1. Introduction

This document is intended to record on-going RDS PDP WG progress made on Phase 1, Task 12: *Deliberate on possible fundamental requirements*.

Deliberations on detailed requirements may be more productive and time effective if the WG first deliberates on key concepts to provide a common foundation. Accordingly, the WG has adjusted its approach to start deliberating on sub-questions relating to charter questions for Users/Purposes, Data Elements, and Privacy, further detailed within this document. The WG will use these sub-questions – refined as necessary during deliberation – to discuss and attempt to reach rough consensus on possible answers and associated key concepts, to be recorded in this working document.

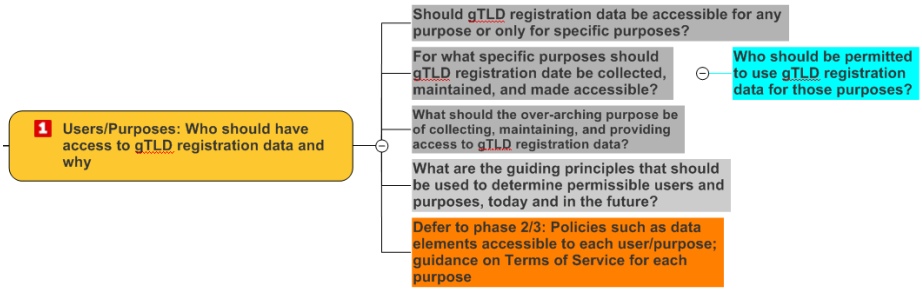
When developing its work plan, the WG agreed to iteratively look at all three questions as applicable, with the understanding that WG deliberation will likely bounce around some and be iterative in nature. To rotate among the charter questions, the WG will start by deliberating on the first sub-question under a randomly-selected charter question. Deliberation will continue on that sub-question until sufficient agreement has been reached to serve as an assumption for any dependencies in the next charter question's first sub-question. Deliberation will continue, iterating through all three charter questions and sub-questions in a flexible manner, using draft agreements as working assumptions to address interdependencies, but allowing for further refinement as those agreements evolve.

After reaching rough consensus on a collection of key concepts in this manner, it is hoped that the WG will have established a foundation for completing deliberations on its long list of individual possible requirements, as necessary. See Section 5 for next steps to follow this initial deliberation.

Edits reflected in this update:

- WG agreements from 21 December and 10 January call added to sections 2.1 and 2.2.
- WG agreements from 18 January call added to section 2.2.
- WG agreements from 24 January call added to section 2.2.
- WG agreements from 14 February call added to section 4.1.
- WG agreements from 22 February call added to section 2.3.
- WG agreements from 7 March call added to section 2.3
- WG agreements from 4 April call added to section 2.3
- WG agreement from 2 May call added to section 5.1
- Proposed WG agreement from 17 May call added to section 2.3
- Proposed WG agreements from 17 May call added to section 5.1

2. Charter Question: Users and Purposes



2.1 Should gTLD registration data be accessible for any purpose or only for specific purposes?

2.1.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Page 5:
The EWG unanimously recommends abandoning today's WHOIS model of giving every user the same entirely anonymous public access to (often inaccurate) gTLD registration data.

Instead, the EWG recommends a paradigm shift to a next-generation RDS that collects, validates and discloses gTLD registration data for permissible purposes only.

While basic data would remain publicly available, the rest would be accessible only to accredited requestors who identify themselves, state their purpose, and agree to be held accountable for appropriate use.

In December 2016, the WG agreed to focus its initial deliberation on "thin data" as defined by the Thick WHOIS Report: *"A thin registry only stores and manages the information associated with the domain name. This set includes data sufficient to identify the sponsoring registrar, status of the registration, creation and expiration dates for each registration, name server data, the last time the record was updated in its Whois data store, and the URL for the registrar's Whois service."*

2.1.2 Draft agreements

Should gTLD registration thin data elements be accessible for any purpose or only for specific purposes?

WG Agreement #1: The WG should continue deliberation on the purpose(s) of "thin data."

WG Agreement #2: Every "thin data" element should have at least one legitimate purpose.

WG Agreement #3: Every existing "thin data" element does have at least one legitimate purpose for collection.

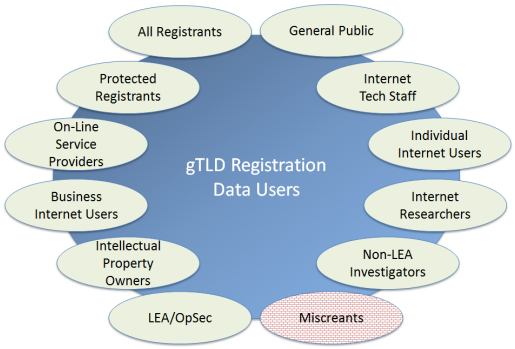
2.2 For what specific purposes should gTLD registration data be collected, maintained, and made accessible? Who should be permitted to use gTLD registration data for those purposes?

