# Input from ICANN Org

**EPDP TEAM QUESTIONS FOR ICANN ORG**

**Temporary Specification Expiration**

1. *The Team seeks clarification on the exact expiry date of the Temporary Specification. In Section 3, the effective date of the Temporary Specification is 25 May 2018, but was adopted on 17 May 2018.*

Per Section 3 of the Temporary Specification, the effective date of the Temporary Specification is 25 May 2018. Additionally, the ICANN Board resolution adopting the Temporary Specification states: "The Temporary Specification will be effective for a 90-day period beginning 25 May 2018. The Board will reaffirm its temporary adoption every 90 calendar days for a total period not to exceed one year."

**Temporary Specification Amendments**

1. *If the Board is considering any amendments to the Temporary Specification, it would be helpful if the EPDP Team can be made aware of any proposed changes in advance. Is the Board currently considering any amendments to the Temporary Specification? To address what requirement?*

ICANN Org is not aware that any amendments are currently being considered. The Board is scheduled to meet in August to consider reaffirming the Temporary Specification according to the process in ICANN's agreements for adopting temporary policies and specifications.

2. *Can an update be provided on the status of the reconfirmation of the Temporary Specification by the ICANN Board?*

The Board reaffirmed the Temporary Specification with no changes on 21 August 2018.

**Temporary Specification Clarifications**

1. *When ICANN refers to "security" as part of its mission - can ICANN describe what types of security are included??*

The word "security" appears 36 times in the ICANN Bylaws in relation to topics such as: the DNS, the Internet, the Internet's system of unique identifiers, the Internet's root server systems, the registry database, and Top Level Domains.

2. *With regard to the term "content," in Section 4.4.5 - can ICANN provide context for use of the term?*

It is generally believed that ICANN does not see itself in the role of a content regulator but there are scenarios where use of the term "content" is appropriate in this section.

Section 4.4.5 of the Temporary Specification provides a mechanism for third parties to contact Registered Name Holders to address "technical issues and/or errors with a Registered Name or any content or resources associated with such a Registered Name." With regards to the question about ICANN being a "content regulator," Section 1.1.c of ICANN's Bylaws makes clear that ICANN does not regulate content.

3. *Regarding Temporary Specification section 4.4.8 - Supporting a framework to address issues involving domain name registrations: the team requests additional specificity. Does this mean that registrars and registries must support a uniform access mechanism when approved or is there some present requirement?*

Section 4.4.8 identifies that addressing issues involving domain name registrations, including but not limited to: consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection using a framework to be developed is a legitimate purpose for the processing of registration data. With regard to the second question, section 4.4.8 does not by itself require that registrars and registries must support a uniform access mechanism when approved. Please note however that section 4.1 of Appendix A does have a requirement for registrars and registries to "provide reasonable access to Personal Data in Registration Data to third parties on the basis of legitimate interests pursued by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Registered Name Holder or data subject pursuant to Article 6(1)(f) GDPR." Separately, section 4.2 of Appendix A requires registrars and registries to "provide reasonable access to Personal Data in Registration Data to a third party where the Article 29 Working Party/European Data Protection Board, court order of a relevant court of competent jurisdiction concerning the GDPR, applicable legislation or regulation has provided guidance that the provision of specified non-public elements of Registration Data to a specified class of third party for a specified purpose is lawful." Section 4.2 of Appendix A further requires that registrars and registries "provide such reasonable access within 90 days of the date ICANN publishes any such guidance, unless legal requirements otherwise demand an earlier implementation."

4. *Regarding Temporary Specification section 4.4.13 - Handling contractual monitoring requests: which data sets will be required to measure compliance against which contractual provisions?*

The data requested by ICANN Contractual Compliance will vary depending on the particular compliance issue. For example, for a registrant's complaint that a renewal reminder email was not received, ICANN Contractual Compliance may request from the registrar of record a copy of the communication to the Registered Name Holder.

