EPDP Phase 1 Recommendation 27: Registration Data Policy Impacts

Wave 1 Report

ICANN org
18 February 2020

TABLE OF CONTENTS

Executive Summary

ICANN org has performed a detailed review of each existing policy and procedure listed in this document to create an inventory of the areas impacted by the EPDP Phase 1 policy recommendations. This report provides an analysis of the impacted areas identified as well as potential changes to address the impact, which are summarized below under each policy and procedure reviewed. Impacts may include outdated provision language (e.g., references to administrative contact requirements), higher-level issues such as the relevance or inconsistency of an existing policy or procedure with the new Registration Data Policy, or implications for existing contractual provisions. Where there are no impacts identified for an item, this is also noted for completeness.

This draft report was presented and reviewed with the EPDP Phase 1 Implementation Review Team currently working with the organization on implementation of the policy recommendations, for completeness and validation of the proposed paths for the items included in this report. During this review step, the IRT did not identify any issues with the proposed paths or additional items to be added to the inventory. As the IRT review period did not result in any changes or updates to this report, it is being submitted to the GNSO Council who will then determine next steps.

This report includes 15 policies or procedures, including all consensus policies currently in effect. Through this analysis, some have been identified as substantively affected, while others are affected in one area, about half have little to no impact. Based on this analysis, these items can be put in buckets as follows:

High	Medium	Low
Registry Registration Data Directory Services Consistent Labeling and Display Policy	Expired Domain Deletion Policy (EDDP)	AGP Limits Policy
Thick RDDS (Whois) Transition Policy for .COM, .NET and .JOBS	Whois Data Reminder Policy (WDRP)	Additional Whois Information Policy (AWIP)
Transfer Policy		Expired Registration Recovery Policy (ERRP)
Uniform Domain Name Dispute Resolution Policy (UDRP) and Rules		Protection of IGO and INGO Identifier in All gTLDs Policy
Uniform Rapid Suspension (URS)		Registry Services Evaluation Policy (RSEP)
		Restored Names Accuracy Policy (RNAP)
		Revised ICANN Procedure for Handling WHOIS Conflicts with Privacy Law
		Whois Marketing Restriction Policy

The work plan contemplated a triage step in which each of the items identified would be allocated to a Generic Names Supporting Organization (GNSO) process, an implementation-related update, or a procedure to address contractual matters. Overall, the majority of Wave 1 items appear to be within the remit of the GNSO. Each of the items in this report is either consensus policy or, in case of URS, already being considered in a policy development process (PDP).

1 Introduction

The Expedited Policy Development Process (EPDP) team on the Temporary Specification for gTLD Registration Data delivered its Phase 1 recommendations in February 2019 and 27 of the 29 recommendations contained within the Report were adopted by the ICANN Board in May 2019. In parallel with the EPDP Team's Phase 2 work, ICANN org is working with

the Implementation Review Team (IRT) to draft the new consensus policy (the gTLD Registration Data Policy) based on Phase 1 policy recommendations.

As a number of existing policies and procedures touch on registration data, it is expected that many of these will be impacted by the recommendations being implemented. The EPDP team's Recommendation 27 specifies an initial list of impacted policies with potential anticipated modifications based on these impacts. Consistent with Recommendation 27, the Board directed ICANN org to work with the IRT to examine and report on the extent to which the EPDP Team's policy recommendations require modification of existing consensus policies.

During the ICANN65 in June 2019, ICANN org facilitated the first face-to-face meeting of the IRT and discussed the stages of the Registration Data Policy implementation as well as the implementation process for the recommendations. In addition, the GNSO co-sponsored, with other interested community groups, a cross-community session on the impacts of the new EPDP Phase 1 recommendations on other existing ICANN policies and procedures. A preliminary list of impacted policies and procedures was shared at this session, where the community engaged in a substantive discussion on issues such as expected impacts on various existing policies and procedures, and how to prioritize the review of such policies and procedures.

As part of the planning for the implementation of the EPDP Phase 1 recommendations, ICANN org also prepared a draft work plan (see Annex 1) to address Recommendation 27, which was shared with the GNSO Council and the IRT in August 2019. At the GNSO Council meeting in September 2019, ICANN org provided an update to the Council on the plan and status of its work to date on this recommendation. The work to identify and categorize the impacted items is planned to occur in three parts: 1) Inventory, 2) Review, and 3) Triage. This report is an output of the inventory work; the following stages are described in section 4, Next Steps, below.

ICANN org has performed a detailed review of each affected policy and procedure, and identified the impacted areas included in this report. It is important to note that this inventory will be completed in two waves, based on priority. The items identified may be at multiple levels (i.e., language level and issue level) and include a preliminary recommendation on appropriate path. This draft report is being presented and reviewed with the IRT for completeness and validation of the proposed paths for each item.

2 Report Structure and Methodology

This report provides an analysis of the impacted areas identified as well as potential changes to address the impact, which are summarized below under each policy and procedure reviewed. Each of these contains a brief summary of the policy or procedure and the key findings of ICANN org's review. Impacts may include outdated provision language (e.g., references to administrative contact requirements), higher-level issues such as the relevance or inconsistency of an existing policy or procedure with the new Registration Data Policy, or implications for existing contractual provisions. Where there are no impacts identified for an item, this is also noted for completeness. Where policies are materially affected, there may be a distinction between cases where policy principles may remain in place but rules/methodology may need to change to meet them and cases where the policy principles themselves may be considered for changes.

Throughout the time period of this analysis, ICANN org has worked with the IRT to draft policy language based on the EPDP's Phase 1 policy recommendations. This working draft is expected to become an implemented policy entitled "Registration Data Policy." Where the term "Registration Data Policy" is used throughout this analysis, this refers to the policy recommendations as reflected in the policy language draft in progress. Because this draft is dynamic, however, it may be helpful to review and confirm the conclusions in this report to identify any updates at the time a complete policy draft is available.

Recommendation 27 anticipated updates to policies and procedures affected by the new Registration Data Policy. While this report is primarily focused on policies, the follow-up to this report, Wave 2, will cover the relevant (non-policy) procedures.

It is also noted that Phase 2 of the EPDP is in process as of this report, and that policy recommendations resulting from this work may also impact existing policies and procedures. Analysis of such impacts, where relevant, would follow from issuance of the Phase 2 recommendations and are outside the scope of this report.

3 Analysis

ICANN org has attempted to be as comprehensive as possible in its analysis. A cross-

functional team reviewed each of these policies and procedures in detail and sought additional subject matter expertise or clarification from within the organization where needed.

The scope of the review to support the EPDP's recommendation 27 is to identify the impact of the policy recommendations rather than identifying questions or changes in other areas. Thus, if the policy recommendations are silent on an item, no changes are proposed. However, the report does, in some cases, identify technical or logistical points that may be useful should the GNSO undertake a broad policy discussion on a particular policy.

There are some areas of overall impact that appear in multiple policies and procedures or appear to be generally applicable. These include:

1. Use of the term "Whois." This terminology appears in several existing policy names, policy requirements, and sections of explanatory language, and is used variously to refer to a protocol, a service, and a database. As the ICANN community is in the process of phasing out the Whois protocol and moving to the Registration Data Access Protocol (RDAP), on top of the changes to requirements for registration data processing by contracted parties, the document throughout the report suggests replacing references to "Whois" with "Registration Data," "Registration Data Directory Service," or another term according to what is relevant, to be more precise as to definition and remain generic as to the protocol.

2. Similarly, many policies and procedures make reference to "Whois data" which typically had a particular meaning relating to the published Whois records associated with a particular domain name. In considering how such requirements carry over to the new policy environment, the analysis relies on the definition of "Registration Data" in section 2 of the Temporary Specification, namely, "Registration Data" means data collected from a natural and legal person in connection with a domain name registration.

