Intellectual Property Constituency (IPC)

Comments on the Expedited PDP (EPDP) Initial Report

Submitted on 21 December 2018

EPDP On the Temporary Specification for gTLD Registration Data - Public Comment Proceeding Input Form

* Required

# 1 Email address: ***redacted***

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 multi-part 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").

You can easily navigate from page to page in the form. There is a table of contents below so that you can "fast forward" to the desired section by hitting "next" at the bottom of each page. To preview this entire form in Word format, see, [LINK TBD]

To stop and save your work for later, you MUST (to avoid losing your work):

1. Provide your email address above in order to receive a copy of your submitted responses;

2. Click "Submit" at the end of the Google Form (the last question on every page allows you to quickly jump to the end of the Google Form to submit);

3. After you click "Submit," you will receive an email to the above-provided email address; within the email,

click the "Edit Response" button at top of the email;

4. After you click the "Edit Response" button, you will be directed to the Google Form to return and complete;

5. Repeat the above steps 2-4 every time you wish to quit the form and save your progress.

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

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: *

Brian King

3 Please provide your affiliation *

IPC

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

Mark only one oval. (Please note you can highlight your choice.)

● Yes

○ No

5 If yes, please explain:

This is the official comment of the IPC.

Save Your Progress

6 Do you want to save your progress and quit for now? You will be able to return to the form to complete at a later time.

Mark only one oval.

○ **Yes** *Stop filling out this form.*

○ No, I would like to continue to the next section

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:

Mark only one oval.

○ 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).

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

(IV) TO ESTABLISH THE RIGHTS AND OBLIGATIONS, SUCH AS THEY MAY BE,, such as they may be, OF A REGISTERED NAME HOLDER IN A REGISTERED NAME;

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

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

9 Please provide rationale for your recommendation.

The collection of data from the domain name registrant serves not only the purpose of establishing rights of the registrant in a registered name, but also for establishing obligations. This includes the obligation for the registrant to comply with the various terms and conditions established in the contract between the registrar and the registrant. Rights and obligations go hand-in-hand, and therefore the purpose of obtaining the data from the registrant to establish the rights in the name cannot be separated from the purpose of obtaining the data to fulfill the obligations that go along with domain name ownership. Article 6(1)(b) of the GDPR establishes the legality of collecting and processing personal data "for the performance of a contract to which the data subject is party . . . ." The performance of any contract involves OBLIGATIONS in addition to rights. Therefore, adding the language suggested concerning obligations makes this proposed purpose more compliant with the GDPR.

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:

Mark only one oval.

○ 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).

ENSURING THE SECURITY, STABILITY, AND RESILIENCY OF THE DOMAIN NAME SYSTEM IN ACCORDANCE WITH ICANN'S MISSION, COMMITMENTS AND CORE VALUES THROUGH THE ENABLING OF LAWFUL ACCESS FOR LEGITIMATE THIRD--PARTY INTERESTS OF LAW ENFORCEMENT, CYBERSECURITY, COMBATTING DOMAIN NAME SYSTEM ABUSE, CONSUMER PROTECTION AND INTELLECTUAL PROPERTY RIGHTS PROTECTION TO DATA ELEMENTS COLLECTED FOR THE OTHER PURPOSES IDENTIFIED HEREIN

12 Please provide rationale for your recommendation.

Although we do not object in principle to the Purpose 2 statement, the IPC hopes to clarify that the purpose includes as a component the recognition of protection of intellectual property rights (as the universally, legally defined recognized rights of:

trademark, copyright and patent) and by extension consumer protection and consumer trust within the meaning of "maintaining the security, stability, and resiliency of the Domain Name System in accordance with ICANN's Mission" particularly given that part of ICANN's Mission includes: "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); … reservation of registered names in a TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual property…."

Accordingly, assuming this is the case, we hope to confirm that "lawful access for legitimate third-party interests" as used in this purpose statement includes the implicit recognition that intellectual property enforcement related investigations and actual enforcement measures conducted by intellectual property owners and their agents would therefore be considered "legitimate third-party interests" and thus permitted "lawful access" to the requisite data elements collected for other purposes as outlined elsewhere in the Initial Report. Note that while we suggest the addition of "Commitments and Core Values" to the purpose statement, these additions may not be necessary if the above can otherwise be clarified and confirmed.

In addition, Article 13(1) of the GDPR states

> *"Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*
>
> *. . .*
>
> *(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
>
> *(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;" (emphasis added)*

The current list of purposes would benefit by greater specificity as embodied in the proposed new purpose. ICANN's purposes with respect to WHOIS data and registry directory services include, according to ICANN'S Bylaws "whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust, security, stability and resiliency, malicious abuse issues, sovereignty concerns and rights protection." (ICANN Bylaws Section 4.6). Purpose #2 from the Initial Report only addresses "security, stability and resiliency" and does not address the other ICANN purposes and concerns as articulated in Section 4.6 of the Bylaws.

Article 13(1) of the GDPR requires that at the time personal data are collected, data subjects be given information about both the purposes for the processing and legal basis for the processing AND the legitimate interest pursed by the controller or by a third party. The proposed new purpose seeks to address both of these requirements by enumerating more specific purposes as well as identifying the legitimate interests of

ICANN (as a joint controller) and as pursued by third parties that may seek access to the personal data.

In its letter of 11 April 2018, to Goran Marby, the Article 29 Data Protection Working Party stated that "purposes specified by the controller must be detailed enough to determine what kind of processing is and is not included . . . ." The letter also stated that the WP29 "stresses the importance of explicitly defining legitimate purposes in a way which comports with the requirements of the GDPR." The new proposed Purpose seeks to do just that.

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:

Mark only one oval.

○ 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

15 Please provide rationale for your recommendation.

The proposed wording change is intended as a mere clarification that communication should be enabled for legal issues involving a domain name, to the extent legal issues are not specifically within the "administrative" issues category. Enabling communication for legal issues is aimed at ensuring proper notice and due process where a domain name might implicate certain legal matters. Alternatively, "administrative issues" should be defined to include resolving claims that a domain name is being used to facilitate unlawful conduct, or to infringe on the legitimate rights of others. Under pre-GDPR Whois, third parties often addressed complaints regarding these issues to the administrative contact (a label that ICANN has never defined). Additionally, these uses are already forbidden under the RAA and/or registry agreements. In cases when third parties address their complaints of violations of the RAA to the registrar (or of RA to the registry), these contracted parties need to know who is the “delegated agent for administrative issues” such as these.

