainants are generally given leave to amend the complaint through jurisprudence, the UDRP and URS should include a formal rule that acknowledges the need for an amended complaint. Learning the identity of the respondent will prompt the complainant to investigate additional facts, evidence, and arguments that may apply. Therefore, the rules should permit a minimum of 30 days to amend the complaint after the identity information is communicated to the complainant. The rules should also be amended to allow a complainant to voluntarily withdraw its complaint without prejudice within five (5) days after receiving the registrant’s identity if the complainant reasonably believes that further prosecution of the complaint would be in bad faith and result in a reverse domain name hijacking decision.

**Recommendation #17: UDRP/URS**

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.

81. **Choose your level of support of Recommendation #17:**

Support recommendation as written

**Recommendation #18: Data Processing Agreements**

The EPDP Team recommends that ICANN Org must enter into data processing agreements with dispute resolution providers in which, amongst other items, the data retention period is specifically addressed, as this will affect the ability to have publicly-available decisions.

82. **Choose your level of support of Recommendation #18:**

Support recommendation as written

83. **Provide additional comments for Recommendation #18 here.**

There is a legitimate interest in requiring that decisions and the identity of the parties remains
available in perpetuity. In particular, adverse results in a prior action can be evidence of bad faith, which the Panel should be permitted to take into account.

**Question #4 for Community Input**

84. **Are there any changes that the EPDP Team should consider in relation to the URS and UDRP that have not already been identified?**

While it may be a procedural matter that does not rise to the level of policymaking, the UDRP Section 4.a. distinguishes between an *assertion* that the three elements are met, and the subsequent *administrative proceeding* where the complainant must prove the elements. We encourage the EPDP Team to explore whether policymaking is the appropriate avenue to clarify that disclosure of non-public WHOIS data can be made in the period between assertion and the proceeding, and to explore controls that could be included in the policy to prevent abuse of such a system.

85. **If so, please provide the relevant rationale, keeping in mind compliance with the GDPR.**

As noted above, complainants have been disadvantaged by large-scale redaction of registrant data. Anecdotally, INTA member, MarkMonitor is aware of more than one large organization that has spent thousands of dollars to draft and file a UDRP only to find, upon registrant data disclosure, that the registrant was a department within the same organization and the UDRP had been filed against themselves. By building smart policy around the procedural distinction between assertion and proceeding, the EPDP Team could easily fix this broken system.

**Recommendation #19: Transfer Policy**

The EPDP Team recommends that for the new policy on gTLD registration data, the requirements of the Temporary Specification are maintained 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.

86. **Choose your level of support of Recommendation #19:**

INTENTIONALLY OMITTED

**Recommendation #20: Transfer Policy**
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.

87. **Choose your level of support of Recommendation #20:**

   INTENTIONALLY OMITTED

**Question #5 for Community Input**

INTENTIONALLY OMITTED

**Section 3: Other Recommendations**

Enter any general comments or observations you may have on the findings in Section 3, Other Recommendation.

INTENTIONALLY OMITTED

**Recommendation #21: Joint Controller and Data Processing Agreements**

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.

88. **Choose your level of support of Recommendation #21:**

   INTENTIONALLY OMITTED

89. **If you do not support Recommendation #21, please provide proposed edits/changes here**

90. **Please provide the rationale for your answer here, keeping in mind compliance with GDPR.**
91. **Provide additional comments for Recommendation #21 here.**

**Recommendation #22: Updates to Existing Consensus Policies**

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 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

Please reference the Initial Report, beginning on p. 71 for further details.

92. **Choose your level of support of Recommendation #22:**

**INTENTIONALLY OMITTED**

**Other Comments & Submission**

93. **Are there any other comments or issues you would like to raise pertaining to the Initial Report? If yes, please enter your comments here. If applicable, please specify the section or page number in the Initial Report to which your comments refer.**

**INTENTIONALLY OMITTED**