3. The analysis considers that Whois and RDAP services[1] will operate in parallel until such time as sunset of Whois services offered by gTLD registries and registrars. The EPDP Phase 1 Report provides that: "While the exact date of the possible elimination of WHOIS requirements will be determined in the policy implementation

[1] RDAP service is required for all gTLD registries and registrars as of 26 August 2019. See https://www.icann.org/en/system/files/files/registrar-legal-notice-implementation-rdap-service-27feb19-en.pdf

phase, the EPDP Team notes any current WHOIS requirements negated or made redundant by eventual policy recommendations will no longer be required." The analysis in this report seeks to focus on the policy requirements and how they should be examined or clarified irrespective of which protocol is being used for services associated with registration data.

3.1 AGP (Add Grace Period) Limits Policy

Policy Summary: This policy was developed to limit the behavior known as domain tasting through modifications to the Add Grace Period process. Under this policy, a registry operator does not refund fees to a registrar who exceeds a defined threshold percentage of names deleted during the Add Grace Period.

Estimated impact: Low

Key Points: ICANN org has not identified any substantive impact on the existing requirements of this policy.

Analysis:

1. In the policy section titled "Effect on Registrars," the "Exemption Requests" section provides that a registry operator can require additional information from a registrar to process an exemption request. To the extent this involves personal data associated with a domain name, this requirement may be subject to separate arrangements between the registry and registrar regarding the processing of personal data.

3.2 Additional Whois Information Policy (AWIP)

Policy Summary: The purpose of this policy is to clarify the meaning of the EPP status codes in Whois data and require the consistent identification of registrars by their GURID in Whois.

Estimated impact: Low

Key Points: ICANN org has not identified any substantive impact on the existing requirements of this policy; however, some language changes may be considered and

technical questions addressed to continue these policy requirements as RDAP continues to be deployed.

Analysis:

1. An update to the name of the policy may be considered as title includes “Whois,” which may not remain necessary. Other terminology references to “Whois output” and “Whois data” throughout the text may also be considered for updates, for example, section 1(c), "For more information on Whois status codes, please visit https://icann.org/epp".

2. The AWIP requires that RDDS output include a link to an ICANN org web page defining the respective EPP status codes for a domain name registration (“EPP Status Codes | What Do They Mean, and Why Should I Know?”). The existing page contains an RDAP status mapping for each EPP status code. Accordingly, no changes appear necessary to the requirement to include this link in RDDS output, and, as the status codes do appear in such output under the Registration Data Policy, the requirement to include this reference is still relevant.

3. The opening paragraph of the AWIP includes a reference to existing contractual requirements to “provide query-based access to certain registration data via web pages and at port 43.” This language remains accurate until such time as requirements for Port 43 and web-based Whois service are sunset. However, this language does not affect any policy requirement.

4. AWIP section 1 specifies that “Registrars and registries who include domain name registration statuses in Whois output” must follow the requirements enumerated in the policy. The footnote provides that “This requirement is not intended to require any registrar or registry to include domain name statuses in its Whois output if it is not already obligated to do so. But for those registrars and registries who do include a domain's status in Whois, the status must be in the form of the respective EPP code and conform to the other requirements of this policy.” This appears to be a remnant as when the AWIP went into effect, there were still registrars operating under the 2009 RAA which did not require display of statuses. ICANN org did not identify any registry or registrar not currently required to display domain name statuses in Whois output; accordingly, the footnote may not be necessary.

5. There is an additional technical consideration to applying this policy in RDAP. The protocol does not currently support inclusion of a hyperlink in each status field; rather, a hyperlink can be included at the object level (e.g., domain object, contact object). This can be addressed by (a) adjusting the language of the policy to include the hyperlink reference to the status codes definition page in a single place rather than multiple places, or (b) developing an RDAP extension. Approach (a) is reflected in the current gTLD RDAP Profile; however, adherence to this profile is a recommendation but not a requirement for contracted parties.

3.3 Expired Domain Deletion Policy (EDDP)

Policy Summary: This policy covers various registrar practices for deletion of a domain name registration where a registrant has not renewed.

Estimated Impact: Medium

Key Points: The requirements of this policy were incorporated into the 2009 RAA and have been carried over verbatim in the 2013 RAA (Section 3.7.5). One provision of this policy may be impacted by the new Registration Data Policy requirements.

Analysis:

1. EDDP section 3.7.5.7 references "WHOIS contact information" and the "WHOIS entry." The context of this provision is a requirement that, if a registration expires during a UDRP proceeding, the complainant has the option to renew or restore the registration on the same commercial terms as the registrant. Where this occurs, the EDDP requires that the registrar (a) place the registration in Registrar HOLD and Registrar LOCK[2] statuses, (b) remove the registrant contact information from the WHOIS, and (c) include a message in the WHOIS output that the registration is subject to a dispute resolution proceeding.

[2] If updates to this policy are considered as a result of GNSO policy work, these statuses may be updated to the Extensible Provisioning Protocol (EPP) statuses Client Hold and Client Update Prohibited.

Under the new Registration Data Policy, as there may be no registrant contact information that is publicly displayed, the registrar may not need to take any action to remove the contact information from publicly available data. However, in the event that there is any such registrant contact information being displayed (for example, where processing is not subject to GDPR or as a result of the registrant's consent), the current requirement would apply and that data would be removed. In addition, for non-public data, the registrar should also update its (non-public) registration data to remove the registrant information and indicate the pendency of a dispute resolution proceeding. This section may benefit from some clarification to indicate how these requirements apply under the Registration Data Policy.

The requirements to update the status of the registration and to indicate in the publicly available data that the name is subject to a dispute are unaffected. However, additional guidance may be required on what and where to display this message in RDDS output, for example, if the Registration Data Policy requires a "Redacted for Privacy" notation and the EDDP requires a notation that the name is subject to a dispute proceeding. Note that RDAP is able to support multiple notations in an output.

ICANN org notes that this provision is occasionally invoked to keep a registration active during a dispute resolution proceeding. If changes are considered to this policy as a result of GNSO policy work, it may be beneficial to apply this option to URS cases also.

2. The EPDP Team's Phase 1 recommendations do not address at which point in the cycle of expiration, deletion, and grace periods a data subject's consent for use of their personal data associated with the registration of a domain name would cease to apply, or where the purpose of such data processing runs out. This may be useful as a policy discussion.

3.4 Expired Registration Recovery Policy (ERRP)

Policy Summary: The Expired Registration Recovery Policy is intended to help align registrant expectations with registrar practices by establishing certain minimum communications requirements, making renewal and redemption of registrations uniformly

available in prescribed circumstances, and through the creation and promotion of registrant educational materials.

Estimated Impact: Low

Key Points: ICANN org has not identified any substantive impact of the Registration Data Policy on the ERRP.

Analysis:

1. ERRP section 2.1 requires the registrar to send notices to a registrant in advance of expiration of a domain name registration. No change appears to be needed to this requirement.

2. ERRP section 2.2 requires interruption to the resolution path of a domain name. No change appears to be needed to this requirement.

3. ERRP section 3.2 references "Whois result;" a language change to this may be considered. The context of this provision is a requirement for the registry operator to clearly indicate in its Whois result for the registration that it is in its Redemption Grace Period. The language of this provision may be updated to phase out the reference to Whois; however, the requirement for the RDDS output to show that a registration is in Redemption Grace Period status is still relevant as, under the Registration Data Policy, domain statuses are included in the fields to be published by the registry operator.

4. ERRP section 4.2.1 references the Administrative Contact. The context of this provision is a requirement that registrars describe on their websites the contact methods they use to deliver the pre- and post-expiration notifications described in the policy. "Telephone call to administrative contact" is one of the examples; however, this example can be eliminated without impact to the policy requirements.

5. The ERRP section titled Suggested Best Practices notes that registrars should advise registered name holders to provide a secondary email point of contact that is not associated with the domain name itself so that in case of expiration, reminders can be delivered to this secondary email point of contact (e.g., if the expired domain name is <example.org>, and the contact is <registrant@example.org>, the message

may be undeliverable. The Registration Data Policy does not prohibit a registrar from seeking a secondary email address from a registrant subject to its applicable requirements for processing such data. This allows the registrar to contact a registrant if the primary email address is based on the same expired domain name. As this point concerns a best practice, it does not impact the requirements of the ERRP.

