BC Response to EPDP On the Temporary Specification for gTLD Registration Data Public Comment Proceeding Input Form

* Required

BC members can edit and annotate this doc, and we will paste our final answers into the Google Form when it is time to submit.

Important Instructions PLEASE READ BEFORE PROCEEDING

This Public Comment forum seeks community feedback on the Initial Report published by the Expedited Policy Development Process (EPDP) Team on the Temporary Specification for gTLD Registration Data.

This is a new format for collecting public comment. It seeks to:
Clearly link comments to specific sections of the initial report
Encourage commenters to provide reasoning or rationale for their opinions
Enable the sorting of comment so that the EPDP team can more easily read all the comments on any one topic

There is no obligation to complete all sections within this form – respond to as many or as few questions as desired. Additionally, there is the opportunity to provide comments on the general content of the Initial Report or on new issues not raised by the Initial Report. To preview all questions in the Google Form, please refer to a Word version of this form here [LINK TBD].

As you review the "Questions for Community Input" in the Initial Report, you will note that there is not a 1:1 correspondence with the questions asked in the Public Comment format. This is because, in some instances, the "Questions for Community Input" have been divided into multipart questions so that feedback on these questions would be clear. The Initial Report and Comment Forum have been reviewed to ensure that all the "Questions for Community Input" have been addressed in this Comment Forum.

It is important that your comments include rationale (i.e., by answering the “rationale” question in each section). This is not a vote. The EPDP team is interested in your reasoning so that the conclusions reached and the issues discussed by the team can be tested against the reasoning of others. (This is much more helpful than comments that simply “agree” or “disagree”).

NOTES:
Please refer to the specific recommendation and relevant section or page number of the Initial Report for additional details and context about each recommendation. Where applicable, you are encouraged to reference sections in the report for ease of the future review by the EPDP Team.

Your comments should take into account scope of the EPDP as described by the Charter and General Data Protection Regulation (GDPR) compliance.

For transparency purposes, all comments submitted to the Public Comment forum will be displayed publicly via an automatically generated Google Spreadsheet. Email addresses provided by commenters will not be displayed.

To maximize the visibility of your comments to the EPDP Team, please submit your comments via this form only. If you are unable to use this form, alternative arrangements can be made.

The final date of the public comment proceeding is 23:59 UTC on 21 December 2018. Any comments received after that date will not be reviewed / discussed by the EPDP Team.

Table of Contents

Page 1: Email Address, Important Instructions, Table of Contents

Page 2: Consent & Authorization

Page 3: Section 3, Part 1: Purposes for Processing Registration Data
- Recommendation #1

Page 4: Section 3, Part 1: Purposes for Processing Registration Data (Continued)
- Recommendations #23

Page 5: Section 3, Part 2: Required Data Processing Activities
- Recommendations #413

Page 6: Section 3, Part 3: Data Processing Terms, i.e., roles and responsibilities of parties
- Recommendation #14

Page 7: Section 3, Part 4: Updates to Other Consensus Policies
- Recommendations #1520

Page 8: Section 3, Other Recommendations
- Recommendations #2122

Page 9: Other Comments & Submission

Consent & Authorization

By submitting my personal data, I agree that my personal data will be processed in accordance with the ICANN Privacy Policy (https://www.icann.org/privacy/policy and agree to abide by the website Terms of Service (https://www.icann.org/privacy/tos).

2. Please provide your name: *
Steve DelBianco

3. Please provide your affiliation *

The ICANN Business Constituency

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

5. If yes, please explain:
The ICANN Business Constituency

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

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

● Support Purpose as written
○ Support Purpose intent with wording change
○ Significant change required: changing intent and wording
○ Purpose should be deleted

8. 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).

9. Please provide rationale for your recommendation.

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

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

○ Support Purpose as written

● Support Purpose intent with wording change

○ Significant change required: changing intent and wording

○ Purpose should be deleted

11. 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).

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 -- including law enforcement, security, intellectual property, and consumer protection needs -- to data elements collected for the other purposes identified herein.

12. Please provide rationale for your recommendation.

Purpose 2, as stated, is very general and non-specific. Legitimate third party interests are part of the fabric of security, stability and resiliency for the domain name system. Since the institution of the Temp Spec, the community has seen a degradation in its ability to investigate or address problems in the DNS -- a problem that can be remediated by access granted to these parties. It's important to enumerate the types of third parties that are warranted access for previously identified legitimate purposes.

Key findings of multiple studies have clearly demonstrated that lack of reasonable access is causing harm, and that contracted parties are either slow to respond to legitimate requests or do not respond at all:

- As noted by SSAC in SAC 101, while legal obligations are a reality and must be complied with, access to registration data under the Temp Spec has been diminished far further than legal obligations require, and further than is prudent for responsible stewardship of the namespace. This point is more true under the EPDP's proposals. The EPDP is obligated to consider the recommendations of SAC 101, and the requirements as listed by the GAC in its recent Communique's related to WHOIS. To date, it has not.
- According to the Anti-Phishing Working Group's study, cybercrime investigations have been seriously impeded, permitting harm to users, and Whois has become an unreliable or less meaningful source of threat intelligence.
- The Cybersecurity Tech Accord recently published its own study, detailing the fact that partial data in public Whois following redaction is insufficient to investigate or respond to incidents, and that requests for access for legitimate purposes are routinely refused.

Access for legitimate purposes is a pressing matter and increasing in urgency.