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:

Mark only one oval.

● 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).

18 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

19 Choose your level of support of Purpose #5:

Mark only one oval.

● 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.

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:

Mark only one oval.

○ 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 THE REGISTRATION OF DOMAIN NAMES (AS OPPOSED TO THE USE OF SUCH DOMAIN NAMES, BUT INCLUDING WHERE SUCH POLICIES TAKE INTO ACCOUNT USE OF THE DOMAIN NAMES), NAMELY, THE UDRP, URS, PDDRP, RRDRP, AND 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.

24 Please provide rationale for your recommendation.

The distinction between “registration” and “use” is inconsistent with the intent and substance of existing procedures for resolution of domain name disputes, including specifically the procedures which are mentioned in the purpose statement itself. For example, to prevail in a domain name dispute under the UDRP, the complainant must prove that the disputed domain name "has been registered *and is being used* in bad faith. Limiting this purpose to disputes related to registration and specifically excluding “use” would result in a purpose which is narrower than the policies to which it refers. Furthermore, it may be possible that in future, further policies are defined which similarly refer to “use” within the context of ICANN’s mission and mandate. The proposed language appears to draw a distinction that flows from a specific view about the scope of ICANN’s mandate, and in doing so, falls outside the mandate of the EPDP. It would be inappropriate to attempt to narrow the implementation of existing policies for resolution of domain name disputes by drawing an artificial line through such policies based on the “use” versus “registration” distinction. The correct forum for that debate is in the context of such policies themselves, not here. The scope of such policies should be the guide for definition of this purpose, and the recommendation should be neutral in relation to that scope, unless there is a compelling reason based in compliance with privacy laws - which is absent here.

This purpose must include resolution of disputes pertaining to uses of domain names, because this falls within the mission of ICANN in connection with security, stability, and resiliency of the DNS, and as expressly stated in Annexes G-1 and G-2 of the ICANN Bylaws. The first proposed addition to the purpose statement quotes verbatim the language from the Bylaws. Indeed, domain names can be used to perpetrate threats to SSR, including through leveraging of IP assets to harm consumers/Internet users, and this must be taken into account in this purpose statement. While ICANN is not directly responsible for online content (per Bylaws, art. 1.1(c)), access to registration data to address content-related issues must still be a valid purpose for processing registration data, within the broader SSR related component of ICANN’s mission, as expressed in purpose #2, and in connection with the purpose of facilitating communication with registered name holders to resolve technical, legal, and/or administrative issues per the proposed amended version of the purpose #3.

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:

Mark only one oval.

● 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).

27 Please provide rationale for your recommendation.

28 Enter additional comments to Recommendation #1.

We are concerned that the list of purposes is neither sufficiently complete, nor sufficiently detailed. We have attempted to address these concerns by suggesting edits to some of the recommended 7 purposes as well as suggesting additional purposes below.

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.

The IPC supports the addition of purposes related to research - covering research performed by ICANN Org (as currently described in "Purpose O") but extending to any ICANN group also research performed by relevant and legitimate 3rd parties.

1. [Current Purpose O] - "Research and publish reports on threats to the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS."

The IPC believes this purpose should encompass and enable all ICANN groups and divisions (OCTO, GDD, Compliance) to conduct operations, facilitation 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.

2. ENABLE [RELEVANT AND LEGITIMATE 3RD PARTY] RESEARCH OF DNS ABUSE AND THE SECURITY, STABILITY AND RESILIENCY OF THE DOMAIN NAME SYSTEM

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 5(1)(e) and 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 1st WHOIS Review Team.

2. Research conducted by relevant and legitimate third parties with respect to DNS

Abuse and the security, stability and resiliency of the Domain Name System is a fundamental and legitimate purpose consistent with ICANN's Bylaws and critical for ICANN to fulfill its mission. Since such research can and often does involve analysis of data associated with Registered Name Holders, this purpose is directly related to the collection and processing of such data.

Save Your Progress

31 Do you want to save your progress and quit for now? You will be able to return to the form to complete at a later time.

Mark only one oval.

○ **Yes** *Stop filling out this form.*

○ No, I wish to continue to the next section

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.

32 Choose your level of support of Recommendation #2:

Mark only one oval.

○ 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 IPC 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 accessing registrant data including intellectual property rights holders, cybersecurity firms, organizations that mitigate DNS abuse, and law enforcement agencies."

Per the EPDP Team Charter, EPDP Team is committed to answering the additional gating questions in the charter and recommending a system for Standardized Access to nonPublic Registration Data no later than submission of its Final Report. In this context, amongst others, disclosure in the course of intellectual property infringement and DNS abuse cases will be considered.

34 Please include the rationale for your answers here.

The charter calls for the EPDP team to deliver an Initial Report outlining a proposed model of a system for providing accredited access to non-public Registration Data, not to "consider" doing so. The EPDP fails to fulfill its charter if it does not deliver a model for a system for standardized access to non-public data. At a bare minimum the team should commit to a time certain to complete this work, and no consensus policy superseding the Temporary Specification should be adopted without it.

The IPC 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.

The IPC proposes edits to this recommendation to reflect 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.

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, the IPC recommends the edits provided above.

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:

Mark only one oval.

○ Support recommendation as written Support

○ intent of recommendation with 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 no consensus policy adopted to address registration data interfere with accuracy requirements under current ICANN contracts and consensus policies nor interfere with ICANN's ability to enforce accuracy requirements, including by being able to access full registration data (including any data elements that are redacted from publication in any registration directory) in order to assess data accuracy and enforce accuracy contractual requirements. This includes full access to registration data to enable the operation of the ICANN WHOIS Accuracy Reporting System ("ARS") and all validation functions under the ARS. In addition, because of the data accuracy requirements imposed by the GDPR, the EPDP Team recommends that requirements be developed to increase the accuracy of registration data.

38 Please include the rationale for your answers here.

According to Article 5.1(d) 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."