6. The ERRP section titled Time for Coming into Compliance provides milestones by which registrars must send notices after the effective date of the ERRP. If changes are considered to this policy as a result of GNSO policy work, this section may be eliminated as obsolete.

Cross reference: ERRP section 4.3.1 references the Whois Data Reminder Policy (WDRP). The context of this provision is a requirement for registrars to incorporate links to educational materials if published by ICANN, in communications including the annual WDRP notices sent to registrants.

Cross reference: Recommendation 9 of the Final Report on the Privacy & Proxy Services Accreditation Issues (PPSAI) PDP suggests best practices for accredited P/P service providers and references the ERRP. Specifically, "P/P service providers should facilitate and not obstruct the transfer, renewal or restoration of a domain name by their customers, including without limitation a renewal during a Redemption Grace Period under the ERRP and transfers to another registrar." The Privacy & Proxy Services Accreditation Issues policy recommendations are being analyzed as part of Wave 2 of the Recommendation 27 analysis.

3.5 Protection of IGO / INGO Identifiers in All gTLDs Policy

Policy Summary: This policy relates to protection at the top and second level for specific Red Cross, IOC and IGO names (with an Exception Procedure to be designed for the relevant protected organizations), protection at the top level for specific INGO names and a 90-day Claims Notification process at the second level for certain other INGO names. The policy provides requirements for contracted parties with respect to second-level DNS labels and requirements relating to the delegation of protected gTLD strings.

Estimated Impact: Low

Key Points: ICANN org has not identified any substantive impact of the Registration Data Policy on the existing requirements of this policy.

3.6 Registry Registration Data Directory Services Consistent Labeling and Display Policy (CL&D)

Policy Summary: The goal of the RDDS Consistent Labeling and Display Policy is to align the way registries and registrars label and display registration data outputs.[3] This policy specifies the format for responses to domain name queries.

Estimated Impact: High

Key Points: This policy is substantively impacted by the new Registration Data Policy requirements, indicating a need for additional consideration of the policy's data publication requirements and means to enable consistency among registries.

Analysis:

1. The format specified by CL&D for published registration data will not be possible under the requirements of the new Registration Data Policy, based on the following:
    a. Section 7 requires a registry operator to use a "Registry Admin ID" key in responses to a domain name object query. Under the Registration Data Policy, Administrative Contact data is no longer collected or transferred from a registrar to a registry operator.
    b. Section 10 notes that a registry operator that is permitted to provide redacted RDDS output in its registry agreement[4] may treat certain fields as optional. In some cases, redaction of these fields is specified in the Registration Data Policy, and in others, such as the Administrative Contact fields, these fields

[3] This policy was part of the same set of policy recommendations as the Thick Whois Transition Policy, which recommendations noted that "The provision of thick Whois services, with a consistent labelling and display as per the model outlined in specification 3 of the 2013 RAA, should become a requirement for all gTLD registries, both existing and future."

[4] The .CAT, .NAME, and .TEL registry agreements currently permit the registry operator to provide redacted information in response to domain name RDDS queries.

will no longer be required to be collected or transferred from the registrar to the registry operator. This section may be removed or updated to align with the Registration Data Policy language.

c. Section 11 specifies that the fields for Registry Admin/Tech/Billing/Registrant ID refer to the Repository Object Identifier (ROID) for the contact object as specified in RFC 5733. The Admin ID may be eliminated as administrative contact information will no longer be collected or transferred from the registrar to the registry operator. It is also noted that not all gTLD registry operators currently use a Registrant ID field, and implementing this may involve a transition period. Under the Registration Data Policy, the Registry Registrant ID field is required to be transferred by the registry operator to a data escrow agent (per EPDP Recommendation 8), and may be required to be published or to be redacted with the opportunity for a registrant to consent to its publication (per EPDP Recommendation 10).

d. In regard to ROID, per RFC 5733, the ROID is "a <contact:id> element that contains the desired server-unique identifier for the contact to be created." EPDP Recommendation 5 does not specify the Registry Registrant ID as a data element to be collected or generated. As the Extensible Provisioning Protocol (EPP) requires this information to create a contact, current implementation language for the EPDP Phase 1 recommendations includes the notation that "nothing in this policy changes the collection of the following data elements required by EPP: <contact:id> (Registry Registrant ID, Registry Tech ID), <contact:authInfo>, <contact:city>, <contact:cc>" For the registrar to display this, it must be transferred from the registry.

2. The CL&D policy includes some references to Whois, including:

   a. The opening paragraph notes that registry operators (with the exception of .com, .jobs and .net) shall implement the requirements of the policy in conjunction with the registry agreement or subsequent amendments thereto "in order to comply with WHOIS (available via port 43) and web-based directory services requirements." This language remains accurate until such time as requirements for Port 43 and web-based directory service are sunset.

   b. CL&D section 7 requires display of a key for the "Registrar WHOIS Server." This may be advisable to change" to "Registrar RDDS Server."

   c. The CL&D section titled "Implementation Notes" describes example outputs for the query objects. The example output includes the key-value pair: Registrar WHOIS Server: whois.example-registrar.tld." This example may

need to be replaced with an RDAP server.

3. If changes are considered to this policy as a result of GNSO policy work, it may be beneficial to define to what extent the same type of consistency in labeling and display reflected in this policy remains the goal or should be adjusted. It should be noted that, according to the Registration Data Policy, both registry and registrar publication of data for individual registrations may differ on the basis of conditional policy requirements, (e.g., fields specified in the policy as MUST publish IF collected), differentiation geographically or on the basis of a legal or natural persons classification, and consent of the data subject for publication of certain data fields. The format of the display output for published registration data is impacted by the Registration Data Policy; however, some types of consistency are still possible. If the policy goal of the desired type and nature of consistency in labeling and display can be reviewed and defined, next steps can follow by determining the best means by which this can be accomplished, e.g., updates to the CL&D policy language to conform to the EPDP Team's Phase 1 recommendations, including a specified format in the new Registration Data Policy, requirements in an updated RDAP Profile, or other means.

   As all policies are being considered in light of current Whois-based systems as well as RDAP, it should be noted that the current gTLD RDAP Profile does not support the requirements of the Registration Data Policy. Drafting updates to the profile in parallel with the drafting of the policy language can help streamline the implementation work for all parties. It should also be noted that the current gTLD RDAP Profile is a recommendation rather than a requirement for registries and registrars and, to enable ICANN org to enforce a specific profile, these will need to become requirements. A negotiation process is under way for amendments to incorporate contractual requirements for the Registration Data Access Protocol (RDAP) into the Registration Data Directory Services. See https://www.icann.org/en/system/files/correspondence/marby-to-bunton-21oct19-en.pdf for more information.

Cross-reference 1: CL&D contains an exception for the registry operators of the .COM, .JOBS, and .NET top-level domains, noting that "the Registry Operators of .com, .jobs and .net are expected to be required to implement the requirements set forth in this Policy as part of their transition from thin to thick registries pursuant to the implementation of the Thick Whois GNSO PDP Recommendations adopted by the ICANN Board on 7 February 2014."

Cross-reference 2: CL&D section 2 references the "Advisory: Clarifications to the Registry Agreement, and the 2013 Registrar Accreditation Agreement (RAA) regarding applicable Registration Data Directory Service (Whois) Specifications" published on 12 September 2014 and last updated on 25 May 2018. The context of this provision of the policy is to note that the Registrar Registration Expiration Date and Reseller fields are optional and should be treated as described in the Advisory. The Registrar Registration Expiration date field is not referenced in the current version of the Advisory. Section 50 of the current version of the Advisory provides that the registrar has the option to exclude the field or leave the value blank; however, if shown, the value of the field must be the name of [the] organization, in case the Reseller for the name is a legal entity, or a natural person name otherwise.

