Next Generation Registration Directory Service (RDS) to replace WHOIS Policy Development Newsletter – September 2017

WHAT IS THE CURRENT STATUS OF THIS PROJECT?

The Working Group (WG) for gTLD registration directory services has been working to provide a foundation upon which to recommend answers to these two questions: *What are the fundamental requirements for gTLD registration data and directory services, and is a new policy framework and next-generation RDS needed to address these requirements?*

The WG is currently working to reach initial rough consensus agreement on key concepts related to the WG's charter questions concerning RDS users/purposes, data elements, privacy and access.

WG members, along with the Leadership Team, presented the tentative conclusions reached by the WG to the broader ICANN community at a cross-community discussion during ICANN 59 in Johannesburg. Since ICANN 59, the WG has expanded its deliberation to define requirements for registration data elements beyond the "Minimum Public Data Set" (MPDS) that must be supported by the RDS, using the Expert Working Group on gTLD Directory Services (EWG) Final Report as a starting point of discussion. The WG is continuing to use weekly calls and polls to facilitate development of tentative rough consensus agreements on these key concepts.

Furthermore, to assist in informing WG deliberation on key concepts related to the WG's charter questions that are impacted by data protection laws, such as the European Union General Data Protection Regulation (GDPR), the WG has taken two additional steps:

(1) the WG solicited input from ccTLD Registry Operators on their approaches to GDPR compliance, and
(2) retained the services of independent legal counsel to answer questions about the impact of data protection laws on registration data and directory services previously answered by senior EU data protection experts.

The input received from all three sources (senior EU data protection experts, independent legal counsel, and ccTLD Registry Operators,) is expected to assist the WG in its deliberation on key concepts and possible requirements concerning RDS users/purposes, data elements, privacy and access.

As of the end of August 2017, 38 initial points of rough consensus had been reached during iterative and ongoing deliberation. All initial agreements have been guided by an overall statement of purpose for registration data and directory services drafted by the WG as follows:

Draft Registration Data and Directory Service Statement of Purpose

This statement is intended to define the purpose(s) of a potential Registration Directory Service (RDS) for generic top-level domain (gTLD) names. The statement identifies Specific Purposes for registration data and registration directory services.

Note that it is important to make a distinction between the purpose(s) of individual registration data elements[1] versus the purpose(s) of a RDS, i.e., the system that may collect, maintain, and provide or deny access to some or all of those data elements and services related to them, if any.

Specific Purposes for Registration Data and Registration Directory Services

1. *A purpose of gTLD registration data is to provide info about the lifecycle of a domain name and its resolution on the Internet.*
2. *A purpose of RDS is to facilitate dissemination of gTLD registration data of record[2], such as domain names and their domain contacts[3] and nameservers in accordance with applicable policy.*
3. *A purpose of RDS is to identify domain contacts and facilitate communication with domain contacts associated with generic top-level domain names, [based on approved policy].*
4. *A purpose of gTLD registration data is to provide a record of domain name registrations.*

Note: "Accuracy" as it pertains to the RDS will be defined later in this PDP (see the Charter question on Accuracy).

Footnotes

[1] Here, "registration data elements" refers to data about generic top-level domain names collected in the relationship between registrars to registries and in the relationship between registrars/registries and ICANN.

[2] Draft definition of "gTLD registration data of record": The data set at a given time, relevant to a given registration object, that expresses the data provided in the then-current registration for that object.

[3] Contacts related to the domain name, including those directly related to the domain name and also those involved in the registration system as relevant. Further specification may occur at a later stage in the RDS PDP process.

- Source: Section 2.3, KeyConceptsDeliberation-WorkingDraft

As of 29 August 2017, the WG had reached rough consensus on the following agreements, subject to further refinement during iterative deliberation. A more comprehensive description of the discussions and context resulting in these rough consensus agreements can be found in the 29 August, 2017 Working Draft on Key Concepts Deliberation document.

Initial points of rough consensus (iterative deliberation on-going)

Should gTLD registration data elements in the "Minimum Public Data Set" be accessible for any purpose or only for specific purposes?

1. *The WG should continue deliberation on the purpose(s) of the "Minimum Public Data Set".*
2. *Every data element in the "Minimum Public Data Set" should have at least one legitimate purpose.*

3. *Every existing data element in the "Minimum Public Data Set" does have at least one legitimate purpose for collection.*

For what specific (legitimate) purposes should gTLD registration data elements in the "Minimum Public Data Set" be collected?