The ico. (Information Commissioner's Office in the UK) points out in its writings on "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."   In addition,the European Commission's technical input on ICANN's proposed GDPR-compliant WHOIS models underscored the GDPR's "Accuracy" principle and made clear that "reasonable steps should be taken to ensure the accuracy of any personal data obtained" for WHOIS databases and that ICANN should be sure to incorporate this requirement in whatever model it adopts.

Accuracy of domain name ownership is paramount to collection of WHOIS/Registered Name Holder data in the first instance. In addition, since this data will be used by others (with a lawful interest), ensuring that it is accurate for them is also relevant. Moreover, as demonstrated by the .dk ccTLD, when accuracy and validation of registration data is taken seriously, it leads to dramatic decreases in abuse and illegal activity on the top level domain. See: https://ccnso.icann.org/sites/default/files/field-attached/presentation-difo-increase-trust-25jun18-en.pdf

Prior to the adoption of the Temporary Specification, accuracy of WHOIS data was problematic. When the ARS was running, we know that almost 40% of randomly sampled registrations had a problem that warranted opening a compliance ticket on them. Therefore, even prior to ICANN seeking to modify its policies to comply with GDPR, a serious problem with accuracy existed. Now with the adoption of the

Temporary Specification, the ARS is not even operational. Without improved accuracy, it is likely that the quality of WHOIS data will decline, and the important policies being discussed by the EPDP will increasingly apply to a large amount of data the accuracy of which is questionable, and would be contrary to the public interest rationale for the collection of WHOIS data.

With the accuracy requirements that the GDPR imposes, accuracy is an issue fully within scope of the EPDP so that ICANN and contracted parties proactively address how they will ensure the accuracy of data in the first place, not just how they rectify inaccurate data brought to their attention after collection.

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

Save Your Progress

40 Do you want to save your progress and quit for now? You will be able to return to the form to complete at a later time.

Mark only one oval.

○ **Yes** *Stop filling out this form.*

○ No, I wish to continue to the next section

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.

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

1) Registrars should be required to provide an option for registered name holders to indicate that they are either a Legal or Natural Person.

2) Registrar should also generate a data element of the date on which registrant contact data was last verified/validated in accordance with the RAA, and the method used to do so.

45 Please provide the rationale for your answer.

1) GDPR does not apply to Legal Persons, 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.

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.

2) Currentness is a critical element of accuracy as required by the GDPR. Anyone obtaining access to this data for any of the authorized purposes will need to know how fresh it is. This includes but is not limited to ICANN compliance, which otherwise will not be able to enforce the data quality requirements of RAA.

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.

The IPC does not believe that collection of Technical Contact information should be “Mandatory”, however registrars should be required to offer the OPTION for registrants to provide this information. Many registrants wish to provide secondary contact information, including large corporate registrants who need to route the appropriate communications within their organization, and technically-novice registrants who need to enlist the help of an organization with greater technical expertise to manage their web presence. Even more registrants may simply want to list a backup contact for estate or succession planning or mere peace of mind of having a backup.

If this were to be made optional for registrars, many registrants would, in effect, be deprived of their ability to choose to list a second contact, especially if they lack the sophistication to know they could choose a different registrar that allows them to do so. Further, registrants who have already designated a different technical contact could be deprived of the choice they have already made if their registrar is permitted to discontinue the service.

Therefore, the IPC believes that Registrars should be ***required*** to provide registrants with the “OPTION” to provide Technical Contact information, although provision of this alternative contact information by registrants should not be mandatory.

Moreover, if the registrant opts 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?

Mark only one oval.

● Yes

○ No

49 Please provide the rationale for your answer.

Registrars should be required to offer this OPTION for registrants to provide this information, since some registrants desire or need to provide this information for the purposes listed above.

Many domain registrants will *want* to be contacted swiftly if anyone discovers a technical issue with their domain name.

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?

Mark only one oval.

○ Yes

● No

51 Please provide the rationale for your answer.

The IPC agrees that billing contact data should not be collected for any ICANN purposes as issues related to billing are firmly in the realm of the Registrar.

We do believe however that in addition to the optional collection of the technical contact (See Question 47) that Registrants should be given the option to provide an Administrative contact. Both the Technical and Administrative contact fields allow for the Registrant to designate additional suitable points of contact for these functions, adequate to facilitate timely resolution of any problems that arise in connection with his/her/its domain name. A mechanism to specify a separate Administrative Contact ensures the proper delegation of requests associated with domain name management, such as registration renewals or cancellations, purchase or sale-related inquiries or efforts, and other similar kinds of issues relating to the status, disposition, or control of the domain name.

The Security and Stability Advisory Committee (SSAC), which “advises the ICANN community and Board on matters relating to the security and integrity of the Internet’s naming and address allocation systems” addressed the importance of administrative and technical contact roles for maintaining control of a domain registration in its advisory, “SAC044: A Registrant’s Guide to Protecting Domain Name Registration Accounts.” SAC044 (https://www.icann.org/en/system/files/files/sac-044-en.pdf) specifically noted, among other things, that maintaining administrative and technical contacts plays a role in reducing single points of failure or attack.[8] This report was adopted by the ICANN Board and provides justification for mandating collection of this data from ICANN’s perspective and from a Registrant perspective – in line with ICANN’s purpose of ensuring contacts adequate to facilitate timely resolution of any problems that arise in connection with a domain name.

Administrative and Technical Contacts are also vitally important to a number of ICANN consensus policies developed by the global multi-stakeholder community over the last two decades that aim to protect the Registrant, and facilitate the efficient resolution of domain name disputes. Those policies are:

ICANN Transfer Policy, which supports robust competition in the domain name industry. Confirmation of a request to transfer a domain name from one registrar to another prevents domain name “hijacking” or unauthorized theft of the domain name.

ICANN’s Transfer Dispute Resolution Policy grants administrative contacts the right to contest an unauthorized transfer of the domain name. This serves a similarly important “consumer protection” safeguards for the registrant.

ICANN’s Expired Domain Name Recovery Policy specifies that notice of expiration can be sent to the administrative contact for a domain name.

ICANN’s WHOIS Data Reminder Policy is sent to administrative contacts annually to ensure that the domain name registrant’s contact data is up to date and accurate.