3.7 Registry Services Evaluation Policy

Policy Summary: This policy provides for ICANN org to evaluate a proposed Registry Service for potential significant security, stability, and competition issues. gTLD Registry Agreements identify the RSEP process as the mechanism for a gTLD registry operator to submit a request to ICANN organization to add a proposed service, modify an existing service, or remove an existing service.

Estimated Impact: Low

Key Points: ICANN org has not identified any substantive impact on the existing requirements of this policy.

3.8 Restored Names Accuracy Policy (RNAP)

Policy Summary: This policy provides that when a domain name registration is deleted on the basis of submission of false contact data or non-response to registrar inquiries, if a registrar restores the name from the Redemption Grace Period, the name must be placed on Registrar Hold status[5] until the registrant has provided updated and accurate contact data. The policy recommendations for this policy noted that: "the purpose of this policy is to make

5 If updates to this policy are considered as a result of GNSO policy work, the REGISTRAR HOLD status may be updated to the Extensible Provisioning Protocol (EPP) status Client Hold.

sure that the redemption process cannot be used as a tool to bypass registrar's contact correction process."

Estimated Impact: Low

Key Points: These requirements are built into RAA Whois Accuracy Specification Sections 4 and 5. ICANN org did not identify any substantive impacts on this policy.

Analysis:

1. The RNAP references the data accuracy obligations of registrars in cases where names are deleted and restored. Per the EPDP Team's Phase 1 recommendation 4, "requirements related to the accuracy of registration data under the current ICANN contracts and consensus policies shall not be affected by this policy." The RNAP may accordingly remain in place without changes.

2. The policy requires names restored during the Redemption Grace Period after having been deleted for submission of false contact data or non-response to registrar inquiries to be placed in "Registrar Hold" status. If changes are considered to this policy as a result of GNSO policy work, this reference may be updated to the EPP status "Client Hold."

3. Given that the RNAP requirements are incorporated into the Registrar Accreditation Agreement, it may be advisable to keep the policy in place and document that it has been incorporated into the agreement and that any subsequent contractual negotiations to change the agreement should not overwrite the consensus policy.

4. ICANN org identified a potential corner case of overlap among policies. If a domain name's registration data (containing Administrative and Technical contact data) was accurate before the effective date of the new Registration Data Policy, but later deleted due to inaccuracy (e.g., the information changed and the registrant did not update it or respond to the registrar requests), after the effective date of the Registration Data policy, then when the name is restored with the new data provided, this data would conform with the dataset requirements under the new policy (without the Administrative or Technical contacts).

3.9 Revised ICANN Procedure for Handling Whois Conflicts with Privacy Law

Policy Summary: This policy allows ICANN and contracted parties (both ICANN-accredited registrars and gTLD registries) to demonstrate when they are prevented from complying with contractual obligations to collect, display, or distribute registration data because of a conflict with other legal obligations, namely, local or national laws.

Estimated Impact: Low

Key Points: This procedure is based on GNSO policy recommendations and advice on a procedure for handling conflicts between a registrar/registry's legal obligations under privacy laws and their contractual obligations to ICANN. The procedure was revised in April 2017 following the work of an Implementation Advisory Group (IAG), and the GNSO has pending additional work related to it.[6] The procedure does not appear to be substantively impacted by the new Registration Data Policy requirements; however, there are several instances where terminology could be updated.

Analysis:

1. This procedure appears to remain applicable under the new Registration Data Policy, as there remains potential for a gTLD registry or registrar to be subject to a law that may raise a potential conflict with its obligations under the policy.

2. If changes are considered to this policy as a result of GNSO policy work, for consistency with other policies, it may be useful to consider the following updates:
    a. adding a definitions section with relevant terms referenced in the gTLD Registration Data Policy.
    b. to the extent the section titled Introduction and Background is retained, updating the text to describe the background, history, and rationale for changes to the procedure.
    c. the name of the procedure and references to Whois throughout, e.g., “Whois Proceeding.”

[6] At its 13 March 2019 meeting, the GNSO Council agreed to defer further discussion for 12 months but reserved the right to revisit the deferral period at any time.

3. Feedback from some stakeholders in June 2019 during an ICANN65 session questioned whether this procedure was the right instrument to solve a problem, or suggested that the lack of use of the procedure was an indication it had not met its policy objectives. The GNSO may wish to consider this feedback in determining next steps.

3.10 Thick Whois Transition Policy for COM, NET, JOBS

Policy Summary: This policy requires that all new domain name registrations must be submitted as "thick" registrations as of a certain date, and those gTLD registry operators currently providing "thin" WHOIS services must support "thick" data for all new registrations as of a certain date. These registries must also migrate all existing domain name registrations to a thick format, which transition is to occur according to a set schedule. While this policy is in effect, its enforcement is deferred pending specified milestones in implementation of the Registration Data Policy.

Estimated Impact: High

Key Points: This policy was part of the same set of policy recommendations as the CL&D Policy, which noted that "The provision of thick Whois services, with a consistent labelling and display as per the model outlined in specification 3 of the 2013 RAA, should become a requirement for all gTLD registries, both existing and future." As described above, if the goal is to define a standard minimum data set across all gTLDs, this may be accomplished via the new Registration Data Policy or other means. If this can be achieved, there may not be a need for a policy aimed at specific registries.

Analysis:

1. The new Registration Data Policy does not use the terms "thin" and "thick" data. Rather, the policy defines data elements to be collected, transferred, and published. The Thick Whois Transition Policy Section 2 references Thin and Thick definitions, which may be eliminated if there is no need for a distinction among these types of registries.

2. The Thick Whois Transition Policy, section 4, Registry Operator Requirements, notes that, for a period of time, if no data exists in certain fields for existing registrations,

these may be treated as optional. The context appears to refer to both transfer and publication, though this is not explicitly stated. Under the new Registration Data Policy, there is a different set of data elements transferred from registrar to registry than is displayed by the registry. If these policy requirements are carried over, this clause should eliminate all Administrative Contact data elements and clarify the requirements for the other elements listed.

3. As noted in the EPDP Team's Phase 1 recommendation 12, it is not contemplated that there will be a means for transfer of consent from registrar to registry. Accordingly, in cases where registries require certain data elements, this transfer could only occur on a legal basis other than consent of the data subject. The result would be that the outputs of various registries would look different based on the registry operator's determinations.

4. A key foundation of this policy is the migration of records to occur over time. It is expected that all gTLD registry operators will be required to make changes to their systems to support the updated requirements for the Registration Data Policy, for new and existing registrations. This transition may take different forms depending on the previous requirements each registry operator was following.[7] This policy addresses the specific case of what is necessary for transitioning registrations from a "thin" to a "thick" format. If changes are considered to this policy as a result of GNSO policy work, a foundational question is whether a policy is needed to deal with the specific case of com and net registrations under the new Registration Data Policy.[8]

Cross-reference 1: Section 4.8 references the CL&D Policy. This provision notes that Registry Operator MAY implement the requirements of the CL&D Policy by a date certain.

Cross-reference 2: Section 4 of the policy references the "Advisory: Clarifications to the Registry Agreement, and the 2013 Registrar Accreditation Agreement (RAA) regarding applicable Registration Data Directory Service (Whois) Specifications" published on 12 September 2014 and last updated on 25 May 2018. The context of this provision is to note

[7] It may be useful for the IRT to discuss whether a similar set of phased implementation milestones is appropriate for the Registration Data Policy.

[8] The policy is titled Thick Whois Transition Policy for COM, NET, JOBS. The .JOBS TLD has already transitioned to the requirements of this policy. See output at http://webwhois.nic.jobs/webwhois-ui/index.jsp

that, between certain dates, where no data exists for certain fields in existing registrations, the registry operator may treat these fields as optional as described in the Advisory.

3.11 Transfer Policy

Policy Summary: This policy aims to provide a straightforward procedure for domain name holders to transfer their names from one ICANN-accredited registrar to another should they wish to do so. The policy provides standardized requirements for registrar handling of transfer requests from domain name holders. The policy also includes procedures covering a change of registrant where a registration remains with the same registrar.[9]

Estimated Impact: High

Key Points: This policy is substantively affected by the new Registration Data Policy requirements. Some areas identified have been addressed by the EPDP Phase 1 recommendations. It is also noted that the GNSO has work in progress to review the Transfer Policy.