2.2.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

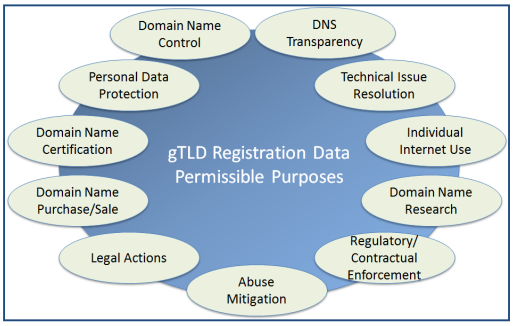
From Pages 7-9:
The EWG examined existing and potential purposes for collecting, storing, and providing gTLD registration data to a wide variety of users, examining an extensive, representative set of actual WHOIS use cases.

The EWG considered the totality of these use cases and the lessons learned from them, as well as reference material and community input, to derive a consolidated set of users and permissible purposes that must be accommodated by the RDS and potential misuses that must be deterred.



Purposes to be Accommodated or Prohibited
Consistent with the EWG's mandate, all of these users were examined to identify existing and possible future workflows and the stakeholders and data involved in them.

Domain name registration information needs were analyzed to derive mandatory data elements, related risks, privacy law and policy implications, and address other questions explored in this report. The EWG's recommended permissible purposes are summarized at right.



Currently-identified permissible purposes and associated registration data, contact, and query needs are defined below and further detailed in Section III [of the EWG Report].

Purpose	***Includes tasks such as…***
Domain Name Control	*Creating, managing and monitoring a Registrant's own domain name (DN), including creating the DN, updating information about the DN, transferring the DN, renewing the DN, deleting the DN, maintaining a DN portfolio, and detecting fraudulent use of the Registrant's own contact information.*
Personal Data Protection	*Identifying the accredited Privacy/Proxy Provider or Secure Protected Credential Approver associated with a DN and reporting abuse, requesting reveal, or otherwise contacting that Provider.*
Technical Issue Resolution	*Working to resolve technical issues associated with domain name use, including email delivery issues, DNS resolution failures, and website functional issues, by contacting technical staff responsible for handling these issues.*
Domain Name Certification	*Certification Authority (CA) issuing an X.509 certificate to a subject identified by a domain name needing to confirm that the DN is registered to the certificate subject.*
Individual Internet Use	*Identifying the organization using a domain name to instil consumer trust, or contacting that organization to raise a customer complaint to them or file a complaint about them.*
Business Domain Name Purchase or Sale	*Making purchase queries about a DN, acquiring a DN from another Registrant, and enabling due diligence research.*
Academic/Public-Interest DNS Research	*Academic public-interest research studies about domain names published in the RDS, including public information about the Registrant and designated contacts, the domain name's history and status, and DNs registered by a given Registrant.*
Legal Actions	*Investigating possible fraudulent use of a Registrant's name or address by other domain names, investigating possible trademark infringement, contacting a Registrant/Licensee's legal representative prior to taking legal action and then taking a legal action if the concern is*

Purpose	*Includes tasks such as…*
	not satisfactorily addressed.
Regulatory and Contractual Enforcement	*Tax authority investigation of businesses with online presence, UDRP investigation, contractual compliance investigation, and registration data escrow audits.*
Criminal Investigation & DNS Abuse Mitigation	*Reporting abuse to someone who can investigate and address that abuse, or contacting entities associated with a domain name during an offline criminal investigation.*
DNS Transparency	*Querying the registration data made public by Registrants to satisfy a wide variety of needs to inform the general public.*

See also Annex D, pages 129-132, for Thin Data elements identified by the EWG for each of the above-listed purposes.

2.2.2 Draft agreements

For what specific (legitimate) purposes should gTLD registration thin data elements be collected?

WG Agreement #4: EWG-identified purposes apply to at least one "thin data" element.

WG Agreement #5: Domain name control is a legitimate purpose for “thin data” collection.

WG Agreement #6: Technical Issue Resolution is a legitimate purpose for “thin data” collection.

WG Agreement #7: Domain Name Certification is a legitimate purpose for "thin data" collection.

WG Agreement #8: Business Domain Name Purchase or Sale is a legitimate purpose for "thin data" collection.

WG Agreement #9: Academic / Public Interest DNS Research is a legitimate purpose for "thin data" collection.

WG Agreement #10: Regulatory and Contractual Enforcement is a legitimate purpose for "thin data" collection.

WG Agreement #11: Criminal Investigation & DNS Abuse Mitigation is a legitimate purpose for "thin data" collection.

WG Agreement #12: Legal Actions is a legitimate purpose for "thin data" collection.

WG Agreement #13: Individual Internet Use is a legitimate purpose for "thin data" 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.

<results of further deliberation on this subquestion to be added here>

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

2.3.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Page 7:
To guide its deliberations, the EWG developed a high-level statement of purpose, using it to align this report's recommendations with ICANN's mission and design a system to support domain name registration and maintenance which:

- *Provides appropriate access to accurate, reliable, and uniform registration data;*
- *Protects the privacy of Registrant information;*
- *Enables a reliable mechanism for identifying, establishing and maintaining the ability to contact Registrants;*
- *Supports a framework to address issues involving Registrants, including but not limited to: consumer protection, investigation of cybercrime, and intellectual property protection; and*
- *Provides an infrastructure to address appropriate law enforcement needs.*

2.3.2 Draft agreements

The RDS PDP WG considered the EWG's high-level statement of purpose (above), using it as input to develop the following 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 information about the lifecycle of a domain name and its resolution on the Internet.*

[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. *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 name servers, in accordance with applicable policy.[4]*
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].*

A purpose of gTLD registration data is to provide a record of domain name registrations.