4. *EWG-identified purposes apply to at least one data element in the "Minimum Public Data Set".*
5. *Domain name control is a legitimate purpose for "Minimum Public Data Set" collection.*
6. *Technical Issue Resolution is a legitimate purpose for "Minimum Public Data Set" collection.*
7. *Domain Name Certification is a legitimate purpose for Minimum Public Data Set" collection.*
8. *Business Domain Name Purchase or Sale is a legitimate purpose for "Minimum Public Data Set" collection.*
9. *Academic / Public Interest DNS Research is a legitimate purpose for "Minimum Public Data Set" collection.*
10. *Regulatory and Contractual Enforcement is a legitimate purpose for "Minimum Public Data Set" collection.*
11. *Criminal Investigation & DNS Abuse Mitigation is a legitimate purpose for "Minimum Public Data Set" collection.*
12. *Legal Actions is a legitimate purpose for Minimum Public Data Set" collection.*
13. *Individual Internet Use is a legitimate purpose for "Minimum Public Data Set" collection.*

    Note: Additional work on definitions will be needed to clarify purpose for collection vs. purpose for disclosure/use, as well as who/what is collecting registration data.

For the "Minimum Public Data Set" only, do existing gTLD registration directory services policies sufficiently address compliance with applicable data protection, privacy, and free speech laws about purpose?

14. *Existing gTLD RDS policies do NOT sufficiently address compliance with applicable data protection, privacy, and free speech laws about purpose.*
15. *As a WG, we need to agree upon a purpose statement for the RDS.*
    (refer to agreements 16 – 19 below, and the Statement of Purpose above)

What should the over-arching purpose be of collecting, maintaining, and providing access to gTLD registration data?

16. *A purpose of gTLD registration data is to provide info about the lifecycle of a domain name and its resolution on the Internet.*
17. *A purpose of RDS is to facilitate dissemination of gTLD registration data of record[2], such as domain names and their domain contacts[3] and nameservers in accordance with applicable policy.[4]*
18. *A purpose of RDS is to identify domain contacts and facilitate communication with domain contacts associated with generic top-level domain names, [based on approved policy].*
19. *A purpose of gTLD registration data is to provide a record of domain name registrations.*

Should gTLD registration data in the "Minimum Public Data Set" be entirely public or should access be controlled?

20. *gTLD registration data in the "Minimum Public Data Set" must be accessible without requestor identification, authentication, or stated purpose.*
21. *There must be no RDS policies that prevent RDS operators from applying operational controls such as rate limiting and CAPTCHA, provided that they do not unreasonably restrict legitimate access.*
22. **What guiding principles should be applied to "Minimum Public Data Set" access?** *At least a defined set of data elements must be accessible by unauthenticated RDS users.*
23. *RDS policy must state purpose(s) for public access to the "Minimum Public Data Set".*
24. *(based on EWG principle #44, set aside pending further deliberation)*

Which gTLD registration data elements should be included in the "Minimum Public Data Set"?

25. *"Minimum Public Data Set" to be used as a replacement term (within WG Agreements to date) for what had previously been referred to as "thin data."*
26. *The DNSSEC data element should be added to the "Minimum Public Data Set."*
27. *Today's gTLD WHOIS registration data elements classified as "thin" are sufficient at this time, to be referred to within WG Agreements hereafter as the "Minimum Public Data Set."*

What are the guiding principles that should be applied to all data elements to determine whether they are mandatory/optional to collect, public/non-public to access, etc?

28. *Registrant Country must be included in RDS data elements; it must be mandatory to collect for every domain name registration.*
29. *RDS policy must include a definition for every gTLD registration data element including both a semantic definition and (by reference to appropriate standards) a syntax definition.*
30. *At least one element identifying the domain name registrant (i.e., registered name holder) must be collected and included in the RDS.*
31. *Data enabling at least one way to contact the registrant must be collected and included in the RDS.*
32. *At a minimum, one or more e-mail addresses must be collected for every domain name included in the RDS, for contact roles that require an e-mail address for contactability.*
33. *For resiliency, data enabling alternative or preferred method(s) of contact should be included in the RDS; further deliberation to determine whether such data element(s) should be optional or mandatory to collect.*
34. *At least one element enabling contact must be based on an open standard and not a proprietary communication method.*
35. *To improve contactability with the domain name registrant (or authorized agent of the registrant), the RDS must be capable of supporting at least one alternative contact method as an optional field.*
36. *Purpose-based contact (PBC) types identified (Admin, Legal, Technical, Abuse, Proxy/Privacy, Business) must be supported by the RDS but optional for registrants to provide.*
37. *The URL of the Internic Complaint Site must be supported for inclusion in the RDS.*
38. *The Registrar Abuse Contact Email Address must be supported for inclusion in the*