ICANN’s Uniform Domain Name Dispute Resolution Policy (UDRP) and Uniform Rapid Suspension (URS) system are domain name dispute resolution mechanisms to resolve cyber-squatting, and which require that service of process of the complaint be made on the administrative contact and the technical contact in WHOIS, in addition to the registrant. By requiring service on all of the contacts in the WHOIS, registrants are better protected in terms of due process and notice of service, and are less likely to fail to receive a complaint or ignore the complaint, which could result in a default judgment that could cause them to lose their domain name.

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

○ 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.

56 Enter additional comments for Recommendation #5 here.

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.

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:**

Mark only one oval.

● 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.

# 59 Please provide the rationale for your answer.

# 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 of recommendation 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.**

Contractual compliance is a critical and necessary function of ICANN, and part of its obligations to ensure that registrars/registries comply with their commitments in their contracts with ICANN. As such, the proper lawful basis for contractual compliance should be Art. 6(1)(b), and ICANN should receive all information it deems reasonably necessary to satisfy its compliance function.

This means that Annex D, Workbook 5, to the extent incorporated by reference into the recommendation, should be modified to ensure the best legal basis is used (i.e. Art. 6(1)(b)) or it should be revised to state that the lawful basis includes both Art. 6(1)(b) and Art. 6(1)(f). ICANN shouldn’t be subject to the risk that a rogue registrar decides to not provide personal information about a registrant to ICANN for compliance purposes under Art. 6(1)(f) because the registrar claims that the interests of the registrant outweigh the interests of ICANN just so that registrar can avoid a compliance audit.

In addition, Workbook 5, again to the extent incorporated by reference into the recommendation, should be modified to clarify that ICANN should receive all information that it deems reasonably necessary for compliance, not just the “minimum”, to ensure that ICANN can satisfy this important function.

This is particularly important for contractual compliance complaints, such as false whois concerns. The only way ICANN can investigate these complaints is to receive or have access to all of the relevant registrant information so that it can check for compliance. We disagree with the comment in Workbook 5 that suggests that transmission of registration data is not technically necessary to perform the registration contract (which we assume means to perform a compliance audit or compliance check). We believe that ICANN should receive or have as much access to the data as it deems necessary for the compliance function, and that it should not be unduly limited in a manner that makes it difficult or overly burdensome for ICANN to perform this function.

# 65 Enter additional comments for Recommendation #7 here.

Please see response to question 64. We also note that our members have submitted several contractual compliance complaints to ICANN about registrars' failure to provide registrant information to them in accordance with the requirements of the temporary specification. Those complaints have been pending for over 5 months with no response from ICANN. This inability of ICANN to investigate and respond to contractual compliance complaints is very troubling and points to a potential breakdown in the ICANN model.

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 14-15 of the Initial Report for details of the data elements.

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

Mark only one oval.

○ Yes

● **No**

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

City should not be redacted
Email should not be redacted

# 68 Please provide the rationale for your answer.

City needed in order to serve legal process and city not a sensitive personal data element

Email has been recognized as most important data element for law enforcement as well as DNS abuse, consumer protection and IP rights violation investigations. In the balance of privacy and other rights and interests, it is appropriate that this data element remain unredacted and publicly accessible. This is particularly the case because a registrant has the ability to create, at no cost, an email address that contains no personal data, such as the registrant’s name. We recommend that in addition to the registrant’s e-mail address remaining unredacted, that registrars inform registrants that their e-mail address will not be redacted, will be publicly accessible and that the registrant may create a valid e-mail address for purposes of registering the relevant domain name which e-mail address contains no personal data.

Email: The disclosure of a registrant's email address in a public WHOIS system is essential for the legitimate purpose of expeditiously contacting the registrant in case of possible infringements or illegal actions. The email address serves as a prime data point for both notifying a potential victim and communicating with a potential infringer in an objective manner without necessarily identifying the domain name holder. The legal basis of article 6.1 (f) GDPR and the corresponding balancing exercise favour the rights and interests of several third parties, including law enforcement, commercial entities and intellectual property rights holders. The publication of the email address has a limited impact on the registrant. A registrant always retains the ability to register a domain name with an unidentifiable email address (example: info@organisation.com). There are numerous free email address providers available and a registrant may even opt to use a privacy or proxy service when registering the domain name. Additionally, at the registration of a domain name, a registrant is (and can always be) sufficiently informed about the publication and possible further use of essential “personal” information. In this regard, the data subject will have reasonable expectations that this information will be accessible in relation to the registered domain name. The risk for the registrant receiving unsolicited emails cannot outweigh the accountability and transparency necessary when operating a website or email address related to a domain name. Masking the email address of registrants unduly restricts the protection of consumers, and enforcement of intellectual property and commercial rights and prevents parties from amicably settling disputes related to potential online infringements.

Should it be considered that the registrant's privacy interest in keeping his (freely chosen) email address hidden overrides the provided legitimate third party interests, than at least an effective and standardised policy for replacing the email address with a pseudonymised email must be implemented. A pseudonymised email address would redact any information potentially identifying the registrant by providing a unique registrant-specific replacement email address which is non-identifiable. Taking into account the balancing exercise of article 6.1 (f) GDPR, such pseudonymisation, together with the limited impact on the data subject, would tilt the balance sufficiently in favour of the legitimate third party interests for having a reliable measure of contact which can be associated to multiple domain names belonging to the same owner. [Please refer to Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC of the Article 29 Working Party (currently the European Data Protection Board), p. 42-43.]

Further, pseudonymising consistently across registrars in such a way that enables connecting registrants for research and dispute resolution expediency would prove prohibitively difficult. Web forms do not provide the same evidence of delivery as can be established by sending an email in the absence of subsequently receiving a "bounceback," and web forms can impose unreasonable and unrealistic character limits.

Finally, the IPC notes the letter from Dave Jevans to Göran Marby, Cherine Chalaby, and Rod Rasmussen sent on June 4, 2018 [https://www.icann.org/en/system/files/correspondence/jevans-to-marby-et-al-04jun18-en.pdf] that recommends "replacing plain text point of contact details with consistently hashed values, rather than redacting those POC details altogether. Consistently hashed values would allow an investigator or research to search registration data sets and to associate multiple domains that use the same POC details, while not disclosing the original POC data of a potential GDPR data subject."   We believe this, and similar mechanisms, should be explored more thoroughly and encourages SSAC to review and comment on the viability and utility of the proposal as a replacement for redaction.