Deleted: *provide an authoritative source of information about, for example,*

Deleted: *, domain names*

Deleted: *for gTLDs, [based on approved*

Deleted: *]*

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

The following goals discussed during the 22 February and 28 February Calls were confirmed by polling but subsequently moved from the body of the statement of purpose to here, in order to serve as on-going guidance to the WG as it finishes drafting this statement of purpose:

Goals for each RDS Purpose

i. *Consistency with ICANN's mission*
ii. *Consistency with other consensus policies that pertain to generic top-level domains (gTLDs)*
iii. *To provide a framework that enables compliance with applicable laws*
iv. *To help articulate a rationale for a potential RDS*
v. *To communicate purpose(s) of the RDS to registrants (and others)*
vi. *To establish sufficient relationship between the purpose(s) and the use(s) of the RDS*

In addition, the following agreements were reached during the 7 March Call and reflected by edits to the above-draft statement of purpose:

WG Agreement #16: A purpose of gTLD registration data is to provide info about the lifecycle of a domain name.

WG Agreement #17: A purpose of RDS is to identify domain contacts and facilitate communication with domain contacts associated with gTLDs, [based on approved policy]

WG Agreement #18: A purpose of gTLD registration data is to provide a record of domain name registrations

WG Agreement #19: A purpose of RDS policy is to facilitate the accuracy of gTLD registration data

The WG also agreed to remove brackets from the above-draft purpose statement, as there were no comments on other occurrences, but leave brackets around "[based on approved policy]" to enable further discussion.

---

[2] 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.

[4] Alternatives for specific purpose 2) are still under consideration, pending WG definition of "data of record".

Deleted: "authoritative."

2.4 What are the guiding principles that should be used to determine permissible users and purposes, today and in the future?

2.4.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

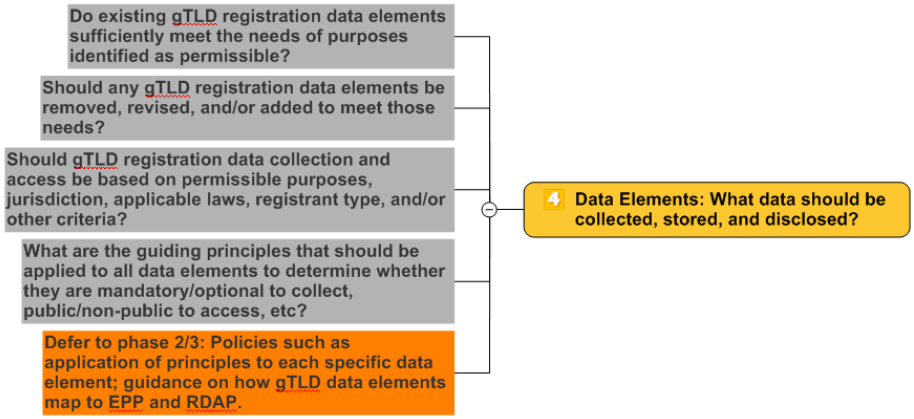
From Page 31:

No.	*Permissible Purposes Principles*
1.	*ICANN must publish, in one place, a user-friendly policy describing the purpose and permissible uses of registration data, to clearly inform Registrants why this data is being collected and how it will be handled and used.*
2.	*There must be clearly defined permissible/impermissible uses of the RDS.*
3.	*The RDS must support defined permissible purposes, including uses that involve:* • *Identifying the Registrant and contacts designated for a given purpose;* • *Communicating with contacts designated for a given purpose;* • *Using data published by Registries about Domain Names; and* • *Searching portions of registration data required for a given purpose.*
4.	*The RDS must be designed with the ability to accommodate new users and permissible purposes that are likely to emerge over time. [Phase 2/3 detail deleted]*
5.	*All identified permissible purposes should be accommodated by the RDS in some manner, with the exception of known malicious Internet activities that must be actively deterred. The EWG's recommended permissible purposes are summarized in Table 1, RDS Users and Purposes, and Figure 3, Permissible Purposes.*
6.	*gTLD registration data should be collected, validated, and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use.*
7.	*Every Registrant must have the ability to access all public and gated information published in the RDS about their domain name, including designated contact data.*

2.4.2 Draft agreements

<crafted as deliberation converges on text to answer the sub-question or give a key concept>

3. Charter Question: Data Elements



3.1 Do existing gTLD registration data elements sufficiently meet the needs of purposes identified as permissible?

3.1.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Page 10:

The EWG further analyzed all registration data elements – starting from those defined in the 2013 RAA – to derive a set of guiding principles for data collection and disclosure which dovetails with the recommended [purpose-based contact] framework, as well as with recommendations made to enable compliance with data protection laws. The EWG made further recommendations to identify new data elements that Registrants and contacts may choose to publish to make communication more robust. These recommendations are detailed in Section IV and examples given in Annex E.

From Page 29:

The scope of registration data needed to fulfil these purposes is further summarized in the following table, including domain names involved, the kinds of data needed (Registrant data, contact data, domain name data), and additional queries needed.