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

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

○ Support Purpose as written

● Support Purpose intent with wording change

○ Significant change required: changing intent and wording

○ Purpose should be deleted

14. 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

5. Please provide rationale for your recommendation.

Legal issues involving a domain name deserve a channel for communication to the registered name holder or agent; this is not enumerated in the current wording of the purpose, and particularly is not/should not be part of the "administrative" issues category. Legal communication can enable proper notice and/or due process in matters involving domain names, and those submitting such matters would benefit from specificity. The BC also recommends that the EPDP team further define "administrative" (a term that never has been fully defined in this context) as inclusive of matters such as rights infringement or resolution of claims of unlawful conduct. These clarifications will further assist third parties reporting contractual violations, who will be able to discern a "delegated agent" for administrative issues.

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

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

● Support Purpose as written

○ Support Purpose intent with wording change

○ Significant change required: changing intent and wording

○ Purpose should be deleted

17.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).

The BC supports this purpose and we believe that registrars should be required to allow registered name holders to provide technical contact information, as some would so elect, to facilitate communication regarding technical issues.

18.Please provide rationale for your recommendation.

The BC does not believe that collection of Technical Contact information should be mandatory. However, the OPTION to provide this information should be required since some registrants, particularly large corporate registrants, elect to provide this information in order to route appropriate communications within their organization.

The EPDP team has pursued policy recommendations that, in many areas, guarantee registrant rights. The BC therefore advocates for the same in this instance: to preserve this registrant right, registrars should be required to offer the non-mandatory option.

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

19.Choose your level of support of Purpose #5:

● Support Purpose as written

○ Support Purpose intent with wording change

○ Significant change required: changing intent and wording

○ Purpose should be deleted

20. 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).

21.Please provide the rationale for your recommendation.

The BC supports the purpose as written, on the assumption that ICANN is performing contractual compliance monitoring and audits under its remit. This clarifies ICANN Compliance's purpose for processing as detailed in the Summary of ICANN Org Contractual Compliance Data Processing Activities.

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

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

○ Support Purpose as written

● Support Purpose intent with wording change

○ Significant change required: changing intent and wording

○ Purpose should be deleted

23. 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 domain names, namely, the UDRP, URS, PDDRP, RRDRP, and future developed domain name registration-related dispute procedures in accordance with ICANN's Bylaws for which it is established that the processing of personal data is necessary.

24. Please provide rationale for your recommendation.

The language of the recommendation is problematic as it perpetuates the artificial distinction between the act of registration and the use of a domain name in the context of ICANN's general remit. It also is directly in conflict with the provisions of the UDRP and URS policies themselves.

Further, the language of the recommendation as currently written is not a full and accurate quotation from the ICANN Bylaws, which state, in pertinent part:

> The topics, issues, policies, procedures and principles referenced in Section 1.1(a)(i) with respect to gTLD [registrars/registries] are:…"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)…"

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

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

○ Support Purpose as written

● Support Purpose intent with wording change

○ Significant change required: changing intent and wording

○ Purpose should be deleted

26. 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).

Enabling registrars and registry operators to confirm that a registered name holder meets registration policy eligibility criteria required by the registry operator.

27. Please provide rationale for your recommendation.

The language is sharpened here to reflect the fact that at the time data is processed, the registered name holder is required to meet the registration eligibility established by the registry operator. It is not voluntary on the part of the registrant.

28. Enter additional comments to Recommendation #1.

The GDPR defines data controllers and data processors in Art. 4 as:

> *(7) '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;*
> *(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

Under the Registrar Accreditation Agreement between registrars and ICANN, ICANN determines the purposes and means of the processing of personal data, in some instances for the purpose of WHOIS, by mandating data collection, transfer, storage, and display through minimum contractual terms that registrars maintain in contracts with Registered Name Holders (the data subjects). While there may be other terms in these contracts with Registered Name Holders aimed at allowing registrars to maintain a customer relationship (process payments in exchange for domain names), where ICANN determines the purposes and means of the processing of personal data for, things like WHOIS or escrow, ICANN is clearly a controller and the registrar a processor for the control.

This does not exclude registrars as controllers of the same data where that data is collected for the registrar's purposes (e.g., maintaining a customer relationship with the Registered Name Holders). Indeed, the eco (Association of the Internet Industry) GDPR Domain Industry Playbook V. 1.0 at page 61 notes that:

> "The main purpose of any data processing operation in connection with domain registration is the provision of the services associated with domain registration within the scope of the contractual relation. However, the activity of the enterprise participating in domain registration cannot be reduced to this singular purpose. Rather, the registration of domains is a service, which - jointly with the services of

> other companies - guarantees the overall functionality of the Internet (namely conveying content available in the World Wide Web). **<u>The special roles of registrar and registry within this technical ecosystem is also reflected e.g. in the fact that they are subject to certain duties as operators of critical infrastructures. The activity of registry and registrar - in this light - also serves other purposes beyond the mere domain registration for customers, in particular also with regard to the functionality of the technical infrastructure as such. Registrar and registry therefore also have to a certain extent a regulatory function, which for example may include participation in the prosecution of legal infringements committed under usage of this ecosystem</u>.** Against this background we would consider processing of data for the purpose of maintaining security measures or technical analysis (also operated by third party providers) as likely (depending on the individual case) being justified under Art. 6 (1) lit. f) GDPR." (emphasis added)

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

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

1. A new purpose to address the needs and benefits provided by DNS security and stability research conducted through publication of reports on threats to the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS, and on the accuracy of WHOIS.
2. A new purpose to enable ICANN to conduct operations, facilitate activities, and implement consensus policies (adopted in accordance with the ICANN Bylaws) consistent with its mission of furthering the operational stability, reliability, global interoperability, resilience and openness of the DNS.