City is needed to serve legal process, identify proper venue for litigation, and understand which controlling law and procedure applies. For example, "San Francisco" would indicate that controlling precedent and procedure from the Northern District of California might apply to litigation concerning the domain name, where "San Diego" would indicate that completely different law and procedure from the Southern District of California would control.

# **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.**

The GDPR is only to be applied as written to natural persons, not legal persons. To redact an organization name is not at all required or supported through application of the GDPR. This is extremely valuable information to identify or get in touch with the legal owner of the domain or to track abusive behavior by or against persons and entities, including against the RNH. When, in rare instances, and organization name includes personal data, such as a natural person's name, the person, in securing a license to do business under that name has provided clear consent in the use of that organization as a non-personal identifier. This is clearly stated in Recital 14 of the GDPR.

Redacting the "organisation" field in the public WHOIS would not only go beyond the GDPR remit, it would go against other important EU regulatory frameworks related to (online) accountability and transparency of businesses and e-commerce in the EU. Article 5 of Directive 2000/31/EC on electronic commerce for example requires that online service providers shall render easily and permanently accessible the following information: (i) their name, (ii) their geographic address, (iii) their contact details, including their electronic email address , (iv) their trade or commercial register number, etc. According to article 46 of Directive 2017/1132/EU relating to certain aspects of company law, Member States are also required to disclose the particulars of company officers in central national company registers. This personal data is specifically considered to be of public interest and may be accessed by any third party.

The organisation field normally does not contain any personal information as it pertains to legal entities to which the GDPR is not applicable. In the rare cases that the organisation reflects the name of an identifiable natural person, this person is required by EU law to disclose his (personal identifying) company information anyway. Redacting the organisation field would therefore go against other EU regulatory frameworks while not being necessary under the principles and obligations of the GDPR.

# **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 IPC supports the maintenance of the Organization field as this is not personal data and the GDPR does not cover legal entities. The IPC submits that, if an Organization name includes personal data, the individual whose name is included as part of the Organization name has filed the name as part of a license to bo business and therein has provided implicit and explicit consent of use of the name within the context of the Organization name and identity. Thus, the RHN should be provided with educational text around this and asked to provide the Organization name, if applicable.

# **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
●

Intent and wording of this recommendation requires

○ **amendment** Delete recommendation

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

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.

2.5.1.1. The email address MUST be unique and uniform across domain name registrations of the registrant at a given Registrar.

2.5.1.2. The email address ~~and the URL to the web form~~ MUST provide functionality to forward communications received to the email address of the applicable contact and MUST describe the methods used to forward communications and confirm their receipt.

2.5.1.3. Registrar MAY implement commercially reasonable safeguards to filter out spam and other form of abusive communications.

2.5.1.4. It MUST NOT be feasible to extract or derive the email address of the contact from the email address ~~and the URL to the web form~~ provided to facilitate email communication with the relevant contact.

# 78 **Please provide the rationale for your answer.**

At least an effective and standardised policy for replacing the email address with a pseudonymised email must be implemented. A pseudonymised email address would redact any information potentially identifying the registrant by providing a unique registrant-specific replacement email address which is non-identifiable. Taking into account the balancing exercise of article 6.1 (f) GDPR, such pseudonymisation, together with the limited impact on the data subject, would tilt the balance sufficiently in favour of the legitimate third party interests for having a reliable measure of contact which can be associated to multiple domain names belonging to the same owner. [Please refer to Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC of the Article 29 Working Party (currently the European Data Protection Board), p. 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 of recommendation 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 2 years. Cybersecurity incidents have dwell time that can go 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, particularly when it involves law enforcement, can be lengthy. It's important that information on previously registered domains is retained for a useful period for security and law enforcement needs. One year is simply not enough time for lookback needs. The consistent utilization, by security and LEA personnel, of historic data from various 3rd 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.**

On November 16, 2018, The EPDB issued Guidelines 3/2018 on the Territorial Scope of the GDPR. These Guidelines address the factors mentioned above. The Guidelines should be consulted by the EPDP Team as it considers the question of differentiating between registrants on a geographic basis. The Guidelines were issued following the expression of positions from contracted parties that it would not be feasible to distinguish between registrants on a geographic basis for the purposes of determining whether the GDPR should be applied. These positions should be reevaluated and further justified in light of the Guidelines, which suggest that it would be possible to agree that redactions to the data of registrants for the purposes of compliance with the GDPR should only be applied 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. The EPDP Team should continue to consider means to practically implement this principle, but the IPC submits that the principle itself should guide discussions, and not the purported impracticality of geographic differentiation.

# **85 Please provide the rationale for your above answer.**

The IPC is concerned that some have sought to globalize the application of the GDPR through the application of a policy that does not oblige contracted parties to apply a geographically limited law in a geographically limited manner. ICANN (and its policies) should not serve as a means to achieve global application of a law that has limited territorial application. ICANN should be primarily concerned with the the objectives set forth in its mission, which has from the inception of the WHOIS framework included the practice of collecting and displaying the information of domain registrants for the purposes of ensuring the security and stability and resiliency of the DNS. To the extent exceptions are required to accommodate national laws, the WHOIS Conflicts Policy was agreed. The purpose of this exercise is to determine how to accommodate exceptions to the collection and processing of data, as it existed prior to the GDPR, to accommodate the GDPR. The purpose should not be to maximize and globalize the application of the GDPR. While doing so may suit the objectives of some stakeholders, it would also raise the risk that some countries may seek to enact counterbalancing rules or laws to oblige disclosure of registrant data for what it considers to be legitimate purposes, leading to a more fractured and complex compliance landscape.

# **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.**

The question should also be posed, what are the risks of not differentiating on a geographic basis. Longer term, the risks to the status of ICANN as an independent multistakeholder organization are greater where the geographic limitations of laws are not practically acknowledged in the implementation of its policies.

# 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 other factors to consider are the practicalities of application and looking to live examples of other businesses and entities that are differentiating between legal and natural persons because that is how the GDPR is set-up and it needs to be applied as intended, if not immediately, eventually. Therefore, if not required immediately, it should be required to be implemented within a reasonable timeframe when the technical set-up is commercially feasible. It is possible to set-up a self-identification system, with supportive educational language, alerting RNH to the definitions of legal and natural persons and to specify that any information provided is attested to be true, accurate and submitted to the best knowledge of the RNH. We note that in the GDPR Domain Industry Playbook v. 1.0 issued by eco it was recommended that “input from DPAs should be sought as to whether a distinction could be made based on a self-identification by the registrant.”