Analysis:

1. Transfer Policy section I.A.1.1 provides that either the Registrant or the Administrative Contact can approve or deny a transfer request. Under the

[9] This policy is subject to Supplemental Procedures of the Interim Registration Data Policy for gTLDs, including provisions that:

- Until such time when the RDAP service (or other secure methods for transferring data) is required by ICANN to be offered, if the Gaining Registrar is unable to gain access to then-current Registration Data for a domain name subject of a transfer, the Gaining Registrar is not required to obtain a Form of Authorization, in which case the Registrant must independently re-enter its registration daata with the Gaining Registrar. In such instance, the Gaining Registrar is not REQUIRED to follow the Change of Registrant Process as provided in Section II.C. of the Transfer Policy.
- Registrar and Registry Operator SHALL follow best practices in generating and updating the "AuthInfo" code to facilitate a secure transfer process.
- Registry Operator MUST verify that the "AuthInfo" code provided by the Gaining Registrar is valid in order to accept an inter-registrar transfer request.

Registration Data Policy, Administrative Contact data is no longer collected by the registrar. Accordingly, the registrant would be the only authorized transfer contact.

2. Transfer Policy section I.A 2.1, Gaining Registrar Requirements, relies on the specification of transfer authorities in section 1.1, defining either the Registrant and Administrative Contact as a "Transfer Contact." Given that Administrative Contact data is no longer collected by the registrar, there may not be a need for "transfer contact" terminology, but such references can be replaced by "registrant" as the registrant is the only valid transfer authority. "Transfer Contact" terminology is referenced in part I (A) of the policy in sections 2.1, 2.1.1, 2.1.2, 2.1.2.1, 2.1.3.1(b), 2.1.3.3, 2.2.1, 3.2, 3.3, 3.6, 3.7.4, and 4.1.

3. Transfer Policy section I.A.3 enumerates the reasons a registrar of record may deny a transfer. These include section 3.7.2, "reasonable dispute over the identity of the Registered Name Holder or Administrative Contact." The Administrative Contact reference may be eliminated as the Administrative Contact data is no longer collected by the registrar. Section I.A.3 also enumerates the reasons a registrar of record may not use to deny a transfer request. These include section 3.9.2, "no response from the Registered Name Holder or Administrative Contact." The Administrative Contact reference may be eliminated as the Administrative Contact data is no longer collected by the registrar.

4. Transfer Policy section I.A.4.6.5 provides that both registrars will retain correspondence in written or electronic form of any Transfer Emergency Action Contact (TEAC) communication and responses, and share copies of this documentation with ICANN and the registry operator upon request. This requirement does not appear to be affected by the new Registration Data Policy, which provides for retention of data elements for a period of 18 months following the life of the registration.

5. Transfer Policy section I.A.5.6 provides that the "AuthInfo" codes must be used solely to identify a Registered Name Holder, whereas the Forms of Authorization (FOAs) still need to be used for authorization or confirmation of a transfer request, as described in Sections I.A.2, I.A.3, and I.A.4 of the policy. Where registrant contact data is not published, and absent an available mechanism for the Gaining Registrar to obtain such contact data, it is not feasible for a Gaining Registrar to send an FOA to the registrant contact data associated with an existing registration, as required by

the policy. However, the requirement for the Registrar of Record to send an FOA confirming a transfer request (covered in section I.A.3) is still achievable as the registrar does not need to rely on publicly available data.

6. Transfer Policy section II.B.1, Availability of Change of Registrant, provides that "Registrants must be permitted to update their registration/Whois data and transfer their registration rights to other registrants freely." This language may be updated to clarify what updating registration data means, i.e., whether requirements differ according to whether a change of registrant changes anything that is displayed.

7. Transfer Policy section II.B.1.1.4 references the Administrative Contact. The context of this provision is to define a change of registrant as a material change to certain fields, including "Administrative Contact email address, if there is no Prior Registrant email address." This section may no longer be necessary, as, under the new Registration Data Policy, Administrative Contact data is no longer collected by the registrar.

8. The Transfer Policy contains references to Whois in sections I.A.1.1, I.A.2.1.2, I.A.2.2.1, I.A.3.6, I.A.3.7.5, I.B.1, and the Notes section titled "Secure Mechanism." If updates are considered to this policy as a result of GNSO policy work, it may be beneficial to consider replacing these references with RDDS. (The Temporary Specification, Appendix G, Section 2.2.4, on Supplemental Procedures to the Transfer Policy, provides that the term "Whois" SHALL have the same meaning as "RDDS." This is carried over in the EPDP Phase 1 recommendation 24) Transfer Policy section II.C.1.4 provides that a registrar must obtain confirmation of a Change of Registrant request from the Prior Registrant, or the Designated Agent of such, using a secure mechanism to confirm that the Prior Registrant and/or their respective Designated Agents have explicitly consented to the Change of Registrant. The footnote to this section notes that "The registrar may use additional contact information on file when obtaining confirmation from the Prior Registrant and is not limited to the publicly accessible Whois." If changes are considered to this policy as a result of GNSO policy work, it may be beneficial to consider updating this footnote to eliminate the reference to Whois.

9. The EPDP Team's Phase 1 Recommendation 24 recommends that the following requirements apply to the Transfer Policy until superseded by recommendations from the Transfer Policy review being undertaken by the GNSO Council:

(a) Until such time when the RDAP service (or other secure methods for transferring data) is required by ICANN to be offered, if the Gaining Registrar is unable to gain access to then-current Registration Data for a domain name subject of a transfer, the related requirements in the Transfer Policy will be superseded by the below provisions:
(a1) The Gaining Registrar is not REQUIRED to obtain a Form of Authorization from the Transfer Contact.
(a2) The Registrant MUST independently re-enter Registration Data with the Gaining Registrar. In such instance, the Gaining Registrar is not REQUIRED to follow the Change of Registrant Process as provided in Section II.C. of the Transfer Policy.

(b) As used in the Transfer Policy:
(b1) The term "Whois data" SHALL have the same meaning as "Registration Data".
(b2) The term "Whois details" SHALL have the same meaning as "Registration Data".
(b3) The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".
(b4) The term "Whois" SHALL have the same meaning as "RDDS".

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

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

These requirements are being implemented as part of implementing the Registration Data Policy.

10. Feedback from some stakeholders in June 2019 during an ICANN65 session suggested an approach of starting from a clean slate rather than looking at specific transfer issues individually. This appears to be the path the GNSO is taking, based on discussions at the September Council meeting.

Cross-reference: Transfer Policy section I.B.3.1 contains a footnote referencing the Expired Registration Recovery Policy. The context for this reference is a provision specifying when the Change of Registrant Procedure does not apply, in this case, when the registration agreement expires. The footnote provides that if registration and Whois details are changed

following expiration of the domain name pursuant to the terms of the registration agreement, the protections of the Expired Registration Recovery Policy still apply.

Cross-reference: Transfer Policy section I.B.3.5 references the Expired Domain Deletion Policy. The context for this reference is a provision specifying when the Change of Registrant Procedure does not apply, in this case, when the Registrar updates the Prior Registrant's information in accordance with the Expired Domain Deletion Policy.

3.11.1 Transfer Dispute Resolution Policy (TDRP)

Summary: This policy addresses disputed domain name transfers between registrars, and all ICANN-accredited registrars must abide by its procedures and decisions.

Key Points: This policy is substantively affected by the new Registration Data Policy, particularly around sources of registration data to be used in the dispute and the basis for a panel's decision under the TDRP.

Analysis:

1. TDRP section 2.2, Statute of Limitations, provides that a dispute must be filed within 12 months of the alleged violation. This is the stated basis for the EPDP Team's Phase 1 recommendation 15 requiring registrars to retain only those data elements deemed necessary for the purposes of the TDRP, for a period of fifteen months following the life of the registration plus three months to implement the decision, as the TDRP has "the longest justified retention period of one year." Accordingly, this provision can be maintained under the Registration Data Policy.