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

1. Research is a legitimate basis for processing, per GDPR Article 6(1)f, with specific safeguards defined in Article 89. It is also squarely within ICANN's mission and mandate, as the requirement for research derives from Section 1.2a (Commitments) of the ICANN bylaws:

(i) Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet;

(ii) Maintain the capacity and ability to coordinate the DNS at the overall level and work for the maintenance of a single, interoperable Internet;

This purpose exists to ensure that ICANN may continue to use registration data in support of its mission, whilst maintaining the privacy of data subjects through appropriate safeguards such as pseudonymisation. In addition, this purpose enables ICANN to continue to operate its Accuracy Reporting System (ARS), which publishes periodic reports on accuracy, using full WHOIS contact fields. The ARS is an important program approved by the ICANN Board in response to the recommendations from the first WHOIS Review Team.

2. Prior to May 25, and consistent with its mission and mandate under the Bylaws, ICANN used full WHOIS data as part of operational security-related activities via the Office of the CTO -- this included collaborating with public/private sector investigators, training law enforcement agencies in techniques for mitigating cybersecurity threats (such as CONFICKER), and working with a compliance related complaint. ICANN also used WHOIS as it implemented consensus policies involving the use of WHOIS data fields (for example, transfer policy processes or Thick WHOIS). It is important that ICANN retain the ability to provide these services in order to fulfill its role in safeguarding the DNS.

Section 3, Part 1: Purposes for Processing Registration Data
<u>Recommendation #2: Standardized Access</u>

Per the EPDP Team Charter, the EPDP Team is committed to considering a system for Standardized Access to nonpublic 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 nonpublic 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.

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

○ Support recommendation as written

● Support intent of recommendation with edits

○ Intent and wording of this recommendation requires amendment

○ Delete recommendation

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

The BC recommends that the final line of the recommendation should be edited to read:

“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, such as intellectual property rights holders, cybersecurity firms, organizations that mitigate DNS abuse, and law enforcement agencies.”

34. Please include the rationale for your answers here.

Now that the EPDP team’s gating questions have been sufficiently addressed, the BC strongly supports a recommendation that the EPDP Team contribute to ICANN Org’s development of a standardized, or “unified,” system for access to non-public registration data.

Thus, the BC proposes edits to this recommendation to ensure that the protection of intellectual property and other rights are expressly recognized as a legitimate interest under GDPR and therefore understood to be within scope of the final policy.

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 emphasized in a May 27 communication to ICANN, in which the European Data Protection Board reiterated its expectation that ICANN is "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."

35. Enter additional comments for Recommendation #2.

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.

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

○ Support recommendation as written Support

● Support intent of recommendation w/edits

○ Intent and wording of this recommendation requires amendment

○ Delete recommendation

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

The EPDP Team recommends that requirements related to the accuracy of registration data under the current ICANN contracts be incorporated into this policy.

38. Please include the rationale for your answers here.

According to Article 5 of the GDPR, 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." Within the GDPR, this is the second of three principles about data standards, along with data minimization and storage limitation that needs to be addressed.

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. 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."

Accordingly, It is the position of the BC that the accuracy requirements that currently exist under the contracts must be at a minimum maintained. These should be expanded to improve accuracy levels in light of the requirements under GDPR for accuracy, and especially in light of the unacceptably low levels of accuracy as reflected in ICANN's ARS reports.

The EPDP's work to align WHOIS with GDPR will be incomplete if it fails to recommend a policy to improve accuracy. The EPDP's policy should address accuracy from the following perspectives:

Collection: At intake, the EPDP should consider whether the current forms of validation are sufficient. In addition:

- The 2013 RAA contains requirements for cross-field validation that should be implemented as one component for demonstrating compliance with the GDPR.
- The EPDP policy should strive to improve accuracy consistent with GDPR, by revising the validation requirements specified under the RAA. For example, rather than having only one field in WHOIS validate (currently email OR phone number), the policy should consider requiring the validation of additional fields (as recommended by the EWG).
- The EPDP team should consider requiring additional forms of validation to examine accuracy of contact information from the perspective of syntactical and operational validity -- e.g., Syntax + Operability Accuracy methods (using the methodology of SSAC 058 found in the WHOIS Accuracy Reporting System (ARS). *Please note that this is NOT a request to conduct validation of the Identity of the registrant.*

Maintenance: Once data is collected, Article 5 of the GDPR says that data must be kept up to date, which seemingly requires some sort of process that to be developed, documented, and put into place. The process should be used to:

- identify specific records that need to be erased or rectified without delay;
- flag and place registrar hold on domain name registrations identified as having false or incorrect data (pending correction from the Registered Name Holder);
- ensure a registrar doesn't fall below certain statistical thresholds in terms of accuracy; and
- trigger an ICANN compliance inquiry where statistical thresholds for accuracy for any given registrar fall below certain levels. This should be considered for the registrars or registries that are well below the norm as reported by ICANN's ARS. ICANN compliance should have the tools to require these registrars to submit and implement a rectification plan to improve its accuracy levels.

Rectification: Article 5 of the GDPR says that ICANN and the contracted parties must ensure that personal data that are inaccurate … are erased or rectified without delay. Accordingly, a process should be developed, documented and put into place for a uniform method to report and rectify inaccurate data. This method should be published for the public, data subjects, and members of the community to have as a uniform method to report and rectify inaccurate data. In this regard, ICANN Compliance should be empowered to receive and act on complaints related to rectification of inaccurate WHOIS complaints, by creating a process specifically for this purpose.

39. Enter any other additional comments or observations you have on Section 3 Part 1 that are not covered by these questions.

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

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**
Registry Registrant ID**
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

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

Mark only one oval.

● Yes
○ No

42. If your answer is 'no', please enumerate which data elements should not be collected / generated.

43. Please provide the rationale for your answer.

These data elements are required by ICANN to fulfill its mission and are in line with ICANN's pursuit of a legitimate interest in this data, as well as the performance of the domain name registration contract, to which the data subject is party. Therefore, these data elements align to GDPR Article 6(1)b and 6(1)f.