5. *In section 5.7 of the Temporary Specification (and other sections), what is the meaning of "reasonable access"? Is it access to personal data reasonably provided? Does "reasonably" relate to the effort necessary to retrieve it? Does it mean how criteria for releasing it are applied, i.e., legitimate and not overcome by the rights of others? Should it just be "access"?*

"Reasonable access" is not defined in the Temporary Specification. Generally, compliance with the requirement for registrars and registries to provide reasonable access to non-public registration data is evaluated on a case-by-case basis, based on evidence provided by the requestor, including its request for access to non-public registration data, evidence of the requestor's legitimate purpose for accessing the non-public registration data, the timing and content of the contracted party's response to the request (if any), and any other information or evidence relevant to assessing the request and response.

6. *Regarding data disclosures concerning LEA requests: does GDPR compel a report of those disclosures to be made to the data subject? Please provide analysis of "in-jurisdiction" and "out-of-jurisdiction" requests.*

The latest Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data – For Discussion addresses the question of "whether or not logs of query activities concerning non-public data must be available to the registrant upon request except if prohibited by a relevant court order or legal requirement." Please refer to Section 8 of the draft framework for more information on this topic. The draft framework is published for community discussion and to seek guidance from the European Data Protection Board. With a better understanding of the law, we will all be well positioned to develop, implement and enforce a legally sound, consistent unified model for access to non-public registration data, and lower the risk for the contracted parties in order for them to be able to accept such model.

7. *The text in the preamble of Appendix C is simply an overview of the processing requirements that follows. The preamble does reference the GDPR, and it states that generally "terms with initial capital letters have the meaning given under the GDPR." But we would need more clarity around what specific language in the preamble is seen to be similar to what specific language in the GDPR to be able to comment further on this question.*

The text in the preamble of Appendix C is simply an overview of the processing requirements that follows. The preamble does reference the GDPR, and it states that generally "terms with initial capital letters have the meaning given under the GDPR." But we would need more clarity around what specific language in the preamble is seen to be similar to what specific language in the GDPR to be able to comment further on this question.

8. *Why did ICANN include the term content in 4.4.5?*

To be clear, ICANN does not regulate content.

Section 4.4 lists purposes for processing personal data in registration data*. The processing activities in this section are not limited to ICANN's, they include the processing activities by Registrars and Registries and other third-parties. Section 4.4.5 says one of those purposes is "Enabling a mechanism for the communication or notification to the Registered Name Holder of technical issues and/or errors with a Registered Name or any content or resources associated with such a Registered Name." For example, a law enforcement agent investigating potentially illegal content might use the registration data to identify and contact the registered name holder as part of the investigation. As a point of reference regarding processing by third parties, on 25 May 2018 the EDPB endorsed a statement of the WP29, which stated that the "WP29 expects ICANN to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data." <https://www.icann.org/en/system/files/files/statement-edpb-whois-27may18-en.pdf>

(*Note that Registration Data is defined in the Temporary Specification as "data collected from a natural and legal person in connection with a domain name registration." This is broader than just data displayed in RDDS and includes all data collected in connection with the domain name registration.)

9. *Is making the natural vs legal distinction WHOIS within the picket fence, i.e., a suitable topic for policy discussion?*

Yes, access to gTLD registration data generally is one of the allowed topics for consensus policy as set forth in ICANN Bylaws and registry and registrar agreements. (That list of topics is referred to by some as "the picket fence"). Please refer to AnnexG-1 and G-2 of the ICANN Bylaws as well as Specification 1 Section 1.3.4 of the Base Registry Agreement and the Consensus Policies and Temporary Policies Specification of the Registrar Accreditation Agreement, which provide that: "maintenance of andaccess to accurate and up-to-date information concerning domain name registrations" is one of the topics on which ICANN may enforce consensus policies.