Purpose	*Query Scope*	*Contact(s) Needed*	*Registrant Data Needed*	*DN Data*	*Other Queries Needed*
Domain Name Control	*Own DN*	*All*	*Public+Gated*	*Yes*	*Reverse (Own Data) WhoWas (Own DN)*
Personal Data Protection	*PP DN**	*PP*	*Public*	*Yes*	*None*
Technical Issue Resolution	*Any DN*	*Tech*	*Public*	*Yes*	*None*

Domain Name Certification	*Any DN*	*None*	*Public+Gated*	*Yes*	*None*
Individual Internet Use	*LP DN**	*Business*	*Public*	*No*	*None*
Business Domain Name Purchase or Sale	*Any DN*	*Admin*	*Public+ Approved Gated*	*Yes*	*Reverse (Approved Data) WhoWas (Any DN)*
Academic/Public Interest DNS Research	*Any DN*	*All*	*Public+ Approved Gated*	*Yes*	*Reverse (Approved Data) WhoWas (Any DN)*
Legal Actions	*Any DN*	*Legal*	*Public+ Approved Gated*	*Yes*	*Reverse (Approved Data) WhoWas (Any DN)*
Regulatory and Contractual Enforcement	*Any DN*	*Legal*	*Public+Gated*	*Yes*	*Reverse (Any Data) WhoWas (Any DN)*
Criminal Investigation & DNS Abuse Mitigation	*Any DN*	*Abuse*	*Public+Gated*	*Yes*	*Reverse (Any Data) WhoWas (Any DN)*
DNS Transparency	*Any DN*		*Public*	*Yes*	*None*

Table 3. Scope of Registration Data needed for each Purpose

3.1.2 Draft agreements

<crafted as deliberation converges on text to answer the sub-question or give a key concept>

3.2 Should any gTLD registration data elements be removed, revised, and/or added to meet those needs?

3.2.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Pages 9-10:
To deliver purpose-based access to registration data while improving communication and personal privacy, the EWG developed principles for Purpose-Based Contacts (PBCs). Supported by defined roles and responsibilities, PBCs have been mapped to all permissible purposes where contact is needed. Three examples are illustrated below and further detailed in Sections III and IV [of the EWG Report].

From Page 35-36:
As summarized in Figure 4 and detailed in Table 1, the EWG analyzed representative use cases to identify the kinds of users who want access to gTLD registration data and the permissible purposes currently served by that data. To deliver purpose-based access to registration data, all permissible purposes have been mapped to PBCs. For example:

- *A "legal" contact can be designated to handle TM disputes or other legal claims regarding a domain name. To enable contact for associated purposes, this PBC just have a physical address capable of receiving legal notice, an active email address to receive inquiries, and a working phone or fax number to receive queries.*

- *An "abuse" contact can be designated to handle inquiries about abusive behavior emanating from a domain and manifesting in traffic or other highly time-sensitive malicious Internet activities. To enable contact for associated purposes, this PBC must have an email address capable of receiving and responding to valid complaints and an active phone number to receive inquiries. The PBC may also include Social Media and Instant Messaging addresses to facilitate real-time interaction, a physical address or fax number to receive queries, and a published URL that facilitates abuse reporting.*

PBCs are also recommended to designate administrative, technical, accredited Privacy/Proxy Provider, and business contacts. A complete list of PBC types and responsibilities is provided in Table 5; see also Section IV, Data Collection Principle #20, for data element needs for every PBC type.

As shown in the following figure, the EWG recommends that the Registrant's own ID be used if more specific PBCs are not provided for a given domain name. For example, if a Legal Contact has not been specified for a given domain name, the Registrant should be informed that parties may need to contact them for this permissible purpose and be given an opportunity to designate a PBC to receive such requests for this domain name.

If the Registrant opts not to designate a PBC, such requests will be sent to the Registrant, using data required for this purpose associated with the Registrant's Contact ID. If the Registrant prefers to not make public those data elements, the domain name may be registered using an accredited Privacy/Proxy service. See Section IV [of the EWG Report] for further discussion of Data Element principles and PBCs.

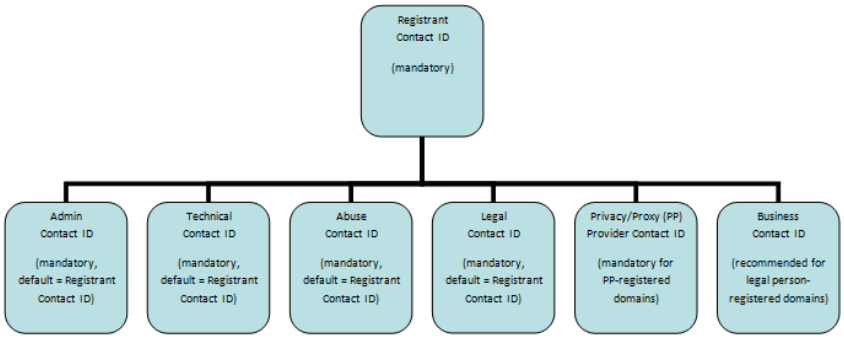


Figure 4. RDS Contact Types

From Pages 57-58 (summarized to illustrate the types of elements added):
All data elements are as defined in the 2013 RAA, with the following additions:

- *Registrar and Registry Jurisdiction*
- *Registration Agreement Language*
- *Original Registration Date*
- *Client Status, Server Status*

- *Registrant Company Identifier*
- *Registrant Contact ID*
- *Registrant/PBC Contact Validation Status Registrant/PBC Contact Last Validated Timestamp*
- *Registrant/PBC SMS, IM, Social Media*
- *Registrant/PBC Alt Email, Alt Phone, Alt Social Media*
- *Registrant/PBC Contact_URL, Abuse_URL*
- *PBC Contact ID*

For a full list of recommended Data Elements, see Section IV and Annex D of the EWG Report.