RDS, and must be provided by Registrars.

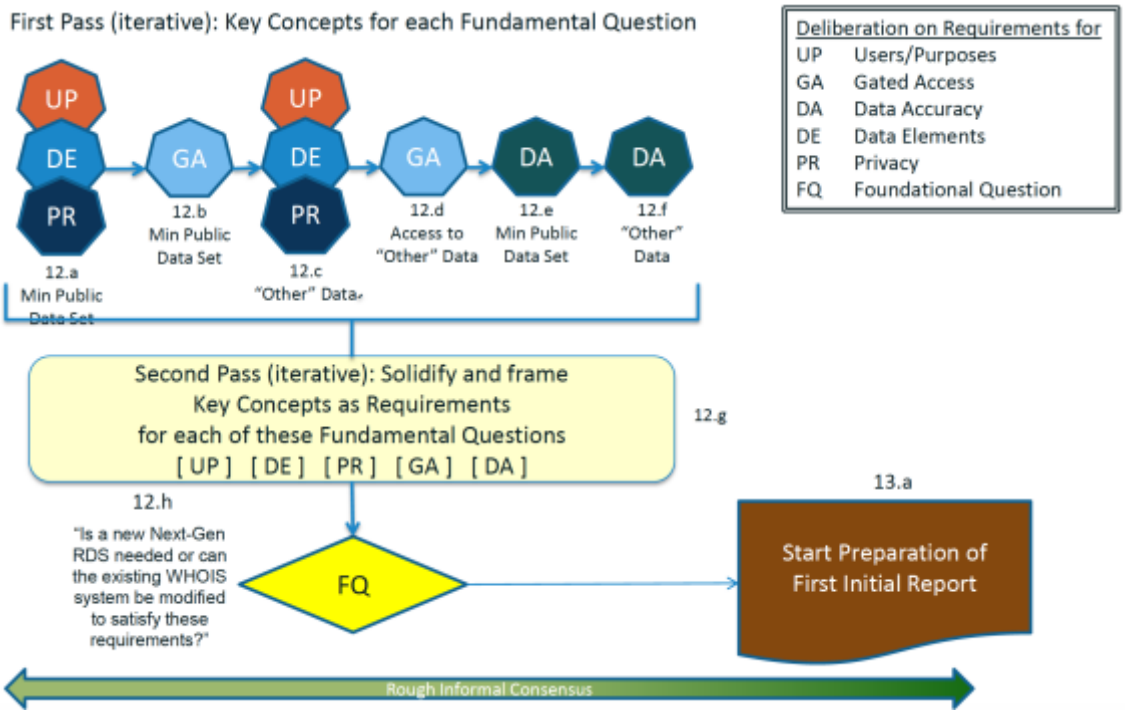
- Source: Sections 2.1-2.3, 3.4, 4.1, 5.1, 5.4 KeyConceptsDeliberation-WorkingDraft

WHAT ARE THE EXPECTED NEXT STEPS?

The WG is continuing its current task to reach rough consensus agreements on key concepts concerning all registration data elements – including those beyond a Minimum Public Data Set. Specifically, the WG will continue to use weekly polls to reach rough consensus on key concepts for which data elements must be supported by the RDS, and whether it is mandatory or optional to collect all identified data elements. The WG will then try to answer other charter questions for that universe of data elements, including users/purposes (who needs each data element, for what purpose(s), access (should access to each data element be public or controlled in some way), and privacy (how do data protection and privacy laws apply to each data element).

To help the WG make progress on these difficult questions, the WG is expecting to apply answers provided by both independent legal counsel and senior EU data protection experts, concerning RDS compliance with data protection laws, including the European Union General Data Protection Regulation (GDPR). The WG expects to receive that legal analysis by the end of September 2017.