Due account should be taken of existing registers (ccTLD, company, trademarks, etc.) to which the GDPR applies. Based on existing processes with various ccTLD registry operators, such as EURid, the distinction can be made based on the self-identification of the registrant together with clear information on the implications of each choice. The registrant must be made aware that the name and contact information of a legal person will be published and that he is responsible for providing non-identifiable contact information. With regard to natural persons designated as admin or technical contact, an option can be provided to redact the name of that person in case he/she is a natural person.

# 88 Please provide the rationale for your above answer.

The distinction would prevent the over-application of the GDPR and allow for the required transparency and accountability online. The information of legal persons must be made available by default for law enforcement, consumer protection, anti-counterfeiting and cybersecurity purposes. In this regard, the EU E-Commerce Directive also requires legal entities who provide services to Internet users to be transparent and provide their identification and contact information in a direct and easily accessible manner (Art. 5 E-Commerce Directive 2000/31/EC). An incorrect self-identification could serve as an indication of bad faith and a legitimate reason for the registrar or registry to immediately disclose the identity and contact information of the underlying registrant upon request.

The risks of making the above distinction would be minimal. Registrars would only be required to provide clear information so to avoid unnoticed or unintended publication of personal data. A person registering a domain name for a legal person is not required to provide contact information which are related to an identified or identifiable natural person as this contact information can easily be anonymized (i.e. domainadmin@company.com).

In situations where it is difficult to separate the data of natural persons from that of legal persons, such as if the legal person is a sole proprietorship, if the name of a person appears in the company's name, or if the business address is a natural person's residence, this relevant (personal) information is also made public on a mandatory basis in the national company register where the legal entity is registered (see art. 30 and onwards of Directive 2017/1132).

Registrars would not face an increased liability unless related to their transparency requirements. Sufficiently clear information must be provided to prevent a registrant from unwillingly disclosing personal data. With regard to the provision / collection of information, it is not required to discharge the registrant of all responsibility for providing non-identifiable information, as long as the registrant is properly informed.

# **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.**

The IPC supports a study showing live examples of the application of the natural and legal persons differentiation.

# **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.**

The .TEL gTLD has been making this distinction since at least 2006. See ICAA, TEL Registry Agreement, Appendix S, Part VI, Section B, (May 2016).

Generally, in ccTLDS and certain gTLDs, a system of self-identification is implemented where a potential registrant must indicate whether it is a natural or legal person (most notably EURid for .eu, also DNS Belgium for .be, FICORA for .fi, AFNIC for .fr, SIDN for .nl, etc.). The registrant is informed of the implications of this choice (such as the publication of the legal person's name and contact information) before registering. A registrant which is a legal person must then evaluate whether his contact information refers to an identified or identifiable natural person and adjust accordingly (or not).

EURid's Domain Name Whois Policy v. 4.0, Sections 2.3 - 2.4 provides that "those requesting to register a .eu Domain Name in one of the available scripts are required to provide certain information through an accredited Registrar. In respect of the name of the Registrant there are two fields: The first is 'Name' and the second is 'Company'. Both fields may be completed or just the 'Name' field. If only the first field is completed, it is assumed that the registration is in the name of a private individual (natural person). If the 'Company' field is completed, it is assumed that the company is the Registrant. … All Registrants are required to accept the Terms and Conditions in which the Registrant authorises the Registry to publish certain personal data. (i) When the Registrant is a legal person or another form of organisation the Registry generally publishes the following information in its WHOIS: a) name, address and telephone and fax number of the Registrant; b) technical contact person; c) e-mail address …". [Domain Name Whois

Policy v. 4.0, EURid, available at https://eurid.eu/d/22380/whois_policy_en.pdf]

The CENTR Report on WHOIS Status and Impacts from GDPR determined that “to differentiate between private and organisations as registrants, 68% of registries allow the registrant to self-select. In several cases, the registry uses social security number, business number or even tax file number. 18% make no distinction.” [CENTR Survey - Whois status and impacts from GDPR, June-July 2018, available at https://centr.org/library/library/survey-report/centr-report-whois-status-and-impacts-from-gdpr.html.]

For trademark applications in the EU or national trademark registers, an applicant is asked whether he is a natural or a legal person. Irrespective of the distinction, the name and address of the applicant is always made publicly available, as this information is considered to be of public interest (article 111(9) Regulation 2017/1001).

Finally Many ccTld registries differentiate between natural and legal person 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,Nic-hdl
>
> .BE legal person data is publicly available in the whois and provides the Organization, language, street address, city, country and phone. Contact form available
>
> .CZ legal person data is publicly available in the whois and provides registrant organization, street address, city, country and nic-handle. Also provides the same data fields for admin and tech contact.
>
> .DK treats natural and legal person data the same 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 the whois and provides registrant org, admin contact name and name of technical contact
>
> .EU 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. Technical contact name and email address.

.FR legal person data is publicly available in the whois and provides the registrant org, street address, city, country, phone and email address. Technical contact name, registrant org, street address, city, country, phone and email address. Admin contact, name, registrant org, street address, city, country, phone and email address.

.IE legal person data is publicly available in the the whois and provides the registrant org, admin and tech nic-handles

.IT legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code, phone number and email address. Same data fields are available for admin and tech contact and includes individual names.

.LT legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code, phone number and email address. Same data fields are available for tech contact.

.LV distinguishes between natural and legal person. Legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code, phone number and email address. Same data fields are available for admin and tech contact and includes individual names.

.LU legal person data is publicly available in the the whois and provides the registrant org, street address, city, country and postal code Admin and Tech contacts are masked.

.MT legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code, phone number and email address. Same data fields are available for admin and tech contact.

.NL legal person data is publicly available in the the whois and provides the registrant org and admin email address.

.PL legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code. Indicates Organization in the record.

.PT legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code. Same data fields are available for managing body role.

.SI legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code, phone number and email address. Also provides Tech contact email address.

.SE legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code, phone number and Contact ID. Same data fields are available for admin and tech contact 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 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:

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.

Change first sentence to read:

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 AND INCORPORATED IN THE TEAM’S FINAL REPORT, noting that the term should be modified to refer to “parameters for responding to lawful disclosure requests.”