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

Registrars should be required to provide the option for registered name holders to indicate whether they are Legal or Natural Persons.

45. Please provide the rationale for your answer.

GDPR does not apply to Legal Persons and, therefore, allowing registered name holders to indicate they are such Persons creates the opportunity and possibly the legal basis needed to publish the full Whois record or at least more fields therein.

According to Recital 14 of the GDPR:
The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings

established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

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

46. 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)?

Mark only one oval.

● Optional

○ Mandatory

47. Please provide the rationale for your answer.

As noted above, the BC does not believe that collection of Technical Contact information should be mandatory. However, the OPTION to provide this information should be required since some registrants, particularly large corporate registrants, elect to provide this information in order to route appropriate communications within their organization.

The EPDP team has pursued policy recommendations that, in many areas, guarantee registrant rights. The BC therefore advocates for the same in this instance: to preserve this registrant right, registrars should be required to offer the non-mandatory option. Further, should the registrant elect to enter this data, the registrar should be required to publish it.

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

● Yes

○

No

49. Please provide the rationale for your answer.

As noted, some registrants elect to provide this data for a variety of reasons. Registrars should thus be required to offer the option to those who wish to exercise it. This is a prudent step in the EPDP's various guarantees of registrant rights.

50. 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?

○ Yes
● No

51. Please provide the rationale for your answer.

Registrants have always been afforded the ability to enter different points of contact for different needs regarding the performance of their contract with the Registrar. This should continue. Further, ICANN's stated goal was, and is, to preserve Whois to the greatest extent possible -- presuming that to be the case, these fields should continue to be collected. Such a measure, as is the case elsewhere, is preservation of further registrant rights.

52. Enter additional comments for Recommendation #4 here.

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.

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

Mark only one oval. YES

● Yes
○ No

54. If your answer is 'no', please enumerate which data elements should not be transferred from the registrar to the registry.

55. Please provide the rationale for your answer.

All data should be transferred to the registry, including data for the .com,.net and .jobs TLDs, the only remaining "thin" registries. Thick Whois Policy development concluded, several years ago, that we should transition data from thin to thick for the remaining thin registries. GDPR should not affect the agreed upon policy. Data transfer from registrar to registry can be completed in a manner that is compliant with GDPR.

56. Enter additional comments for Recommendation #5 here.

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 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).

57. Choose your level of support of Recommendation #6:

○ Support recommendation as written Support

○ intent of recommendation with edits

● Intent and wording of this recommendation requires amendment

○ Delete recommendation

58. If your response requires an edit or deletion of Recommendation #6, please indicate the revised wording here. Additionally, please enumerate which data elements should not be transferred from the registrar/registry to the data escrow provider.

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 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 Registration Data contains the specifically identified data elements the EPDP Team recommends be transferred by Registries and Registrars to data escrow providers, along with the administrative contact, technical contact

and any specialized data required by the registry and collected by the Registrar. (see Annex D, Workbook)

59. Please provide the rationale for your answer.

The BC recommends transferring all registration data collected by Registries and Registrars to data escrow providers. This would include all administrative and technical fields provided by the registrant and any "special data" required by Registries.

60. Enter additional comments for Recommendation #6 here.

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 Internet users (see Annex D, Workbook 5).

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).

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

Mark only one oval.

○ Support recommendation as written

○ Support intent with edits

● Intent and wording of this recommendation requires amendment

○ Delete recommendation

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

Mark only one oval.

● Yes

○ No

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

64. Please provide the rationale for your answer.

The BC agrees that all the data elements listed in Workbook 5 should be transferred from the registrar/registry to ICANN. We further recommend that all registrant data collected by registrar/registry be transferred to ICANN

If a registrar/registry collects registrant data it should be transferred to ICANN to properly enable Compliance and other critical functions.

65. Enter additional comments for Recommendation #7 here.

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
Domain Name
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

Registrant Fields
- State/province
- Country
- Anonymized email / link to web form

Tech Fields
- Anonymized email / link to web form

NameServer(s)
DNSSEC No
Name Server IP Address
Last Update of Whois Database

REDACTED
Registrant Fields
- Name

- Street
- City
- Postal code
- Phone
- Email

Tech Fields
- Name
- Phone
- Email

UNDECIDED (REDACTED/ NOT REDACTED)
- Organization (opt.)

Please reference page 1415 of the Initial Report for details of the data elements.

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

○ Yes

● No

67. If your answer is 'no', please enumerate the data elements that should not be redacted.
No. Registrant Email and City should <u>not</u> be redacted

68. Please provide the rationale for your answer.

Because time often is of the essence during security and law enforcement investigations, there must be an immediate method for contacting domain registrants that is more precise and affirmative than a web form or anonymous link. Unfortunately, experience with registrars following implementation of the Temp Spec (and further previous experience with Privacy/Proxy services) confirms that responsiveness to reveal requests is slow and unpredictable at best and entirely absent at worst. Email addresses, especially for Legal Persons, do not have to reveal personal data. The BC believes that, in order to serve the investigatory needs of law enforcement, security authorities and brand protection interests, registrars should, at a minimum, provide a uniquely hashed email string.

In addition, the EPDP Charter (Part 1(f)) relates to publication of data. Registrars should give registrants the option to opt in to having their WHOIS Contact Data published rather than be redacted. The Temporary Specification 7.2.1/ Appendix C – Section 2.3 contains this requirement:

As soon as commercially reasonable, Registrar MUST provide the opportunity for the Registered Name Holder to provide its Consent to publish the additional contact information outlined in Section 2.3 of Appendix A for the Registered Name Holder.