3.2.2 Draft agreements

<crafted as deliberation converges on text to answer the sub-question or give a key concept>

3.3 Should gTLD registration data collection and access be based on permissible purposes, jurisdiction, applicable laws, registrant type, or other criteria?

3.3.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Page 10:
The recommended RDS takes a clean slate approach, abandoning today's one-size-fits-all WHOIS in favor of purpose-driven access to validated data in hopes of improving privacy, accuracy and accountability. The EWG believes that this new access paradigm could increase accountability for all parties involved in the disclosure and use of gTLD domain name registration data by:

- *Logging all access to gTLD registration data, including unauthenticated access to public data elements, to enable detection and mitigation of abuses;*
- *Gating access to more sensitive data elements that would only be available to requestors who applied for and were accredited to receive RDS access, at the level appropriate for each user and stated purpose; and*
- *Auditing both public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use, in accordance with terms and conditions explicitly agreed upon by each requestor.*

From Page 41:
The only data elements that must be collected are those with at least one permissible purpose.

Not all data collected is to be public; disclosure must depend upon Requestor and Purpose.

Public access to an identified minimum data set must be made available, including PBC data published expressly to facilitate communication for this purpose.

Data Elements determined to be more sensitive (after conducting the risk & impact assessment) must be protected by gated access, based upon:

- *Identification of a permissible purpose*
- *Disclosure of requestor/purpose*
- *Auditing/Compliance to ensure that gated access is not abused*

3.3.2 Draft agreements

<crafted as deliberation converges on text to answer the sub-question or give a key concept>

3.4 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?

3.4.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Pages 41-42:

No.	*Data Element Principles*
19.	*The RDS must accommodate purpose-driven disclosure of data elements. (See Section III [of the EWG Report] for a list of permissible purposes and associated Purpose-Based Contacts (PBCs).)*
20.	*Not all data collected is to be public; disclosure must depend upon Requestor and Purpose.*
21.	*Public access to an identified minimum data set must be made available, including PBC data published expressly to facilitate communication for this purpose.*
22.	*Data Elements determined to be more sensitive (after conducting the risk & impact assessment) must be protected by gated access, based upon:* • *Identification of a permissible purpose* • *Disclosure of requestor/purpose* • *Auditing/Compliance to ensure that gated access is not abused*
23.	*Only the data elements permissible for the declared purpose must be disclosed (i.e., returned in responses or searched by Reverse and WhoWas queries).*
24.	*The only data elements that must be collected are those with at least one permissible purpose.*
25.	*Each data element must be associated with a set of permissible purposes.* • *An initial set of acceptable uses, permissible purposes, and data element needs are identified by [the EWG] report (see Section III and Annex D).* • *Each permissible purpose must be associated with clearly-defined data element access and use policies.*

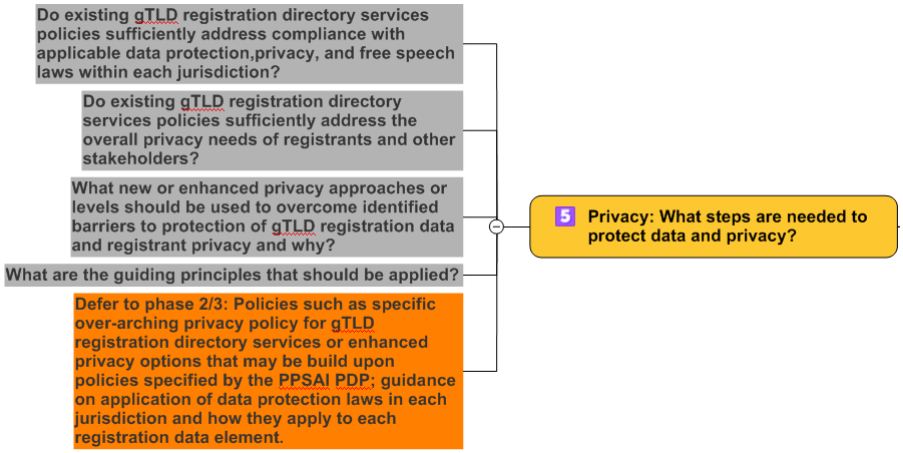
No.	Data Element Principles
	• *As specified in Section III, an on-going review process must be defined to consider proposed new purposes and periodically update permissible purposes to reflect approved additions, mapping them to existing data elements.* • *A Policy Definition process must be defined to consider proposed new data elements and, when necessary, update defined data elements, mapping them to existing permissible purposes.*
26.	*The list of minimum data elements to be collected, stored and disclosed must be based on known use cases (reflected in [the list of permissible purposes]) and a risk assessment (to be completed prior to RDS implementation).*

See also Data Collection and Data Disclosure Principles (Pages 42-46)

3.4.2 Draft agreements

<crafted as deliberation converges on text to answer the sub-question or give a key concept>

4. Charter Question: Privacy



4.1 For thin data only -- Do existing gTLD registration directory services policies sufficiently address compliance with applicable data protection, privacy, and free speech laws within each jurisdiction? If not, what requirements might those laws place on RDS policies regarding purposes associated with thin data?