2. TDRP sections 3.1.2(ii), 3.2.1, and 3.5.2 specify complainant contact information to be included in the complaint, which may include personal data. Processing of personal data that is not registration data is expected to be covered in the data processing terms in EPDP recommendations 22 and 26.

3. TDRP section 3.1.4 (i)(b) references a "copy of Whois output." The context for this provision is a listing of documentary evidence to be annexed to a complaint by the gaining registrar. This requirement may need to be further defined for clarity on what data the registrar must copy and include. Applying the definition of "Whois data" to have the same meaning as "Registration Data" as provided in EPDP

recommendation 24, this would include all data elements that were collected by the registrar.

4. TDRP section 3.1.4(ii)(c) enumerates the materials to be annexed to a complaint by the losing registrar. This provision specifies that the losing registrar is expected to provide a history of any Whois registration data changes made to the applicable registration. This requirement may need to be further defined as to what constitutes Whois modifications i.e., changes to public and/or non-public data elements. This provision may also need to be revised to clarify the scope of history available to the registrar, as it can only go as far back as data is retained. If the relevant data retention policy and uses of registration data including TDRP were disclosed to the data subject at the time of registration, this should cover such disclosure within the applicable period.

5. TDRP section 3.2.4 provides that a panel appointed by a TDRP provider will “review all applicable documentation and compare registrant/contact data with that contained within the authoritative Whois database and reach a conclusion not later than thirty (30) days after receipt of Response.” This provision relies on comparison with the "authoritative Whois database," which does not have a clear analogue in the new Registration Data Policy.

   The purpose of this provision appears to be for the panel to validate the information provided to them by the registrars; however, it is not clear what source a panel would use as a basis for comparison with the registrar submissions under the new policy. The TDRP provides for the panel to match what the registrars provide with its own lookup; this does not seem to be possible unless a) the panel requests non-public data from the registrar in a similar manner as a UDRP provider, which would result in duplicative data or b) the complaint only includes publicly accessible data, and the panel is able to request and obtain the non-public data from the registrar. Registration data held by the registry operator is not referenced in this section except to note that in cases where the Registrar of Record's Whois is not accessible or invalid, the applicable Registry Operator's Whois should be used, except in the case of a thin Registry, in which case the dispute should be placed on hold. It may be necessary to establish what is authoritative and what sources the panel should use in considering a TDRP complaint.

Alternatively, the provisions of this section could be restated at a higher level to define what the panel is being asked to do. The specific steps regarding comparison of various registration data sources may not be the basis for the panel's determination; rather, the panel is asked to consider the facts and circumstances and evidence presented by the parties to the dispute to determine whether a violation of the Transfer Policy has occurred.

3.11.2 STANDARDIZED FORM OF AUTHORIZATION | DOMAIN NAME TRANSFER - Initial Authorization for Registrar Transfer

Summary: The Transfer Policy mandates that the gaining registrar request an authorization for a registrar transfer from the Transfer Contact using a Standardized Form of Authorization. Enforcement of the Transfer Policy's Gaining Registrar FOA requirement is currently deferred pending the GNSO Council's planned Transfer Policy review.[10]

Key Points: This form can be updated with language changes but the text is not substantively impacted by the Registration Data Policy. The policy requirements around use of this form are discussed in section 3.11 above.

Analysis:

1. The sample form includes instruction to "<insert Registered Name Holder or Administrative Contact of Record as listed in the WHOIS>" as well as text stating that: "You have received this message because you are listed as the Registered Name Holder or Administrative contact for this domain name in the WHOIS database." To the extent this form is retained, the language may be updated to eliminate "Administrative Contact" and "WHOIS" references.

3.11.3 Standardized Form of Authorization - Confirmation of Registrar Transfer Request

Summary: The Transfer Policy mandates that the losing registrar request a confirmation for a registrar transfer from the Transfer Contact using a Standardized Form of Authorization.

[10] At its 26 January 2020 meeting, the ICANN Board approved the GNSO Council's request to defer compliance enforcement of the Gaining Registrar FOA requirement until this issue is settled in the GNSO's planned Transfer Policy review.

Key Points: This form can be updated with language changes but the text is not substantively impacted by the Registration Data Policy.

Analysis:

1. The sample form includes instruction to "<insert Registered Name Holder or Administrative Contact of Record as listed in the WHOIS>" as well as noting that "a registrar may choose to include one or more of the following in the message sent to the Registered Name Holder or Admin contact." To the extent this form is retained, the language may be updated to eliminate "Administrative Contact" and "WHOIS" references.

3.12 Uniform Domain Name Dispute Resolution Policy (UDRP)

Summary: The UDRP sets out the scope of relief and legal framework for the resolution of disputes between a domain name registrant and a third party (i.e., a party other than the registrar) over the registration of an Internet domain name.

Estimated Impact: High

Key Points: ICANN org did not identify any impacts of the Registration Data Policy on the UDRP itself. Some impacts on the UDRP Rules are discussed in section 3.12.1 below.

3.12.1 Rules for Uniform Domain Name Dispute Resolution Policy (UDRP Rules)

Summary: The UDRP Rules provide the baseline procedural requirements that must be followed for each stage of a dispute resolution administrative proceeding, such as required notice to a Respondent, time for filing a response, and appointment of the administrative panel for a UDRP proceeding.

Key Points: The UDRP Rules are substantively affected by the new Registration Data Policy requirements. Some areas identified have been addressed by the EPDP Phase 1 recommendations. It is also noted that the GNSO has work planned to review the UDRP.

Analysis:

1. UDRP Rules sections 1 and 2 reference the “Whois database.” The context of this provision is a definition for “Mutual Jurisdiction,” noting that this refers to either (a) the principal office of the registrar, or (b) the domain-name holder's address as shown in the Registrar's Whois database at the time the complaint is submitted, as appropriate. If changes are considered to these rules as a result of GNSO policy work, it may be beneficial to update this terminology to specify the intended source of the registrant’s address.

2. UDRP Rules section 1 includes definitions of terms used. If changes are considered to these rules as a result of GNSO policy work, it may be beneficial to update this to include the term and definition for “Registration Data Directory Services.”

3. UDRP Rules section 2(a)(i) and 2(a)(ii)(A) include references to the Administrative Contact. The context of this provision is the UDRP provider’s responsibility to use available means to achieve notice when notifying a registrant that a UDRP complaint has been filed. The references to Administrative Contact can be removed without altering the substance of the requirement.

4. Also in UDRP Rules section 2, the stated principle is that “it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent.” Given this aim, it may be beneficial to clarify that the Provider should continue to send the notice to all contacts publicly available in RDDS, and also to note that, per EPDP Recommendation 23, the UDRP provider may also request non-public registration data from the registrar, which may aid the provider in enabling the notification to the registrant.

5. UDRP Rules section 3(b) describes the required elements for submission of a complaint under the UDRP. These include, in item (v), “the name of the Respondent (domain-name holder) and all information (including any postal and email addresses and telephone and telefax numbers) known to Complainant regarding how to contact Respondent or any representative of Respondent, including contact information based on pre-complaint dealings, in sufficient detail to allow the Provider to send the complaint as described in Paragraph 2(a).” Per the EPDP Team’s Phase 1 recommendation 23, this provision may be updated to clarify that a complaint will not be deemed administratively deficient for failure to provide the name of the Respondent and all other relevant contact information.

6. Current practices relating to amending a UDRP complaint vary.[11] In one instance, a provider requires the complainant to amend its complaint to reflect the registrant information received from the registrar so that the proceeding can go forward. If the complainant does not amend the complaint, the UDRP complaint is dismissed. In another, a provider strongly encourages the complainant to amend its complaint, however, a complainant's failure to do so would not be treated as a formal deficiency under the UDRP Rules. This process may benefit from some clarification to ensure consistency among UDRP providers.