10. *The Temporary Specification for gTLD Registration Data EPDP Team is currently considering language on a "Purpose M" regarding ICANN's role in coordinating the development and implementation of policies concerning ICANN's dispute resolution processes in the context of domain name registrations. Two of the processes currently being considered within scope of this purpose are the PDDRP (Post Delegation Dispute Resolution Process) and the RRDRP (Registry Restrictions Dispute Resolution Process). It would particularly be very helpful and important to the EPDP Team if ICANN could provide clarification on any point within the processes of PDDRPs and RRDRPs where processing of gTLD Registration Data is necessary for the dispute resolution processes to be completed. This clarification should identify which (if any) data elements within gTLD Registration Data are necessary, as well as all parties involved in the processing activities.*

The PDDRP rules and the RRDRP rules each require the complainant (a trademark holder in PDDRP proceedings; an established institution in the relevant community in RRDRP proceedings) to "provide the name and address of the current owner of any at-issue domain name registration related to the dispute, to the best of the Complainant's knowledge[.]" See PDDRP Rules, Section 3(b)(iv); RRDRP Rules, Section 3(b)(iv). The dispute resolution provider is required to serve the respondent (the registry operator) with a copy of the complaint, and to retain information related to the provider's transmission of the complaint. Thus, these procedures may result in the complainant, provider, and/or respondent's processing of gTLD registration data.

It should be noted that neither of these procedures have been used yet.

ICANN org would not process gTLD registration data in proceedings of either of these procedures because they are administered by independent dispute resolution service providers. However, if either procedure is used and ICANN org receives a panel's decision, then that decision would include gTLD registration data.

On another note, the current wording of Purpose M states: "coordinating the development and implementation of policies concerning ICANN's dispute resolution processes in the context of domain name registrations." It is unclear how developing and implementation of policy would involve processing of gTLD registration data or personal data.

11. *What is the rationale for not redacting organization field in the Temporary Specification?*

Including the registrant organization field was determined to be consistent with ICANN org's stated goal of complying with the GDPR while maintaining the WHOIS system to the greatest extent possible. The name of an organization refers to a legal person and not a natural person and therefore is arguably not covered under the GDPR. Additionally, the organization field is an optional field for registrants so to the extent that the registrant provides the organization name, the Temp Spec allows for publication of that information.

Leading up to the development of the Temporary Specification, ICANN org consulted with the community and the DPAs to determine which data elements should continue to be made publicly available. Through the data matrix exercise where ICANN org asked contracted parties and interested stakeholders to identify user types and purposes of data elements required by ICANN policies and contracts, 40 user purposes for the registrant organization field were identified.

For reference, Section 5.5.16(i) of the Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation (also called the Cookbook) states that "the registrant "organization" would be required to be published (if applicable) so that registrations of legal entities would readily include the name of the entity."

*12. Has ICANN given any thought to scenarios where the „Organization" field might contain personal information? 2.) As the Organization field shall be populated on an optional basis, has ICANN given any thought to a consent requirement or, where another legal basis than Art. 6 I a GDPR was considered, what legal basis shall be applicable based on what rationale?*

The organization field, which is an optional field, was one of the topics of discussion among the community during the development of the Cookbook. See sections 5.4 and 5.5 of the Cookbook.

Additionally, the 5 July 2018 letter from the European Data Protection Board states: "The GDPR does not apply to 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." Recital 14 of the GDPR states: "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."

Registrars have always been obligated to inform and obtain consent from the registrants regarding what data elements are collected, what data elements are published, what data elements are optional, and the intended uses and recipients of the data. (See for example Section II.J.7.b in the 1999 RAA and Section 3.7.7.4 of the 2013 RAA.)

The Temporary Specification relies on 6(1)(f) as the legal basis for the mandatory publication of certain fields, including registrant organization. As noted in our original response, the registrant organization field refers to a legal person and not a natural person. The registrant may give consent for publication of additional fields, for example, the registrant name field.

In considering the applicability of the possible legal bases and after consultations with the community, it was determined that 6(1)(f) was the most appropriate legal basis to support the stated goal of complying with the GDPR while maintaining the existing WHOIS to the greatest extent possible.