Legal entity registrants such as corporations should not have any WHOIS data redacted.

Natural person registrants may wish to display their information to ensure that their customers can confirm the authenticity of their website and prevent phishing and other

impersonations. Domain owners may wish to be easily contactable in order to solicit interest in secondary market sales of their domain names. Enabling the consent feature is consistent with the accountability principles laid out in GDPR.

69. 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?

Mark only one oval.

○ Yes

● No

70. Please provide rationale for your answer above.

No. An Organization by definition refers to a Legal Person, and Legal Persons are exempt under GDPR and most other national privacy laws. No registrant data collected for a Legal Person should be redacted. The Registrant Organization field is included in the Temp Spec, as it should be, and it is the duty of parties to demonstrate that it should be redacted, not the reverse. (This was established in the email of Nov 19 in which ICANN responded to this very question by confirming the legal standing of Registrant Organizations under Article 6(1)(f).)

71. Enter additional comments for Recommendation #8.

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).

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

Mark only one oval.

● Support recommendation as written

○ Support intent of recommendation with edits

○ Intent and wording of this recommendation requires amendment

○ Delete recommendation

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

74. Please provide the rationale for your answer.

The Business Constituency agrees with the language of this recommendation. Registrars should be required to inform registrants of the significance of providing an organization name and the fact that this information will be publicly displayed in a registrant data directory service.

75. 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.

76. Choose your level of support of Recommendation #10:
Mark only one oval.

○ Support recommendation as written Support

○ intent of recommendation with edits

○ X Intent and wording of this recommendation requires

○ amendment Delete recommendation

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

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 and MUST provide the email address of registered name holders who are legal persons.

The email address MUST be unique and uniform for each domain name registration attributed to a Registrant at a given Registrar.

The email address MUST functionally forward communication received to the email address of the applicable contact and MUST describe the methods used to forward a communication and confirm its receipt.

Registrar MAY implement commercially reasonable safeguards to prevent spam and other forms of abusive communications.

It MUST NOT be feasible to extract or derive the email address of the contact from the email address provided to facilitate email communication with the relevant contact.

78. Please provide the rationale for your answer.

At minimum, the community must implement an effective and standardized method for replacing the email address with a pseudonymized email. Such a pseudonymized email would redact personally identifiable information by providing a unique, registrant-specific replacement address. This policy, in the context of the balancing exercise under 6(1)(f) GDPR, would grant reasonable latitude to legitimate third party interests and provide a reliable method of contact that would further allow for indexing such a contact to multiple domain names registered to the same person or entity. (Please refer to Opinion 06/2014 regarding the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC of the Article 29 Working Party (now the European Data Protection Board), pp. 42-43.)

79. Additional comments for Recommendation #10.

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").

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

Mark only one oval.

○ Support recommendation as written

● Support intent with edits

○ Intent and wording of this recommendation requires amendment

○ Delete recommendation

81. If you do not support Recommendation #11, please provide proposed edits here.

The EPDP Team recommends that Registrars are required to retain the herein specified data elements for a period of three years following the life of the registration.

82. Please provide the rationale for your answer.

ICANN itself recommends a longer period of two years. Cybersecurity incidents have dwell time that can endure for years, as the recent Marriott/Starwood breach news proves. Attack indicators can be discovered long after the attack itself, and after DNS resources are deleted. Investigation timelines, particularly when it involves law enforcement, can be lengthy.

It's important that information about previously registered domains is retained for a useful period for security and law enforcement needs -- one year simply is insufficient. The consistent utilization, by security and LEA personnel, of historic data from various third party Whois services is testament to the need.

83. Additional comments for Recommendation #11.

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

84. 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.

The new policy should differentiate between registrants for which GDPR applies and registrants outside the jurisdictional reach of GDPR. In addition, the EPDP should consider a policy recommendation to explore whether it is possible for ICANN to create a “rules engine” or dynamic chart that determines how the various privacy laws that exist or will exist in the future apply to WHOIS. Recognizing the complexity of this analysis, this policy recommendation could be implemented on a timeline different from other policies emerging from the EPDP. For example, based on the EDPB’s recent guidance, the dynamic chart could determine that the new WHOIS redactions implemented for GDPR apply to specific situations, such as where the contracted party is targeting domain registration services to the EU.

Recently, the EPDP provided guidance on this issue in its Guidelines 3/2018 on the Territorial Scope of the GDPR. These Guidelines address the factors mentioned above and confirm that it should be feasible to distinguish between registrants on a geographic basis for the purposes of determining whether the GDPR should be applied. Redactions to the data of registrants for the purposes of compliance with the GDPR should be applied only where: (a) the contracted party is collecting such data within the context of an establishment of the contracted party in an EU member state, or (b) the contracted party is targeting domain registration services to EU data subjects.

85. Please provide the rationale for your above answer.

The BC is concerned that the EPDP’s proposed policies significantly reduce the utility of WHOIS through the over-redaction of data due to interpretations that, in the end, are not applicable to GDPR. Making a geographic distinction is consistent with ICANN’s stated goal of preserving the WHOIS system to the greatest extent possible while complying with GDPR. ICANN (and its policies) should not serve as a means to achieve global application of a law that has limited territorial application. To do so adversely affects the ability of those that use WHOIS as a practical tool for easily resolving issues that protect consumers, mitigating security threats, and protecting its intellectual property without having resort to legal action.

86. 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.

ICANN risks the adoption of onerous regulations to counter the unnecessarily broad application of GDPR.

87. What other factors should the EPDP team consider about whether Contracted Parties should be permitted or required to differentiate between natural and legal persons?