4.1.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Pages 11-12:
Central to the remit of the EWG is the question of how to design a system that increases the accuracy of the data collected while also offering protections for those Registrants seeking to guard and maintain their privacy.

The EWG recognizes that personal information is protected by data protection law, and that even where there is no law, there are legitimate reasons for individuals to seek heightened protections of their personal information. In addition, some businesses and organizations may seek protection of their information for legitimate purposes, such as when they are preparing to launch a new product line, or, in the case of small business, where contact information discloses personal data.

Accordingly, the EWG formulated a set of recommendations to enable routine compliance with privacy and data protection laws, detailed in Section VI [of the EWG Report]. These principles cover:

- *Mechanisms to facilitate routine legally compliant data collection and transfer between actors within the RDS ecosystem;*

- *Standard contract clauses that are harmonized with privacy and data protection laws and codified in policy;*
- *A "rules engine" to apply data protection laws; and*
- *How RDS data storage location relates to law enforcement access.*

4.1.2 Draft agreements

<crafted as deliberation converges on text to answer the sub-question or give a key concept>

WG Agreement #14: Existing gTLD RDS policies do NOT sufficiently address compliance with applicable data protection, privacy, and free speech laws about purpose.

WG Agreement #15: As a WG, we need to agree upon a purpose statement for the RDS.
<refer to Section 2.3 for this WG's draft purpose statement>

4.2 Do existing gTLD registration directory services policies sufficiently address the overall privacy needs of registrants and other stakeholders?

4.2.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Page 12:
In addition to the privacy afforded by compliance with data protection laws, the RDS also recommended principles to accommodate needs for privacy by including within the RDS ecosystem:

- *An accredited Privacy/Proxy Service for general use; and*
- *An accredited Secure Protected Credentials Service for persons at risk and in instances where free speech rights may be denied or speakers persecuted.*

The EWG further recommends that ICANN investigate the development of a single, harmonized privacy policy that governs RDS activities in a comprehensive manner.

4.2.2 Draft agreements

<crafted as deliberation converges on text to answer the sub-question or give a key concept>

4.3 What new or enhanced privacy approaches or levels should be used to overcome identified barriers to protection of gTLD registration data and registrant privacy and why?

4.3.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Page 12:
To address needs for more uniform and reliable Privacy and Proxy Services that enable greater accountability, the EWG incorporated Privacy/Proxy communication within its PBC principles. It also recommended Privacy/Proxy principles and a framework as input to the GNSO Privacy and Proxy Services Accreditation Issues Working Group.

To address the needs of individuals and groups who can demonstrate that they would be at risk if identified in registration data, the EWG recommends a Secure Protected Credential framework whereby those parties may anonymously apply for and receive domain names registered using secure credentials, aided by attestors and trusted third parties to provide a shield between at-risk entities and Registrars. The EWG recommends that ICANN facilitate the establishment of an independent trusted review board that will validate claims of at-risk organizations or individuals to approve (and when necessary, revoke) credentials.

4.3.2 Draft agreements

<crafted as deliberation converges on text to answer the sub-question or give a key concept>

4.4 What are the guiding principles that should be applied?

4.4.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Page 81:
In its work, the EWG has been guided by some overarching legal principles:

Personal data must be:

- *processed lawfully, fairly and in a transparent manner in relation to the data subject,*
- *collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,*
- *adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed, and*
- *accurate and kept up-to-date as required for the specified purposes.*
- *Lawful processing, including transfer and disclosure can be – subject to the relevant jurisdiction – based on:*
- *consent of the data subject,*
- *the necessity for the performance of a contract to which the data subject is party, and*
- *the necessity for compliance with a legal obligation to which the controller is subject.*
- *A right of access to information and a right to rectify inaccuracy for the data subject have to be ensured.*

The EWG recommends that these and other related principles normally found in data protection law should be considered when drafting final policies and implementation processes for the RDS. In addition, it is well recognized that, in some jurisdictions, privacy rights extend to legal persons and to entities with

respect to free speech and freedom of association. The EWG recognizes both of these separate sets of rights, which are protected separately and differently around the globe.

Given this foundation, the EWG assessed options and then formulated RDS principles for privacy and data protection, and for law enforcement access. Those EWG principles are presented in this section, supported by principles for contractual compliance, accountability, and audit.