*13. What is the rationale for the bolded wording in this Temporary Specification section:* ***As soon as commercially reasonable****, Registrar* ***MUST*** *pr ovide the opportunity for the Registered Name Holder to provide its Consent to publish the additional contact information outlined in Section 2.3 of Appendix A for the Registered Name Holder.*

The "As soon as commercially reasonable" language was added in Section 2.3 of Appendix A of the Temporary Specification because Implementation of this requirement would take development time on the part of the contracted parties. However, due to the timing of the Board adoption of the Temporary Specification, there was recognition that additional time would be needed to implement the requirement.

The "MUST" language goes back to our stated objective of preserving the existing WHOIS to the greatest extent possible while complying with the GDPR. Giving as many registrants as possible the ability to have their full contact information published was in keeping with this stated objective.

*14. What was the community input into this Temporary Specification section that, in each of the two cases, led to the wording, "as soon as commercially reasonable," and "MUST"?*

As far back as the development of the Calzone model, various parts of the community communicated to ICANN that registrants should be afforded the ability to have their full contact information published. See the Working Draft Non-Paper -- Selected Interim GDPR Compliance Models & Comments dated 07 Feb 2018.

During development of the Temp Spec, contracted parties pointed out that this requirement would require development time to implement in their platforms.

*15. Why city field is redacted in the Temporary Specification:*

Regarding the EPDP Team's question about why the City field is redacted in the Temp Spec, the Cookbook provides the following rationale: "The registrant's state/province and country will be published, but the address fields that could be used to more specifically identify the registrant would not be included in the public WHOIS (e.g. street, city, postal code). This would enable non-accredited users to determine the registrant's general location and likely jurisdiction but would generally not enable identification of the registrant". The link to the Cookbook:https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf. The above quote is on page 26.

**EPDB Advice**

1. *Can ICANN summarize in some searchable form the contacts and engagements with the EDPB and/or other DPAs in relation to the Temporary Specification for gTLD Registration Data?*

ICANN org has been open and transparent with our engagements with the EDPB and DPAs. All of the formal written communications from EDPB and DPAs are published on ICANN correspondence. In addition, we've had informal verbal conversations with the EDPB and DPAs to educate, inform, and ask for guidance. Summaries of those informal conversations are published in blogs. To assist the EPDP Team in its work, ICANN org will provide the EPDP Team with a compiled list of correspondence received and blogs published thus far, including the topic of each correspondence/blog.

*2. Can ICANN summarize in some searchable form the contacts and engagements with the EDPB and/or other DPAs in relation to the Temporary Specification for gTLD Registration Data?*

ICANN org has been open and transparent with our engagements with the EDPB and DPAs. All of the formal written communications from EDPB and DPAs are published on ICANN correspondence. In addition, we've had informal verbal conversations with the EDPB and DPAs to educate, inform, and ask for guidance. Summaries of those informal conversations are published in blogs. To assist the EPDP Team in its work, ICANN org will provide the EPDP Team with a compiled list of correspondence received and blogs published thus far, including the topic of each correspondence/blog. See DPA Advice Summary-DRAFT.xlsx.

*3. Is there any further information that can be provided in relation to the discussions that have been held with the EDPB and/or DPAs in addition to the blog posts and correspondence that have been shared, such as briefing notes and summaries of meetings?*

Aside from the blog posts and correspondence that have already been shared, and consistent with ICANN Publication Practices, ICANN org has not identified any additional notes or summaries of meetings that are suitable for publication.

ICANN org has previously stated that having clear guidance may increase legal certainty for ICANN and the contracted parties as well as assist the community in the Expedited Policy Development Process (EPDP) to consider the Temporary Specification for gTLD Registration Data (Temp Spec). Our commitment to transparency in publishing summaries of our interactions with the EDPB supports this stated purpose.

In this regard, we've posted summaries of our conversations with the EDPB and DPAs on ICANN's Data Protection/Privacy Issues page. The purpose of these conversations has been to educate, inform, and request guidance. In these discussions, we have also relayed to the EDPB the concerns and questions that we have solicited from the community.