# **93 Please provide the rationale for your answer.**

The Team’s work is incomplete until the issue of setting parameters for responding to lawful disclosure requests to redacted data has been resolved. A recommendation that lacks any deadline for achieving this resolution is equally defective. As noted above, the Temp Spec should not be superseded by a consensus policy that lacks a strong model for access to redacted data by legitimate third parties. In order to kick start the process, IPC proposes starting from and building upon the consensus policy already adopted (though not yet implemented) for privacy/proxy disclosures.

# **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 of recommendation 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 a Joint Controller Agreement or the appropriate Controller-

Processor agreement with the Contracted Parties and the needed Data Processing Addendums.

# 97 **Please provide the rationale for your answer.**

The IPC believes that based on the factual and legal analysis conducted to date by the EPDP of the data elements processed by the respective parties (ICANN, the Registrars and Registries) that a joint controller relationship exists. It therefore supports this recommendation as the application, negotiation and installation of a Joint Controller Agreement and the needed Data Processing Addendums will proportionality make clear the roles and responsibilities of each party and the attributable respective liability of each party. It will therefore in sum lay out the needed legal framework and working solution for the update ICANN ecosystem in line with GDPR and data protection laws. If further findings on this topic result in a different determination of roles and responsibilities, the IPC ultimately supports the appropriate controller/processor arrangement that can enable ICANN to assume sufficient legal responsibility such that ICANN can compel relevant contracted parties to respond to Whois queries from accredited requestors, most likely as part of a Unified Access Model currently being explored by ICANN.

# 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.**

Save Your Progress

# 100 **Do you want to save your progress and quit for now? You will be able to return to the form to complete at a later time.**

Mark only one oval.

○ **Yes** *Stop filling out this form.*

○ No, I wish to continue to the next section

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: "joint-controller," "controller," and "processor.**

Some of the specifics in the tables beginning on p. 63 may need some 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 P/P 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 then would typically file an amended complaint with the updated registrant information. Thus, we would suggest 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, we would suggest the DRP as the "responsible party" in the sense that 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 IPC 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.**

See response to Question 102.

# **104 Additional comments for Recommendation #14.**

[none]

Save Your Progress

# 105 Do you want to save your progress and quit for now? You will be able to return to the form to complete at a later time.

Mark only one oval.

○ **Yes** *Stop filling out this form.*

○ No, I wish to continue to the next section

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.**

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

# 110 Additional comments for Recommendation #15.

Although we support the recommendation as written, we have some further comments on this issue. In general, the UDRP has become more onerous, because in general, all complaints must now be filed as “Doe” complaints, and then later amended once the full registration information is disclosed to the complainant. 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. It would be exceedingly useful if, as part of a UDRP or URS filing, registries or registrars could somehow 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, but 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.

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:

Mark only one oval.

● 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.**

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

This already is happening in practice, and is not much different from what has been happening historically in cases of UDRP or URS cases involving P/P registrants. However, it would be good to formalize this process in UDRP and URS proceedings through the relevant policies, rules, and supplemental rules. The issue is already on the radar of the RPM Review PDP.

Finally, the requirements of the Temporary Specification should be modified to allow investigation 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 a demonstrable connection between the registrants.

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:**

Mark only one oval.

● 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.

# 117 Please provide the rationale for your answer.

# 118 Provide additional comments for Recommendation #17 here.

Although we support the recommendation as written, we would advise that the proposed representative of the RPMs PDP WG should include a representative of a URS/UDRP dispute resolution provider, who would be best positioned to opine on the issue of access to domain name registration data in the context of conducting the URS and UDRP.

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:

Mark only one oval.

- ● 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.

#   **121 Please provide the rationale for your answer here.**

It is an essential requirement in line with the GDPR that Data Processing Agreements are entered into with any party processing domain name registration data, and the IPC fully supports this Recommendation as written to ensure the continued operation of the UDRP and URS in compliance with applicable requirements concerning data protection.

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

It is important that UDRP/URS and other DRP decisions remain publicly-available and transparent to the greatest extent possible, including the name of the parties. Knowing the name of the parties is important in later cases, especially respondent information, given that losing prior DRPs is a potential indicator of bad faith in other cases. In this context, the legitimate interest in transparency of these disputes must outweigh the privacy interest of the parties, just as is the default rule in a litigation context (except in very limited cases where party identities are redacted for special sensitivities). Data processing provisions should be a component of broader more formal contracts between ICANN and DRPs, an idea that is the subject of discussions within the RPM Review PDP. That said, the retention period must be appropriate in this particular context, and may be longer than the necessary data retention period for other purposes, to ensure continued transparency of determinations in the URS and UDRP, both in published determinations and in the context of dispute resolution providers' internal databases.

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?

We encourage the EPDP Team to explore whether policymaking is appropriate to clarify that disclosure of non-public WHOIS data can be made prior to the administrative proceeding, and to explore what controls are needed to prevent abuse of such a system.

# 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. Anecdotally, 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, 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:
Mark only one oval.

● 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:**
Mark only one oval.

● 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.**

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.

Save Your Progress

# 135 Do you want to save your progress and quit for now? You will be able to return to the form to complete at a later time.

Mark only one oval.

○ **Yes** *Stop filling out this form.*

○ No, I wish to continue to the next section

Section 3: Other Recommendations

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

Please see our comments to questions 145 and 147 below. In general, we note that it appears that the needs of users of WHOIS data are not being properly reflected or considered in the recommendations of the EPDP in favor of the desires to limit risk of the contracted parties and ICANN, and of consistently favoring the privacy interests of the registrants without appropriately balancing the needs of others. In addition, we are concerned that the Recommended Purposes do not set forth with sufficient specificity the legitimate interests of third parties, as well as the full range of ICANN purposes that are consistent with its mission, to comply with the GDPR. We hope the needs of WHOIS users will be more carefully considered as the EPDP work moves more firmly towards questions of access.

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:**

Mark only one oval.

● 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 IPC is in full support of this Recommendation, as written, however we call your attention to our response to Question #97 above that states if further findings on this topic results in a different determination of roles and responsibilities, the IPC ultimately supports the appropriate controller/processor arrangement that can enable ICANN to assume sufficient legal responsibility such that ICANN can compel relevant contracted parties to respond to Whois queries from accredited requestors, most likely as part of a Unified Access Model currently being explored by ICANN.