From Pages 88-90:

No.	*Data Protection Principles*
105.	*Mechanisms must be adopted to facilitate routine legally compliant data collection and transfer between actors within the RDS ecosystem.*
106.	*Standard contract clauses that are harmonized with privacy and data protection laws should be codified in a policy and enforced through contracts between all RDS ecosystem actors involved in handling personal information.*
107.	*An information system to apply data protection laws (i.e., a "rules engine") and localization of RDS data storage must be considered as two means of implementing the high level of data protection required. This must be ensured through standard contractual clauses, which flow from a logical privacy policy for the RDS ecosystem.*
No.	*Law Enforcement Access Principles*
108.	*The RDS must store data in jurisdiction(s) where law enforcement is globally trusted, regardless of implementation model.*

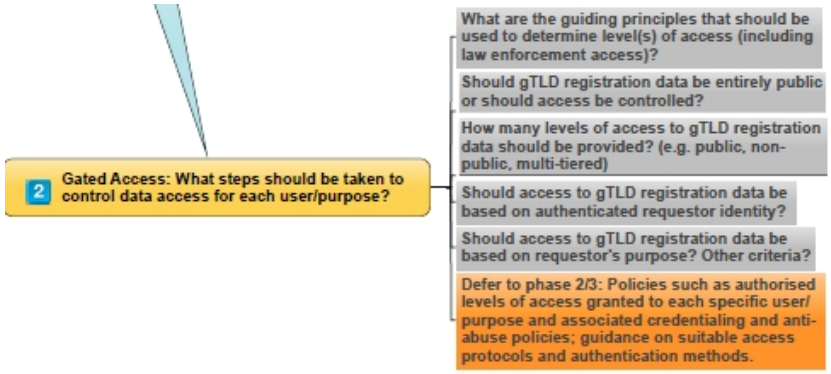
See also Accredited Privacy/Proxy Services Principles (Page 100) and Principles for Secure Protected Credentials (Page 106).

4.4.2 Draft agreements

<crafted as deliberation converges on text to answer the sub-question or give a key concept>

NEW SECTION 5 INSERTED AS STARTING POINT FOR TASK 12.b

5. Charter Question: Gated Access



5.1 Should gTLD registration data be entirely public or should access be controlled?

5.1.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Page 58:
The EWG recommends that a new approach be taken for registration data access, abandoning entirely anonymous access by everyone to everything in favor of a new paradigm that combines public access to some data with gated access to other data.

From Pages 61-62:
As depicted in the following figure, public data elements can still be requested from the RDS by anyone, with or without authentication. Refer to Annex E for more detailed illustration of data elements returned to an unauthenticated public data query.

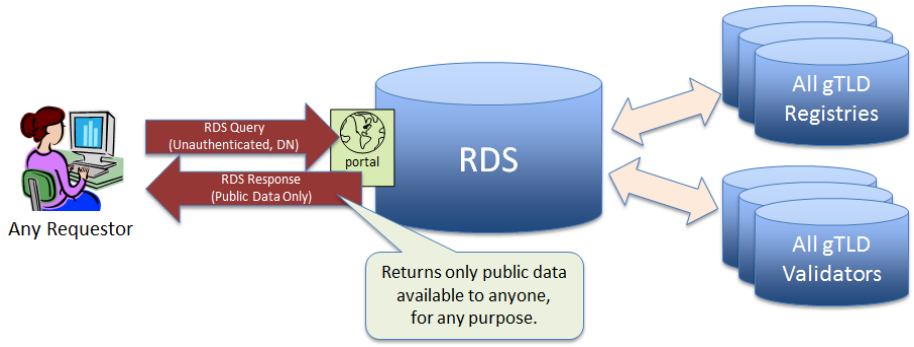


Figure 6. Unauthenticated Public Registration Data Access via RDS

Annex I also contains flow charts and an example use case to illustrate the steps involved in accessing the relevant data elements.

As depicted in the following figure, gated data elements can also be requested via the RDS. To do so, requestors must first be accredited. Thereafter, requestors may submit authenticated queries requesting data elements for a stated purpose. Refer to Annex E for more detailed illustration of data elements returned to an authenticated gated data query.

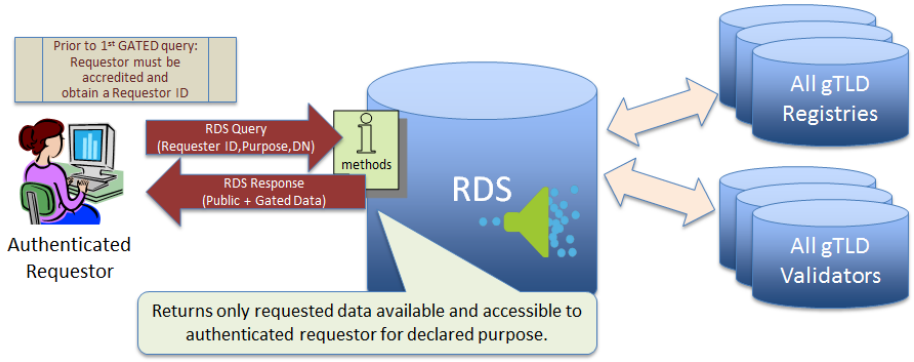


Figure 7. Gated Registration Data Access via RDS

5.1.2 Draft agreements

Should gTLD registration "thin data" be entirely public or should access be controlled?

WG Agreement #20: gTLD registration "thin data" must be accessible without requestor identification, authentication, or stated purpose.

Deleted: should

Deleted: requiring inquirers to identify themselves or state their purpose

Proposed WG Agreement #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. [Rough consensus in 2 May poll, but pending action item]

5.2 How many levels of access to gTLD registration data should be provided? (e.g., public, non-public, multi-tiered)

5.2.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Pages 58-59:
A minimum set of data elements, at least in line with the most stringent privacy regime, must be accessible by unauthenticated RDS users.