Additionally, in the Work and Tools section of the EDPB website, the EDPB states that: "We issue general guidance to promote a common understanding of European data protection laws, both across the European Union and around the world. We clarify data protection provisions, advise the European Commission and provide the general public and stakeholders with our interpretation of their rights and obligations. We can issue guidelines, recommendations and best practices about the GDPR and the Law Enforcement Directive, as well as other documents." Accordingly, guidance from the EDPB to ICANN is publicly posted on their website and ICANN's website so that the guidance is available for all interested parties and can help inform the work of the community.

**ICANN org's GDPR Compliance**

1. *Believing that ICANN org has its own GDPR implementation plan in place, it would be helpful for our group to understand the elements and implementation status of the plan so that the Team can draw comparisons to the EPDP Team's work.*

ICANN org has been open and transparent about its work to get ready for GDPR both in terms of domain registration data collected and processed by registrars and registries (which we refer to as "external" GDPR readiness), and personal data processed by ICANN org in the ordinary course of the organization's operations such as finance, meetings, and human resources (which we refer to as "internal" GDPR readiness). ICANN org's plans and activities regarding "external" (domain registration data) GDPR compliance have been openly and transparently blogged and posted on the ICANN Data Protection page at <https://www.icann.org/dataprotectionprivacy [icann.org]>. On 5 June 2018, ICANN's CEO and President, Göran Marby, shared information about ICANN org's "internal" efforts to be GDPR compliant via a blog. In the blog, Göran shared that several of ICANN's policies have been updated. These include an updated online Privacy Policy [icann.org], a revised Terms of Service [icann.org], a revised Cookies Policy [icann.org], a new Notice of Applicant Privacy [icann.org] (relating to data processed for employment applications), and a revised New gTLD Program Personal Data Privacy Statement [newgtlds.icann.org]. Additionally, ICANN org has also rolled out internal changes to the way we handle personal data, from data processing arrangements with vendors to our various personnel policies. Read the full blog here [icann.org].

2. *We have spent most of this meeting exploring the role of compliance at ICANN, in order to support a proposal that ICANN has an implicit contract with the registrant and that therefore 6 1 b applies as a grounds for processing. This would also facilitate ICANN operating a UAM on behalf of those who want the data. It might also explain Goran's initiative in seeking some kind of recognition by EU authorities that ICANN has a kind of quasi-regulator status, as the authority vested with the responsibility to manage the DNS. Given that all of this is outside the current configuration of ICANN as data controller, which would be more clear had we done a DPIA and had we adequate data maps to work with….can we either get back to our Charter questionsthat we were mandated to address by the GNSO, or get a full explanation of what is going on and why we continue to be focused on the access question.*

This request appears to be directed at the EPDP Team and not ICANN org as ICANN org does not dictate the direction of the EPDP Team's discussion.

*3. Why hasn't a Data Protection Impact Assessment been carried out to clarify data flows and ICANN's relationship with the data subject in light of its acknowledged role as a joint controller and Article 35 of the GDPR?*

This question was also asked during the Data Protection/Privacy Update Webinar hosted by ICANN org on 8 October 2018. John Jeffrey, ICANN's General Counsel and Secretary provided the following response:

"This is something that has been considered since the very beginning. One of the issues is when to do that in a way that is most timely and useful and how to do that. We continue to evolve the thinking of how the interpretation of GDPR applies to WHOIS. We have a number of questions which have been addressed directly to the DPAs and the EDPB and we've have an ongoing discussion with the EC about how to interpret the GDPR. We believe that those are a better format at this point than doing the assessment, but we continue to evaluate whether that assessment would be the right thing to do and when."

The presentation for the webinar is posted here, and the Adobe Connect recording is here. The question and response start at 0:27:00 in the Adobe Connect recording.

4. During the 19 September 2018 EPDP Q&A Session with Becky Burr, there was a request for more information regarding what ICANN org does with personal data as it relates to ICANN contractual compliance. Additionally, on 4 October 2018, ICANN org received a question from the EPDP Team regarding data retention procedures. In response to these two items, please see the attached a summary of ICANN org's contractual compliance personal data processing activities: Summary-Contractual-Compliance-Data-Processing-Activities.pdf.