The team should revisit Recital 14 of the GDPR: Protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data, which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

A registrar should distinguish between natural and legal persons when accepting registrant data for a domain name registration. Legal person data should not be treated as a natural person's data since the GDPR does not apply.

88. Please provide the rationale for your above answer.

As the BC has stated above, legal persons' data should be publicly accessible. A registrar or registry should make the distinction between natural and legal persons in their processes and keep the data separate from natural persons' data so as not to confuse the treatment of legal persons' data.

89. Should there be further study as to whether 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.

90. 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.

Many ccTLD registries differentiate between natural and legal persons in the registration process. The extensive list below demonstrates that this differentiation is both practical and workable:

.AT: Legal person data is publicly available in the whois and provides the organization, Street address, postal code, city, country, phone, email, and NIC handle.

.BE: Legal person data is publicly available in Whois and provides the organization, language, street address, city, country and phone. A contact form is available.

.CZ: Legal person data is publicly available in Whois and provides registrant organization, street address, city, country and NIC handle. It also provides the same data fields for admin and tech contacts.

.DK: Natural and legal person data is treated identically in the publicly available whois and provides registrant organization, street address, city, country and nic-handle. (See .dk statement - https://www.dk-hostmaster.dk/en/gdpr)

.ES: Legal person data is publicly available in Whois and provides registrant organization, admin contact name and name of technical contact.

.EU: This ccTLD differentiates in the publicly available Whois record and provides the registrant name, language, city, country and email address.

.FI: Legal person data is publicly available in the Whois and provides the registrant name, street address, city, country and phone. The technical contact's name and email address are available.

.FR: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country, phone and email address; the technical contact's name, registrant org, street address, city, country, phone and email address; and the admin contact's, name, registrant org, street address, city, country, phone and email address.

.IE: Legal person data is publicly available in Whois and provides the registrant organization, admin and tech NIC handles.

.IT: Legal person data is publicly available in Whois and the registrant organization, street address, city, country postal code, phone number and email address. The same data fields are available for admin and tech contacts and include individual names.

.LT: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code, phone number and email address. The same data fields are available for tech contact.

.LV: This ccTLD distinguishes between natural and legal persons. Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code, phone number and email address. The same data fields are available for admin and tech contact and includes individual names.

.LU: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country and postal code. The admin and tech contacts are masked.

.MT: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code, phone number and email address. The same data fields are available for admin and tech contact.

.NL: Legal person data is publicly available in Whois and provides the registrant organization and admin email address.

.PL: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code. Organization is indicated in the record.

.PT: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country and postal code. The same data fields are available for the managing body role.

.SI: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code, phone number and email address. The tech contact's email address also is provided.

.SE: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code, phone number and Contact ID. The same data fields are available for admin and tech contacts and includes individual names.

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 NonPublic 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:

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

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

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

Mark only one oval.

Support recommendation as written Support

intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

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

The Business Constituency 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:”

93. Please provide the rationale for your answer.

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

According to a survey conducted by INTA, the redaction of registrant data has made enforcement of intellectual property rights more difficult. Data recently published by MarkMonitor, a leading brand protection company, revealed that nearly 80% of the disclosure 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.

94. Additional comments for Recommendation #12.

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.

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

Mark only one oval.

Support recommendation as written Support

intent with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

96. If you believe changes are needed for Recommendation #13, please provide proposed edits here.

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 either a Joint Controller Agreement or Controller-Processor agreement with the Contracted Parties.

97. Please provide the rationale for your answer.

The BC supports any controller/processor arrangement that will enable ICANN to assume sufficient legal responsibility such that ICANN can compel contracted parties to respond to Whois queries from accredited requestors, most likely as part of a Unified Access Model.

98. Additional comments for Recommendation #13.

99. Enter any other additional comments or observations you have on Section 3, Part 2 that are not covered by these questions.

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.

101. Choose your level of support of Recommendation #14:
Mark only one oval.

Support recommendation as written

Support intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

102. If you do not agree with the enumerated data processing activities and responsible parties, please provide proposed edits, including specific processing activities that need to be added/deleted here. The EPDP team particularly seeks feedback with the assignment of roles such as: "jointcontroller," "controller," and "processor.

Specifics in the tables beginning on p. 63 would benefit from further clarification. In particular, on p. 66, under "disclosure," no party is listed in the context of facilitating DRPs (like the UDRP). But disclosure generally occurs upon the filing of a "Doe" or privacy/proxy complaint, where the registrar provides the underlying contact details to the dispute resolution provider (DRP) and the DRP then discloses them to the complainant, who can then file an amended complaint with the updated registrant information. The BC therefore suggests listing Registrar and DRP as responsible parties for disclosure for this purpose, with 6(1)(f) as the lawful basis.

Similarly, for "data retention" in the same table, the DRP can be listed as the "responsible party" -- even where the underlying registration data may no longer be retained at the ICANN/registry/registrar levels, dispute resolution determinations and underlying materials containing the initially disclosed registration data would likely be considered retention of the data. Again, the lawful basis for data retention would be 6(1)(f). In the context of this purpose, both registrar and DRP should be considered as "processors" with ICANN being a controller given that the dispute resolution mechanisms are implemented pursuant to ICANN policies.

The BC also calls the team's attention to footnotes 48-51, where we cite instances where 6(1)(b) is a better lawful basis.

103. Please provide your rationale for the proposed addition/deletion.

104. Additional comments for Recommendation #14.

Section 3, Part 4: Updates to Other Consensus Policies

106. Enter any general comments or observations you may have on the findings in Section 3, Part 4.

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).

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

Mark only one oval.

Support recommendation as written

Support intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

108. If you do not agree that the current updated requirements in the UDRP and URS, as provided in the Temporary Specification should remain in place, please provide proposed edits to the current requirements.