Multiple levels of authenticated data access must be supported, consistent with stated permissible purposes.

From Page 47 (how access principles apply to thick vs. thin data elements):
To maximize Registrant privacy, Registrant-supplied data must be gated by default, except where there is a compelling need for public access that exceeds resulting risk. Registrants can opt into making any gated Registrant-supplied data public with informed consent.

To maximize Internet stability, all Registry or Registrar-supplied registration data must be always public, except where doing so results in unacceptable risk. Registrants can opt into making any public Registry/Registrar-supplied data gated, except as noted below to enable basic domain control.

To meet basic domain control needs, the following Registrant-supplied data, which is mandatory to collect and low-risk to disclose, must be included in the minimum public data set. [Refer to EWG Report Page 46 for list of data elements; refer to section 3 of this document for the RDS PDP WG's agreements on thin data element requirements.]

5.2.2 Draft agreements

<crafted as deliberation converges on text to answer the sub-question or give a key concept>

5.3 Should access to gTLD registration data be based on authenticated requestor identity?

5.3.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

See Charter Question 5 – Handout – For9MayCall.pdf:

5.3.2 Draft agreements

<agreement(s) to be inserted here as deliberation converges on answer or key concept>

5.4 Should access to gTLD registration data be based on requestor's purpose? Other criteria?

5.4.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Page x:
<insert here>

5.4.2 Draft agreements

<agreement(s) to be inserted here as deliberation converges on answer or key concept>

5.5 What guiding principles should be applied to determine level(s) of access?

5.5.1 Starting point for deliberation

The following excerpts are taken from EWG Report as a starting point for deliberation.

From Pages 58-60:
The EWG recommends that a new approach be taken for registration data access, abandoning entirely anonymous access by everyone to everything in favor of a new paradigm that combines public access to some data with gated access to other data. Principles that reflect this recommendation follow.

No.	*Data Access Principles*
41.	*A minimum set of data elements, at least in line with the most stringent privacy regime, must be accessible by unauthenticated RDS users.*
42.	*Multiple levels of authenticated data access must be supported, consistent with stated permissible purposes.*
43.	*RDS user access credentials must be tied to an auditable accreditation process, as further defined in Section IV(c), RDS User Accreditation.*
44.	*Access must be non-discriminatory (i.e., the process must create a level playing field for all requestors, within the same purpose).*

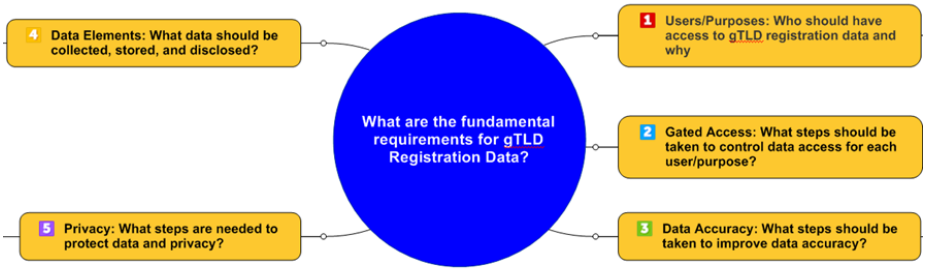
No.	Data Access Principles
45.	*To deter misuse and promote accountability:* • *All data element access must be based on a stated purpose;* • *Access to gated data elements must be limited to authenticated requestors that assert a permissible purpose; and* • *Requestors must be able to apply for and receive credentials for use in future authenticated data access queries.*
46.	*Some type of accreditation must be applied to requestors of gated access:* • *When accredited Requestors query data, their purpose must be stated every time a request is made.* • *Different terms and conditions may be applied to different purposes.* • *If accredited requestors violate terms and conditions, penalties must apply.*
51.	*All disclosures of gated data elements must occur through defined RDS access methods … The entire RDS data set for all gTLDs (or the entire Registry data set for a single gTLD) must not be exported in bulk form for uncontrolled access.*

Additional principles are defined in the EWG report, covering access methods, protocols that can be used to support them, transliteration/translation requirements, and possible approaches to carry out RDS user accreditation.

5.4.2 Draft agreements

<agreement(s) to be inserted here as deliberation converges on answer or key concept>

6. Next Steps: All Fundamental Questions posed by the WG's Charter



From the RDS PDP WG charter:

During Phase 1, the PDP WG should, at a minimum, attempt to reach consensus recommendations regarding the following questions:

- What are the fundamental requirements for gTLD registration data?
  When addressing this question, the PDP WG should consider, at a minimum, users and purposes and associated access, accuracy, data element, and privacy requirements.

- Is a new policy framework and next-generation RDS needed to address these requirements?
  - If yes, what cross-cutting requirements must a next-generation RDS address, including coexistence, compliance, system model, and cost, benefit, and risk analysis requirements?
  - If no, does the current WHOIS policy framework sufficiently address these requirements? If not, what revisions are recommended to the current WHOIS policy framework to do so?

To reach this point in Phase deliberation, the WG must consider the three charter questions detailed in this excerpt, along with the two additional charter questions listed above. This deliberation is reflected in the RDS PDP WG's work plan as Task 12, leading to publication of the WG's first initial report for public comment (Task 13).