**ICANN Org Liaisons Role**

1. *The Council envisioned, via the EPDP Charter, to have direct participation of ICANN org liaisons, within the EPDP Team. As we leave the Triage and head into substantive detail, do the ICANN liaisons see a role or specific set of actions for ICANN supporting the team?*

Section III of the EPDP Charter describes the role of ICANN org liaisons as "ICANN Staff Liaison: The ICANN Org GDD and Legal Liaisons are expected to provide timely input on issues that may require ICANN Org input such as implementation-related queries. The ICANN Staff Liaisons are not expected to advocate for any position and/or participate in any EPDP Team consensus calls." In line with this description of ICANN org liaisons' role, Göran Marby's response [icann.org] to the GNSO Council regarding a request for appointment of ICANN org liaisons confirmed the scope of participation of the ICANN org liaisons as "Trang Nguyen from ICANN organization's Global Domains Division and Dan Halloran from ICANN's legal team will join the working group's mailing list and the group's calls to coordinate responses to requests for GDD or legal input as needed to support the working group's deliberations. Such requests will ordinarily be responded to in writing, following consultation with internal and external experts as appropriate."

**WHOIS Conflicts with Local Laws**

1. *Has the WHOIS Conflicts with local laws procedure been used and successfully used to date? Please indicate the instances where the procedure was invoked and the outcome. Were any specific issues identified with the use of this procedure?*

The procedure was most recently invoked for .FRL in late 2017. However, the request was withdrawn prior to an outcome when .FRL agreed to comply with the requirements of the Temporary Specification. The request was withdrawn early on in the process so ICANN org had not conducted a formal review to identify specific issues with the procedure.

The procedure was also previously attempted by .FRL in late 2016 but the request did not meet the requirements to utilize the procedure. At the time, requirement to trigger the procedure was that the contracted party must have received "notification of an investigation, litigation, regulatory proceeding or other government or civil action that might affect its compliance." However, .FRL was not subject to any such proceeding at the time, and the procedure could not be used.

**Specification or Policy**

1. *Is the GNSO & the EPDP Team creating a policy or a specification?*

As described in the Charter and the Board resolution that launched this Expedited Policy Development Process, the team's task is to develop policy recommendations.

The starting point for these recommendations is the temporary specification adopted by the Board on 17 May 2018.

The temporary specification includes both high-level principles such as defining purposes and legal bases for processing registration data, and also detailed technical requirements such as descriptions of modifications to the registration data display requirements set forth in the registry and registrar agreements.

The Board does have the ability to adopt both temporary policies and specifications. The exact difference between a "temporary policy" and a "temporary specification" is not defined in the Bylaws or registry/registrar agreements.

Although the GNSO's procedures <https://gnso.icann.org/en/council/procedures> generally discuss developing policy recommendations and not "specification" recommendations, the PDP Manual actually outlines a wide variety of "PDP Outcomes and Processes" one of which is "technical specifications". As noted above, the label that is given may not matter too much as during implementation a further assessment is usually made in relation to how to address each approved recommendation. Any remaining questions about the scope of the team's work or how its deliverables should be structured and styled could be referred to the GNSO council.

**Use of data by ICANN Org**

1. *How does ICANN Contractual Compliance use WHOIS data? For example, in the case of a WHOIS inaccuracy complaint, can ICANN Contractual Compliance retrieve data from escrow, or does ICANN Contractual Compliance typically ask the registrar or the registry operator?*

ICANN Contractual Compliance uses WHOIS data to review WHOIS Inaccuracy complaints and other complaints related to domain management (e. g., Transfers, Unauthorized Transfer, Domain Deletion, Renewals, etc.). Depending on the nature of the complaint, ICANN Contractual Compliance may ask the registrar for relevant data to investigate the complaint. Compliance may also look at the Registry public WHOIS to supplement its review or processing. Compliance does not use escrowed data for complaint processing as it is not one of the conditions for escrow deposits release under the data escrow agreements and ICANN agreements.