The key concepts agreed to by the WG, along with guidance on data protection laws provided by independent legal counsel and senior EU data protection experts, and feedback obtained from the community at ICANN59, will be used to establish a foundation for completing deliberations on possible requirements, as required in phase 1 of the PDP charter. The WG will systematically consider possible requirements with the goal of trying to reach as strong a consensus as possible for each possible requirement. Due to interdependencies, WG deliberation will likely continue to be iterative, especially on fundamental questions pertaining to purpose, data, and privacy.



Currently, the target for beginning to draft the first of two initial reports planned for Phase 1 is the first quarter of 2018; that first initial report will include responses to the first five of eleven questions in phase 1. Further formal and informal input opportunities will occur throughout the WG's phase 1 deliberations, as well as during phases 2-3 should the GNSO decide a next-generation directory service is needed to meet phase 1 requirements.

WHAT IS THIS ABOUT?

In April 2015, the ICANN Board reaffirmed its request for a Board-initiated GNSO policy development process to define the purpose of collecting, maintaining and providing access to gTLD registration data, and consider safeguards for protecting data, using the recommendations in the Expert Working Group (EWG) Final Report as an input to, and, if appropriate, as the foundation for a new gTLD policy.

Following the publication of the PDP Final Issue Report, the GNSO Council adopted the charter for the PDP Working Group, which commenced its deliberations at the end of January 2016. During the first phase its work, the Working Group has been tasked with providing the GNSO Council with recommendations on the following two questions: What are the fundamental requirements for gTLD registration data and is a new policy framework and next-generation RDS needed to address these requirements?

WHY IS THIS IMPORTANT?

Comprehensive 'WHOIS' policy reform remains the source of long-running discussions within ICANN. Any discussion of the 'WHOIS' system for gTLD registration data – hereafter called gTLD registration directory services (RDS) – typically includes topics such as purpose, accuracy, availability, privacy, data protection, cost, policing, intellectual property protection, security and malicious use and abuse. Although ICANN's requirements for gTLD domain name registration data collection, maintenance, and provision have undergone some important changes, after almost 15 years of GNSO task forces, working groups, workshops, surveys, and studies, the policy is still in need of comprehensive reforms that address the significant number of contentious issues attached to it.

HOW CAN I GET INVOLVED?

Anyone interested can join this effort at any time. Please complete the registration form at **goo.gl/forms/bb65iIznLv or contact the GNSO Secretariat: gnso-secs@icann.org.**