   The EPDP Team's recommendation 21 provides 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."

7. UDRP Rules section 4 provides that a UDRP provider submits a verification request to the registrar for the domain name(s) that are the subject of the complaint, which verification request includes a request to lock the domain name registration. Per EPDP recommendation 23, this provision may be updated to clarify that along with the verification request, the provider may also request the non-public registration data for each of the specified domain names, which shall be provided to the provider upon its notifying the Registrar of the existence of a UDRP complaint.

8. UDRP Rules section 16(b) require the panel to publish the full decision and the date of implementation on a publicly accessible website, as well as the portion of any decision determining a complaint to have been brought in bad faith. Concerning the publication of decisions, it may be useful to reference Purpose 6-PA5 in the Final EPDP report regarding publication of registration data elements used for complaints on Dispute Resolution Provider websites.

[11] See for example https://www.adrforum.com/domain-dispute/faq; https://www.wipo.int/amc/en/domains/gdpr/

9. UDRP Rules section 21 provides for amendments to the rules, noting that "The version of these Rules in effect at the time of the submission of the complaint to the Provider shall apply to the administrative proceeding commenced thereby. These Rules may not be amended without the express written approval of ICANN."

10. The EPDP Team's recommendation 22 provides that: "ICANN org must enter into appropriate data protection agreements with dispute resolution providers in which, amongst other items, the data retention period is specifically addressed." The form and content of such agreements are being determined as part of the policy implementation process.

11. In relation to the UDRP Rules, the EPDP Team's recommendation 23 provides that:

    i. *The Registrar MUST provide the UDRP provider with the full Registration Data for each of the specified domain names, upon the UDRP provider notifying the Registrar of the existence of a complaint, or participate in another mechanism to provide the full Registration Data to the Provider as specified by ICANN.*
    ii. *Complainant's complaint will not be deemed defective for failure to provide the name of the Respondent (Registered Name Holder) and all other relevant contact information required by Section 3 of the UDRP Rules if such contact information of the Respondent is not available in registration data publicly available in RDDS or not otherwise known to Complainant. In such an event, Complainant may file a complaint against an unidentified Respondent and the Provider shall provide the Complainant with the relevant contact details of the Registered Name Holder after being presented with a complaint against an unidentified Respondent.*

    These requirements are being implemented as part of implementing the Registration Data Policy.

12. Feedback from some stakeholders in June 2019 during an ICANN65 session noted the work plans of the RPM PDP Working Group, but posed the question of whether there were some procedural quick fixes to the UDRP Rules that could be adopted without waiting for the policy development process to complete. The GNSO may wish to consider this feedback in determining next steps.

3.13 Uniform Rapid Suspension System Procedure (URS)

Summary: The Procedure explains how to file a URS claim against a domain name registration, including fees, filing requirements, and steps involved in the process.

Estimated Impact: High

Key Points: The filing and processing of URS complaints is substantively impacted by the new Registration Data Policy requirements. Some areas identified have been addressed by the EPDP Phase 1 recommendations. It is also noted that the GNSO has work planned to review the URS.

Analysis:

1. URS section 1.2 includes various references to "Whois." The context of this provision is a description of the contents of a complaint submitted to a URS provider. References include section 1.2.3, describing Name of Registrant and available contact information available in Whois. Section 1.2.4 requires inclusion of the specific domain names that are the subject of the complaint, accompanied by "a copy of the currently available Whois information."

2. URS section 1.2 provides that a service provider make space in the complaint form for the enumerated information associated with the URS complaint. Per the EPDP Team's Phase 1 recommendation 23, this provision may be updated to clarify that a complaint will not be deemed administratively deficient for failure to provide the name of the Respondent and all other relevant contact information.

3. URS section 3.3 provides that "Given the rapid nature of this Procedure, and the intended low level of required fees, there will be no opportunity to correct inadequacies in the filing requirements."

   URS section 3.4 provides that "if a Complaint is deemed non-compliant with filing requirements, the Complaint will be dismissed without prejudice to the Complainant filing a new complaint. The initial filing fee shall not be refunded in these circumstances. This provision may be modified to clarify that a Complainant's

complaint will not be deemed administratively deficient for failure to provide the name of the Respondent and all other relevant contact information.

A question to consider is whether URS sections 3.3 and 3.4 should be updated to allow for amendment of a URS Complaint. Per the EPDP Team's Phase 1 recommendation 21, the GNSO Council instructs the review of all Review of All Rights Protection Mechanisms in All gTLDs (RPMs) PDP Working Group to consider whether (a) 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, and (b) upon receiving updated RDDS data (if any), the complainant must be given the opportunity to file an amended complaint containing the updated respondent information.[12]

4. URS section 4 describes requirements for notice and locking of a domain name. Section 4.2 notes that, within 24 hours after receiving a Notice of Lock from the registry operator, a URS provider notifies the registrant of the complaint by sending a hard copy "to the addresses listed in the Whois contact information." This may be revised to clarify that the provider should continue to send the notice to all contacts publicly available in RDDS; however, along with the Notice of Lock, the Provider may also request the non-public registration data for each of the specified domain names from the registrar, which shall be provided to the Provider upon the Provider notifying the Registry or Registrar of the existence of a complaint.

5. URS section 6 contains a procedure for default cases. Section 6.2 requires that "During the Default period, the Registrant will be prohibited from changing content found on the site to argue that it is now a legitimate use and will also be prohibited from changing the Whois information." Updates to this section may be considered to provide clarity on the information that may not be changed by a registrant, i.e., public and non-public data elements.

[12] The GNSO's RPM PDP Working Group, tasked with reviewing the URS and UDRP, is discussing text for inclusion in its initial report regarding the URS as follows:

> *(1) URS Rules section 3(b) be amended in light of GDPR and the permissible filing of a "Doe Complaint," and (2) URS Procedure section 3.3 should be amended to enable modification of the Complaint within 2-3 days from disclosure of the data required to advance the complaint by the URS Provider.*

9. URS section 9.4 requires that “Determinations resulting from URS proceedings will be published by the URS Provider on the Provider’s website in accordance with the Rules.” Concerning the publication of decisions, it may be useful to reference Purpose 6-PA5 in the Final EPDP report regarding publication of registration data elements used for complaints on Dispute Resolution Provider websites to Internet users.

10. URS section 10.2 requires that “The Whois for the domain name shall continue to display all of the information of the original Registrant except for the redirection of the nameservers. In addition, the Registry Operator shall cause the Whois to reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration” This language may be updated to refer to registration data rather than Whois.

11. The EPDP Team’s recommendation 22 provides that: “ICANN org must enter into appropriate data protection agreements with dispute resolution providers in which, amongst other items, the data retention period is specifically addressed.” The form and content of such agreements are being determined as part of the policy implementation process.

12. Feedback from some stakeholders in June 2019 during an ICANN65 session noted the work plans of the RPM PDP Working Group, but posed the question of whether there were some procedural quick fixes to the UDRP and URS that could be adopted without waiting for the policy development process to complete. The GNSO may wish to consider this feedback in determining next steps.

3.13.1 Uniform Rapid Suspension System Rules (URS Rules)

Summary: The URS Rules describe how service providers will implement the URS in a consistent manner.

Key Points: The filing and processing of URS complaints is substantively impacted by the new Registration Data Policy requirements. Some areas identified have been addressed by the EPDP Phase 1 recommendations. It is also noted that the GNSO has work planned to review the URS.

Analysis:

1. URS Rules section 1 refers to the “Whois database.” The context of this provision is a definition for “Mutual Jurisdiction,” noting that this refers to either (a) the principal office of the registrar, or (b) the domain-name holder's address as shown in the Registrar's Whois database at the time the complaint is submitted, as appropriate. If changes are considered to these rules as a result of GNSO policy work, it may be beneficial to update this terminology to specify the intended source of the registrant’s address.

2. URS Rules section 1 includes definitions of terms used. If changes are considered to these rules as a result of GNSO policy work, it may be beneficial to update this to include the term and definition for “Registration Data Directory Services.”