# **140 Provide additional comments for Recommendation #21 here.**

The IPC submits that this is a factual and legal determination that is shown and supported by the work of the EPDP to date and which will be further clarified through the completion of its work. The set-up of the joint controller relationship and installation of a JCA will allow for the accurate and legally supported proportional assignment of roles, responsibilities and liabilities of the parties.

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:**

Mark only one oval.

○ 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~~ 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
- Privacy & Proxy Services Accreditation Issues Policy

* Additional WHOIS information Policy (governing insertion of EPP status

codes)

- Expired Registration Recovery Policy

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

# 143 Please provide the rationale for your answer here.

We agree overall with reviewing all existing ICANN Consensus Policies and implementation documents for consistency with final Consensus Policy on RDDS, although the specific contours may evolve by the time the final EPDP recommendations are adopted. For instance, the specific note about admin/technical contacts going away may not be the case, and we might suggest that part of this text be deleted because it presupposes a final conclusion. We also propose adding the PPSAI policy to this list, even though it is still in IRT phase – technically it has still been adopted as a relevant ICANN Consensus Policy. The work of the PPIRT should be resumed immediately.

# 144 Provide additional comments on Recommendation #22 here.

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

A recommendation that describes how Privacy/Proxy data should be displayed in WHOIS is needed.   IPC suggests using the wording from the Temp Spec, as revised below   e.g.

Recommendation XX

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 include in the public WHOIS and return in response to any query full WHOIS data, including the existing privacy/proxy pseudonymized email.

Except as set forth above, the privacy/proxy service policy should not be addressed in the EPDP, and instead, ICANN should immediately proceed with finalizing implementation of the PPSAI.

Save Your Progress

# **146 Do you want to save your progress and quit for now? You will be able to return to the form to complete at a later time.**

Mark only one oval.

○ **Yes** *Stop filling out this form.*

○ No, I wish to continue to the next section

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.**

Overarching Comments

Summary

1. The EPDP WG has not addressed the subject of access to registrant contact data for legitimate purposes, nor the negative impact of lack of redaction to consumers and internet users.
2. In conflict with its charter, which is to affirm the Temp Spec, the EPDP WG has reduced scope of the Temp Spec, though the Temp Spec over-complies with GDPR as it is currently written and applied.
3. The EPDP WG has not been consensus driven, participation has been dominated and overly-influenced by the contracted parties house and the NCUC.
4. The EPDP WG has not considered real use cases nor the actual impact redaction is having on the operation, security and stability of the Internet.

Supporting Detail

1. Access is a consumer safety and security issue which has not yet been addressed by the EPDP WG, the contracted parties, nor by ICANN org:
   - See MarkMonitor's study here detailing lack of success in obtaining Whois data and the adverse impact it has had on MarkMonitor clients. Findings:
     - Only 9% of full publicly available Whois records have un-redacted registrant information post-GDPR.
     - Of more than 350 requests made to more than 70 registrars, Whois data was provided in response only 26% of the time.
     - 74% of Whois requests were either ignored or denied.
     - MarkMonitor has seen a 19% loss of operational efficiency regarding brand enforcement activities.

- See AppDetex letter here outlining lack of registrar fulfillment for reasonable Whois data requests. Findings:
    - Redacted Whois contact data is largely unavailable for legitimate and legal purposes.
    - The majority of registrars do not respond to requests for data.
    - The small percentage of requests that are fulfilled are not completed in a reasonable time period.
    - There is no consistency of process for requesting redacted Whois data.
    - Average response time to a data request: 9.13 days
- See Anti-Phishing Working Group's study here detailing the impedance of cybercrime investigations and the permission of harm to users. Findings:
    - Cyber investigations and mitigations are impeded because investigators are unable to access complete domain name registration data.
    - The mitigation or triage of cyber incidents cannot be accomplished in a timely manner.
    - Whois has become an unreliable or less meaningful source of threat intelligence.
    - Requests to access non-public Whois by legitimate investigators for legitimate purposes are routinely refused.
- See the Cybersecurity Tech Accord Statement here. Findings:
    - Redaction has impacted investigations and mitigations
    - There are real consumer and societal harms
    - Issues are escalating
- See SSAC 101
    - 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.

The negative impact from the reduced access to WHOIS data on public safety and security following the implementation of the of the Temporary Specification has been detailed by the Public Safety Working Group (PSWG) of the GAC and the presentation they gave in Barcelona. See: https://gac.icann.org/presentations/icann63%20pswg.pdf The PSWG conducted a survey of law enforcement agencies around the world and received responses from approximately 40 different countries, including a dozen EU Member States. The survey results found that since the Temporary Specification has come into effect, only 8% of the respondents find WHOIS meeting their needs, 25% say it partially meets their needs and now 67% say it doesn't meet their needs at all (as opposed to only 2% who said that it didn't meet their needs at all before the Temporary Specification became effective). Similarly, 52% say the current unavailability of WHOIS data has delayed investigations and 26% say it has caused investigations to be discontinued.

2. The EPDP has reduced the scope of Temp Spec which already over complied with GDPR
    - Eliminates the Administrative Contact and the possibly redacting the Organization field.
    - In SSAC 101, 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.
    - SSAC - ICANN has an obligation to ensure the continued availability of gTLD registration data to the greatest extent possible.
    - The EPDP has failed to consider SSAC 101, and GAC advice related to WHOIS
3. The WG has failed to consider SO/AC recommendations other than the NCUC and the CPH
    - Consensus must include the vote of all participating SOs and ACs, not just the constituencies of the GNSO.
    - The EPDP WG is failing ICANN's multi-stakeholder policy development model by ignoring the needs of key third party interests such as cybersecurity and intellectual property.
    - The WG has been unreasonably focusing on cost minimization, rather than to design a policy that is reasonably implementable, and allowable under GDPR.
    - This is evident from the inexplicable opposition to conduct research and consider what is already implemented in CCTLDs.

4. The WG is not considering the real impact of redaction and unavailability of whois data for day-to-day tasks.
    - Transferring domain names
    - Issuing certificates
    - Remediation of security and consumer protection threats
    - ICANN compliance
    - Blocking of harmful content such as phishing and malware on compromised legitimate sites