MORE INFORMATION

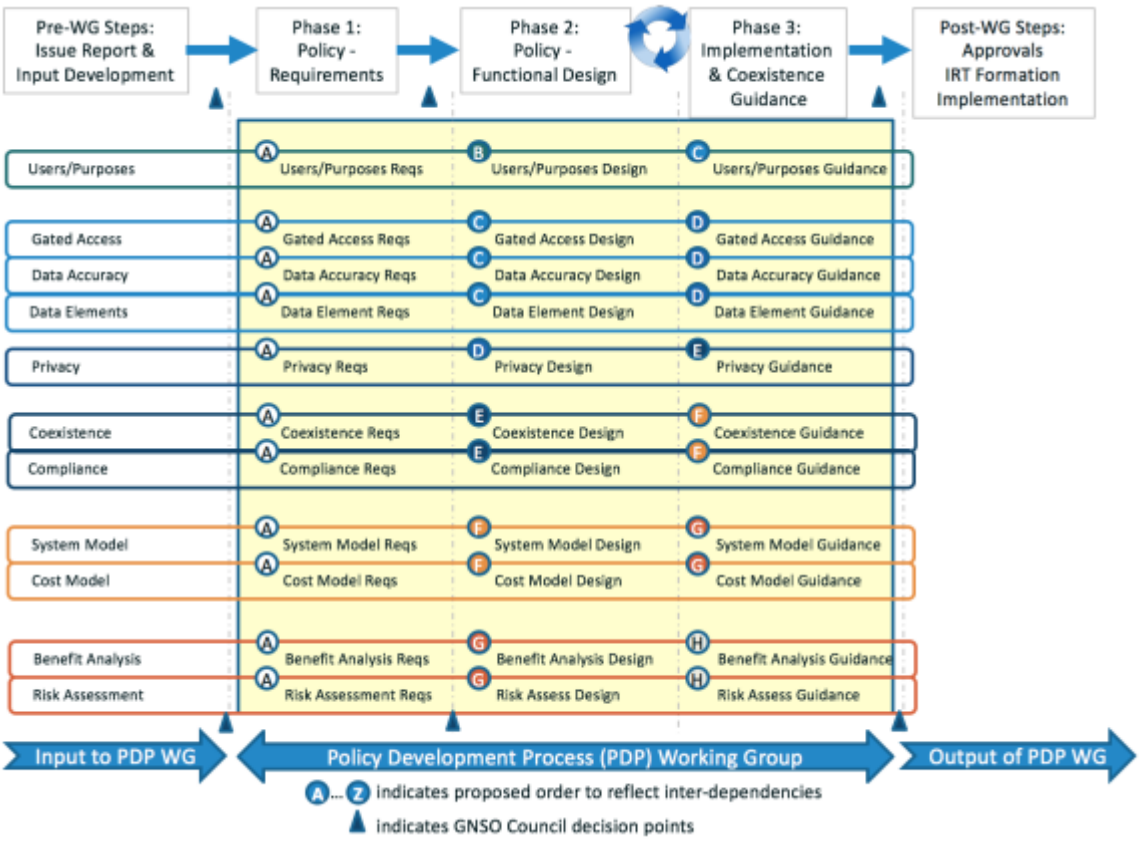
- PDP Working Group Workspace, including Charter, relevant motions, and background documents and information: https://community.icann.org/x/rjJ-Ag
- PDP Working Group Phase 1 Outputs (in progress): https://community.icann.org/x/p4xlAw
- Final Issue Report on Next-Generation gTLD Registration Directory Service (RDS) to replace WHOIS: http://whois.icann.org/sites/default/files/files/final-issue-report-next-generation-rds-07oct15-en.pdf
- Board-GNSO Process Framework for this PDP: https://community.icann.org/x/GIxlAw

BACKGROUND

Pursuant to its Resolution on 8 November 2012, the ICANN Board directed the ICANN CEO to launch a new effort to redefine the purpose of collecting, maintaining and providing access to gTLD registration data, and consider safeguards for protecting data, as a foundation for new gTLD policy and contractual negotiations. Moreover, the Board directed the preparation of an Issue Report on the purpose of collecting and maintaining gTLD registration data, and on solutions to improve accuracy and access to gTLD registration data, as part of a Board-initiated GNSO policy development process. The Board then went on to pass a resolution that led to the creation of the Expert Working Group; the Board referred to this as a 'two-pronged approach' that is based on 'broad and responsive action' in relation to the reform of gTLD Registration Data.

To enable effective consideration of the many significant and interdependent policy areas that the GNSO must address, the Board approved a Process Framework, collaboratively developed by GNSO Councilors and Board members, to structure this complex and challenging PDP for success. This phased process includes:

- Phase 1: Establishing requirements to determine if and why a next- generation gTLD registration directory service (RDS) is needed to replace today's WHOIS system;
- Phase 2: If so, designing a new policy framework that details functions that must be provided by a next- generation RDS to support those requirements; and
- Phase 3: Providing guidance for how a next-generation RDS should implement those policies, coexisting with and eventually replacing the legacy WHOIS system.



Throughout this three-phase process, the many inter-related questions that must (at minimum) be addressed by the PDP include:

- Users/Purposes: Who should have access to gTLD registration data and why (i.e., for what purposes)?
- Gated Access: What steps should be taken to control data access for each user/purpose?
- Data Accuracy: What steps should be taken to improve data accuracy?
- Data Elements: What data should be collected, stored, and disclosed?
- Privacy: What steps are needed to protect data and privacy?
- Coexistence: What steps should be taken to enable next-generation RDS coexistence with and replacement of the legacy WHOIS system?
- Compliance: What steps are needed to enforce these policies?
- System Model: What system requirements must be satisfied by any next-generation RDS implementation?
- Cost: What costs will be incurred and how must they be covered?
- Benefits: What benefits will be achieved and how will they be measured?
- Risks: What risks do stakeholders face and how will they be reconciled?

The framework developed to guide this PDP also includes many opportunities for gathering input to inform this PDP and key decision points at which the GNSO Council will review progress made to determine next steps.