The EPDP Team recommends that for the new policy on gTLD registration data, the requirements of the Temporary Specification (Appendix E) are modified to allow for an unlimited number of domain names to be included in one URS or UDRP filing when there is a good faith belief that the registrants are acting in bad faith and there is a demonstrable connection between the registrants.

When the domain name registration information is received by the complainant the URS or UDRP filing could be amended to remove registrants where no connection was found. Until such time as these are superseded by recommendations from the RPMs PDP WG (if any).

109. Please provide the rationale, keeping in mind compliance with GDPR.

The restriction of information has made it difficult to make a filing with a dispute resolution provider. Access to data prior to filing is much more efficient and helpful.

In general, the UDRP has become more onerous, because all complaints must now be filed as “Doe” complaints but are limited in the number of Doe’s that can be included, and then later amended once sufficient registration data is disclosed to the complainant. Each filing costs the complainant up to $10,000 USD. This includes identifying and adding additional facts and evidence of bad faith, once new information about the registrant’s identity is available. It is still generally more challenging to put forward a complete case, as reverse WHOIS capabilities are severely limited, making evidence of broader schemes or portfolios of abusive domains harder to demonstrate.

Allowing an unlimited number of domain names to be named in one complaint in which there is similar bad faith and other factors that appear to connect the registrants would lessen the burden of that limited access to registrant data has imposed.

It would be exceedingly useful if, as part of a UDRP or URS filing, registries or registrars could provide a list of all domains registered to that same respondent as part of the registrant information disclosure process, to solve the reverse WHOIS problem. This would not disclose any more personal data than has already been disclosed about the registrant; however, it could present other challenges – we suggest this approach be further considered within the EPDP and/or the RPM Review PDP. Otherwise, the requirements in the Temporary Specification regarding the URS and UDRP are acceptable from a practical standpoint, and we have no strong opposition to this recommendation.

110. Additional comments for Recommendation #15.

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.

111. Choose your level of support of Recommendation #16:

Support recommendation as written Support

intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

112. If you do not support Recommendation #16, please provide proposed text/edits.

113. Please provide the rationale for your answer.

The BC echoes its comment as elucidated in the answer to question 108 above. According to the recommendation as currently written, at the time of filing, only publicly available registration data would be able to be used, which would result in a substantially blank filing document. In order to make more impactful and efficient use of dispute resolution procedures, and to confirm infringement, it would be far better to have pre-filing access to the data.

This is already happening in practice, and is at least somewhat similar to what has happened historically in UDRP or URS cases involving privacy/proxy registrants. However, it would be beneficial to formalize this process in UDRP and URS proceedings through the relevant policies, rules, and supplemental rules. The issue currently has the attention of the RPM Review PDP.

Therefore, the Temporary Specification should be modified to allow investigation of a limited number of registrants prior to filing a URS or UDRP when there is a good faith belief that the registrants are acting in bad faith and there is an demonstrable connection between the registrants.

114. Provide additional comments for Recommendation #16 here.

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.

115. Choose your level of support of Recommendation #17:

Support recommendation as written

Support intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

116. If you do not support Recommendation #17, please provide proposed edits or changes.

The EPDP Team should now commence its deliberations on a standardized access framework, since the "gating questions" have been answered.

Further, the EPDP team requests that 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, and that a representative of URS and UDRP providers also provide input on the use of data in conducting resolutions.

117. Please provide the rationale for your answer.

While the BC supports the concept of a representative of the RMPs PDP WG providing such an update, we reiterate here that the gating questions have been substantially answered and deliberations should commence on standardized access. We also recommend that a representative of a UDRP and URS dispute resolution provider be available to the team in order to give perspective on the use of data in conducting resolutions.

118. Provide additional comments for Recommendation #17 here.

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.

119. Choose your level of support of Recommendation #18:

Support recommendation as written Support

intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

120. If you do not agree to Recommendation #18, please provide proposed edits or changes here.

The EPDP Team recommends that ICANN Org enter into data processing agreements with all relevant service providers (such as the Trademark Clearinghouse provider) , including dispute resolution providers. Within such agreements, the data retention period should be specifically addressed, as this will affect the ability to make decisions publicly available.

121. Please provide the rationale for your answer here.

The BC believes agreements should so exist with all relevant service providers (such as the Trademark Clearinghouse provider), and not only the dispute resolution providers.

122. Provide additional comments for Recommendation #18 here.

Question #4 for Community Input

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

The BC points out that the UDRP Section 4.a distinguishes between an *assertion* that the three elements are met, and the *administrative proceeding* where the complainant must prove the asserted elements. The assertion required under UDRP Section 4.a is:

> (i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and
>
> (ii) you have no rights or legitimate interests in respect of the domain name; and
>
> (iii) your domain name has been registered and is being used in bad faith.

We encourage the team to consider policymaking to clarify that disclosure of non-public WHOIS data can be made in the period between assertion and the administrative proceeding, and to explore controls that could be included in the policy to prevent abuse of such an investigative tool.

124. 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. By building smart policy around the procedural distinction between assertion and proceeding, the EPDP Team could easily fix this broken part of the 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.

125. Choose your level of support of Recommendation #19:

Support recommendation as written Support

intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

126. If you do not support Recommendation #19, please provide proposed changes/edits here.

127. Please provide the rationale for your answer, keeping in mind compliance with GDPR.

128. Provide additional comments for Recommendation #19 here.

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.

129. Choose your level of support of Recommendation #20:

Support recommendation as written

Support intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

130. If you do not support Recommendation #20, please provide proposed edits/changes here.

131. Please provide the rationale for your answer here.

132. Provide additional comments for Recommendation #20 here.

It is feasible to support consent for disclosure of various data elements both at an account level and at an individual registration level, depending on the desired feature set of the registrar.