2. *Apart from ICANN Org Compliance, do any other ICANN departments require access to registration data and, as such, might require a specific purpose? If so, please describe in detail sufficient to provide a legal basis for such data processing.*

This question seems to be asking about any use by ICANN Org of registration data that is now masked pursuant to the Temporary Specification. One example of an ICANN Org activity that previously used WHOIS data elements that may now be redacted pursuant to the Temporary Specification is the WHOIS Accuracy Reporting System, which is currently under review as discussed with the EPDP Team on 26 September 2018. If additional information is needed it would be helpful if the EPDP Team could please clarify if the question is for information related to such past uses of now-masked registration data, or to any current ICANN Org (apart from Contractual Compliance) uses of non-public data, or to any future uses of non-public registration data that may be needed in order to implement GNSO-recommended policies.

Also, in discussions that the EPDP Team has had regarding purposes, ICANN Office of the CTO (OCTO) has been mentioned. To inform the EPDP Team's continued discussion on this topic, ICANN Org would like to clarify that ICANN OCTO does not require personal data in domain name registration data for its work. For example, OCTO's Domain Abuse Activity Reporting (DAAR) project <https://www.icann.org/octo-ssr/daar> uses only the registrar and nameserver information.

*3. Further input is requested to explore how WHOIS was used before the Temp Spec was adopted, in OCTO's activities. The original Org response does not address that issue. For example, did OCTO use WHOIS in its law enforcement training and outreach activities, or engagement with the cybersecurity community, or to facilitate or respond to large scale botnet attacks, such as Conficker or Avalanche? Individual members may follow up with the CTO for follow up questions, if available at ICANN63.*

Regarding the EPDP Team's follow-up question on how OCTO used WHOIS data for training and outreach activities, prior to the effective date of the Temporary Specification, use of WhOIS data to identify the registrant and the technical data related to a domain name was part of the training materials. The training showed how one could use WHOIS data to attempt to contact a registrant or the hosting provider in cases of compromised machines, etc. Since the Temporary Specification became effective, the training no longer shows one how to use public WHOIS data to contact a registrant, instead as part of the training, a brief overview of where the policy discussions are and how people can get involved in the discussion is provided.

The EPDP Team's follow-up question also asks how OCTO used WHOIS data for engagement with cybersecurity community, or to facilitate or respond to large scale botnet attacks, such as Conficker or Avalanche. Conficker, Andromeda and other large-scale actions are typically managed by the Law Enforcement agencies, not OCTO. OCTO's role in those activities does not involve the use of personal data in WHOIS. Those Law Enforcement agencies would be better placed to discuss their operational procedures and the effect of the Temporary Specification on their operations.

**Data Retention**

1. *With respect to data retention: For how long and why, should data escrow agents retain old deposits (if at all) in order to fulfill their contractually-required obligations? For how long and why, should data be retained by registries and registrars from the perspective of ICANN Org for purpose A (Establish the rights of a Registered Name Holder in a Registered Name and ensuring that the Registered Name Holder may exercise its rights in respect of the Registered Name)?*

Under the Registrar Data Escrow Specification deposits older than one year must be destroyed, unless a longer period is agreed to by the registrar and the escrow agent. Also, under the base agreement for new gTLDs each escrow deposit must be kept for one year. Legacy gTLD agreements vary; for example the .ASIA, .BIZ, .INFO, and .ORG agreements specify that at least four weeks of deposits must be kept. The purpose of safeguarding a set of prior deposits is to protect registrants in the event a registry or registrar fails or is terminated and the database needs to be reconstituted. In situations where the registration database has to be reconstituted and deposits have not been made in a number of months, safeguarding multiple deposits increases the likelihood that at least one reliable deposit will be available. Also, having multiple deposits increases the likelihood that a reliable deposit is available in the event that the compliance/termination process is contested by the registry operator or registrar. Perhaps registry operators and registrars with operational experience could provide input as to how far back deposits should be kept to ensure that registration databases can be reconstituted when needed.