3. URS Rules section 2(a)(i) includes references to the Administrative Contact. The context of this provision is the UDRP provider’s responsibility to use available means to achieve notice when notifying a registrant that a UDRP complaint has been filed. The references to Administrative Contact can be removed without altering the substance of the requirement.

4. Also in URS Rules section 2(a), the stated principle is that, when forwarding a complaint, “it shall be the Provider's responsibility to employ reasonably available means calculated to achieve actual notice to Respondent.” Given this aim, it may be beneficial to clarify that the Provider should continue to send the notice to all contacts publicly available in RDDS, and also to note that, per EPDP recommendation 23, the provider may also request non-public registration data from the registrar, which may aid the provider in enabling the notification to the registrant.

5. URS Rules section 3(b)(iv) require a complaint to include the domain name(s) that are the subject of the Complaint and “a copy of the currently available Whois information.” This may be updated to clarify that a complaint will not be deemed administratively deficient for failure to provide the name of the Respondent and all other relevant contact information.

6. URS Rules 4(b) provide that the Notice of Complaint sent to the registrant shall be transmitted in English and translated by the provider into the predominant language used in the registrant’s country or territory, as determined by the country(ies) listed in the Whois record when the Complaint is filed. This provision may not be affected by

the new Registration Data Policy because the country field is still publicly displayed. With regard to 4(b), it may be beneficial to clarify that the provider may also request non-public registration data from the registrar upon presentation of a complaint.

8. URS Rules section 15.4 requires that, with certain exceptions, "the Provider shall publish the Determination and the date of implementation on a publicly accessible web site." Concerning the publication of decisions, it may be useful to reference Purpose 6-PA5 in the Final EPDP report regarding publication of registration data elements used for complaints on Dispute Resolution Provider websites to Internet users.

9. In relation to the URS Rules, the EPDP Team's recommendation 23 provides that:

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

   This requirement is being implemented as part of implementing the Registration Data Policy.

10. Many of the points discussed here mirror those discussed in the URS Procedure analysis, above. If changes are considered to these rules as a result of GNSO policy work, it may be beneficial to more clearly differentiate the content of the procedure and the rules to avoid redundancies.

3.13.2 URS High Level Technical Requirements

Summary: The URS High Level Technical Requirements provide information on how registries and registrars are to implement the URS technical requirements in a consistent manner.

Key Points: The URS High Level Technical Requirements are impacted by the Registration Data Policy; however, these points are specifically addressed in the EPDP's recommendation 23. These requirements are being implemented as part of implementing the Registration Data Policy.

Analysis:

1. URS Technical Requirements section 2 describes requirements for registry operators. This may be updated with the requirement that Registry Operator shall provide the Provider with the full registration data for each of the specified domain names, upon the Provider notifying the Registry Operator of the existence of a complaint. In relation to the URS High Level Technical Requirements, the EPDP Team's recommendation 23 provides that:

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

2. URS Technical Requirements section 5 describes requirements for registrars. This may be updated with the requirement that registrar shall provide the Provider with the full registration data for each of the specified domain names, upon the Provider notifying the registrar of the existence of a complaint. In relation to the URS High Level Technical Requirements, the EPDP Team's recommendation 23 provides that:

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

3.14 Whois Data Reminder Policy (WDRP)

Policy Summary: At least annually, a registrar must present to the registrant the current Whois information for each domain name registration, and remind the registrant that provision of false Whois information can be grounds for cancellation of the domain name registration. Registrants must review their Whois data, and make any corrections.

Estimated Impact: Medium

Key Points: The underlying procedure and requirements for this policy can continue under the Registration Data Policy; however, some clarification to the requirements may be required.

Analysis:

1. An update to the name of the policy may be considered as title includes “Whois,” which may not remain accurate. The policy text includes multiple instances of “Whois” terminology, for example: “At least annually, a registrar must present to the registrant the current Whois information, and remind the registrant that provision of false Whois information can be grounds for cancellation of their domain name registration. Registrants must review their Whois data, and make any corrections.”

2. Per the EPDP Team’s Phase 1 recommendation 4, “requirements related to the accuracy of registration data under the current ICANN contracts and consensus policies shall not be affected by this policy.” The policy would accordingly be expected remain in place; however, some clarifications may be needed to harmonize the WDRP policy requirements with the new Registration Data Policy requirements.

3. In considering how such requirements carry over to the new policy environment, this analysis relies on the definition of “Registration Data” in section 2 of the Temporary Specification, namely, "Registration Data" means data collected from a natural and legal person in connection with a domain name registration.[13] Accordingly, to meet the policy objective, the requirement would be for the notice to contain the data that is collected by the registrar.

4. The Registration Data Policy does not speak to whether optional data elements should be included in the WDRP notice; however, under the definition of Registration

[13] The EPDP recommendation 24 concerning the Transfer Policy notes that “the term “Whois data” SHALL have the same meaning as “Registration Data.”

Data above, optional elements are part of the data collected by the registrar and thus should be included, supporting the policy goal of enabling the registrant to keep its information current.

5. It should be noted that the WDRP text consists of only two sentences, followed by several Notes sections. If additional policy work is pursued by the GNSO to update this policy, ICANN org would recommend additional changes to the Notes accompanying the policy with the GNSO's acknowledgement of such, for example, the WDRP section on Time for Coming into Compliance may be eliminated as obsolete.

6. The policy is accompanied by a model WDRP notice that includes Administrative Contact, Technical Contact, and Registrant Organization. If updates to the model notice are being considered as a result of GNSO policy work, it may be beneficial to clarify that the notice should contain the elements that are required to be collected by the Registration Data Policy. Additionally, if changes are considered to the model notice as a result of GNSO policy work, the contact information shown for the ICANN organization example needs to be updated. The Registration Data Policy does not appear to preclude registrars from adding more data elements to the notice than are included in the model notice; this point may be clarified.

7. The requirement for registrars to retain copies of notices falls under the RAA provision (3.4.2) on copies of communications, such records to be maintained for the term of the agreement plus two years.

3.15 Whois Marketing Restriction Policy

Summary: This policy is a revision to the third-party bulk access provisions in ICANN's 2001 Registrar Accreditation Agreement to restrict the use of WHOIS data for marketing and re-use.

Estimated Impact: Low

Key Points: ICANN org did not identify any substantive impacts on this policy.

Analysis:

1. An update to the name of the policy may be considered as title includes “Whois,” which may not remain accurate.

2. The requirements of this policy are reflected in section 3 of the 2013 Registrar Accreditation Agreement. In the event that ICANN determines, following analysis of economic data by an economist(s) retained by ICANN (which data has been made available to Registrar), that an individual or entity is able to exercise market power with respect to registrations or with respect to registration data used for development of value-added products and services by third parties, registrars would be required to provide third-party bulk access to registration data under certain terms. As this has not occurred, the requirements do not currently apply. If ICANN were to make such a determination, the registrar would be required to include these terms in its agreements with third-party recipients of bulk access to registration data.

4 Next Steps

Overall, the Wave 1 impacts described in this report appear to be within the remit of the GNSO. Each of the items in this report is either consensus policy or, in case of URS, already being considered in a GNSO PDP. This draft report was shared with the IRT for review and validation of that the GNSO is the appropriate path for each item included in this report. During this review step, the IRT did not identify any issues with the proposed paths or additional items to be added to the inventory. As the IRT review period did not result in any changes or updates to this report, it is being submitted to the GNSO Council who will then determine next steps.

The GNSO will follow its process to determine next steps (e.g., Expedited Policy Development Process, GNSO Guidance Process, etc.). Given that the impact of the Registration Data Policy reaches across a variety of policies, it may be useful to consider whether there is a need for multiple individual policies or whether the requirements related to registration data could exist in a more consolidated form.

In the event that the Registration Data Policy goes into effect while GNSO work on other affected policies is in progress, ICANN org would anticipate providing guidance and

transparency for contracted parties regarding how affected policies are being treated for enforcement.