This consent mechanism should be applicable to transfer policy for registration data as well.

Implementation is feasible via Extensible Provisioning Protocol (EPP) – see RFC 5733, section 2.9.

Contact objects have a <contact:disclose> element which signals disclosure preferences for each data element that are "exceptional" (i.e. which differ from the EPP server's default policy): if the server's policy is "disclose by default" then they opt those elements out of display; but if the server's policy is "hide by default" then they opt the elements into

display.

The only data elements that cannot be opted in/out are the contact ID and ROID, since they are not among the elements that the XML schema permits to be included in the <contact:disclose> element.

The data escrow specification (for registry data) incorporates the XML schema from RFC 5733, and therefore registries *should* include <contact:disclose> elements for contact objects in their deposits. Also, escrow deposit import tools process <contact:disclose> elements in deposits when importing them into a database as the result of a transfer.

At this time, the contact disclosure element is an OPTIONAL feature and thus is used inconsistently by registrars, and the format used by registrars for their data escrow does not include disclosure preferences at all. But since the existing protocols already support these features, these implementation details can be easily addressed.

Question #5 for Community Input

133. Are there any changes that the EPDP Team should consider in relation to the Transfer Policy that have not already been identified? If so, please provide the relevant rationale, keeping in mind compliance with the GDPR.

134. Enter any other additional comments or observations you have on Section 3, Part 3 that are not covered by these questions.

Section 3: Other Recommendations

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

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.

137. Choose your level of support of Recommendation #21:

Support recommendation as written

Support intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

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

139. Please provide the rationale for your answer here, keeping in mind compliance with GDPR.

The BC supports any controller/processor arrangement that will enable ICANN to assume sufficient legal responsibility such that ICANN can compel contracted parties to respond to Whois queries from accredited requestors, most likely as part of a Unified Access Model.

140. 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.

141. Choose your level of support of Recommendation #22:

Support recommendation as written

Support intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

142. If you do not support Recommendation #22, please provide proposed edits or changes here.

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:

- 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
- Privacy & Proxy Services Accreditation Issues (PPSAI) Policy [added]

  Additional WHOIS Information Policy, governing insertion of EPP status codes [added]
  Expired Registration Recovery policy [added]

143. Please provide the rationale for your answer here.

The BC supports an edited version of this recommendation, provided the data is replaced with that of an appropriate contact. Note that the BC also recommends adding the PPSAI policy to this list. PPSAI is in implementation phase, since it has been adopted as ICANN Consensus Policy, and Implementation should be resumed immediately.

144. Provide additional comments on Recommendation #22 here.

In the case of a domain name registration where a privacy/proxy service used (e.g. where data associated with a natural person is masked), Registrar MUST return in response to any query full WHOIS data, including the existing proxy/proxy pseudonymized email.

145. Enter any other additional comments or observations you have on Section 3: Other Recommendations that are not covered by these questions.

Other Comments & Submission

147. 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.

This EPDP WG -- like all working groups -- is obligated to work toward consensus. Regrettably, there has been a reluctance to consider the positions other than those of the contracted parties and the NCSG, or to include the other SOs/ACs and constituencies in consensus development. It should be pointed out that "consensus" in this scenario must include the vote of **all** SOs and ACs that have been participating, not just the constituencies of the GNSO.

Lack of access to non-public Whois data is contributing to difficulties that worsen by the day. The BC has trusted that the question of access will be addressed by ICANN. Without doing so, the new policy will fail and ICANN's legitimacy will be challenged. The BC believes the "gating" questions have been sufficiently addressed and the time is right to open the discussion on access to non-public Whois by properly accredited requestors.

In conclusion, the BC offers this observation about how ICANN Org, Board, and Community have responded to GDPR.

> ICANN's mission is to "ensure the stable and secure operation of the Internet's unique identifier systems". This EPDP is by definition an ICANN policy process, aligned exclusively and directly to this mission. And yet it will be clear to anyone following the EPDP that stability and security of the DNS is absent from most of the EPDP discourse. Worse, it is being willfully pushed aside in pursuit of other objectives.
>
> Instead, the results of this Interim Report reflect an unbalanced EPDP team where control of data seemingly begets policy authority, where technical limitations instruct policy outcomes, where pursuit of complete online anonymity is championed, and where self-administered risk-profiling of contracted parties is used to justify positioning.
>
> The GDPR clearly does not protect Legal Persons, yet there exists no willingness to account for this in the EPDP.
>
> The Registrant Organization field is legally valid to collect and display, yet efforts are underway to remove it despite the clear legal justification provided in a written response by ICANN in November.
>
> Whois data is clearly needed for ICANN to properly enforce compliance to the RAA, yet those same RAA contracted parties are deciding whether this data is made available to ICANN. That is the definition of moral hazard.
>
> Some individuals on the EPDP somehow claim to speak for internet citizens, and yet they dismiss the right of Registrants to retain the time-honored ability to publish their information in Whois.
>
> Security is enabled, in part, through transparency. In this EPDP, ICANN Org has has impaired its own ability to pursue the mission outlined in its bylaws. We strongly encourage ICANN Org and Board to evaluate the "progress" of this EPDP in the context of its mission and bylaws, and regain its footing lest it leave the security and stability of DNS to empowered individuals and organizations for whom this mission is seemingly last on their list of policy goals and priorities.
>
> Goran Marby repeatedly stated that ICANN wants "to retain Whois to the greatest extent possible." We encourage ICANN Org and Board to follow through on that sentiment and hold themselves accountable to those words.