**UDRP/URS**

1. *With respect to ICANN's references to dispute resolution policies within the Temporary Specification, is there a reason only the URS and UDRP were included and not other dispute resolution procedures such as RDDRP, PDDRP and PICDRP?*

The RDDRP, PDDRP, and PICDRP <https://newgtlds.icann.org/en/program-status/pddrp> are dispute resolution procedures where the gTLD registry operators themselves are the respondents. Under the Registrar Transfer Dispute Resolution Policy <https://www.icann.org/resources/pages/tdrp-2016-06-01-en> the respondents are registrars. This is different from URS and UDRP proceedings where individual domain registrants are the respondents. (Note: gTLD registry agreements may also contain other dispute resolution procedures, for example, .NAME has an "Eligibility Requirements Dispute Resolution Policy" <https://www.icann.org/resources/pages/appendix-11-2013-07-08-en>.)

2. *ICANN Org to provide EPDP Team with copy of agreements with UDRP/URS providers in to demonstrate GDPR compliance in relation to data protection / transfer of data including relevant data protection policies that dispute resolution providers have in place.*

ICANN has used Memoranda of Understanding to govern the relationship with each of the selected URS providers, in which each of the URS providers agree to implement the URS services in accordance with the procedures laid out in the New gTLD Applicant Guidebook, as they might be amended from time to time. Copies of the MOUs are available here: https://newgtlds.icann.org/en/applicants/urs. ICANN does not have agreements or MOUs with UDRP providers. Additional discussion on why ICANN has taken this approach with UDRP providers is available here: https://www.icann.org/en/system/files/files/uniformity-process-19jul13-en.pdf.

In light of the recent changes in data protection laws and the requirements in the Temporary Specification requiring contracted parties to give full registration data to the dispute resolution providers when presented with a complaint if the contact details are not published in WHOIS, ICANN is in discussions with the dispute resolution providers to more fully understand the safeguards they have put in place for the processing of personal data. For example, WIPO has updated its FAQ page concerning the GDPR as it relates to the UDRP: http://www.wipo.int/amc/en/domains/gdpr/, and other providers have reviewed/are in the process of reviewing their supplemental rules in light of changes in privacy laws. ICANN will publish any updates to a provider's supplemental rules on its website.

**Admin/Tech Contact**

1. *For which ICANN policies is admin/tech contact information currently a required data element and/or referenced in the policy?*

Administrative and technical contact information is referenced in the following ICANN policies and procedures:

- Registry Registration Data Directory Services Consistent Labeling and Display Policy. Output requirements for administrative and technical contact information.
- Thick WHOIS Transition Policy for .COM, .NET, .JOBS. Guidance to registry operators for handling output of administrative and technical contact information where no data exists in the SRS during the period when registrars begin sending Thick WHOIS data to registry operators for all new registrations.
- Rules for Uniform Domain Name Dispute Resolution Policy. Notifications of complaints include administrative and technical contacts information.

- WHOIS Data Reminder Policy. WDRP notices may be presented to the registrant either directly or through the administrative contact.
- Transfer Policy. Administrative contact along with the registered name holder have the authority to approve or deny a transfer request. Because of this role, the administrative contact is referenced in parts of the transfer process as well as in the Registrar Transfer Dispute Resolution Policy.
- Uniform Rapid Suspension System (URS) Rules. Notifications of complaints include administrative and technical contacts information.

**Input from ICANN Compliance**

**Contractual Compliance responses to EPDP_25jan19.pdf**

**Summary-Contractual-Compliance-Data-Processing-Activities.pdf**

**OUTSTANDING QUESTIONS**

1. Is indemnification provided by ICANN through a joint controller agreement an option? If EPDP agrees on policy that requires ICANN to indemnify, would the ICANN legal team and Board oppose it?

2. When will the ICANN be released memorandum concerning the roles and responsibilities in processing data. The EPDP team encourages ICANN to issue the memo within 48 hours so its position can be referenced in the Initial Report.