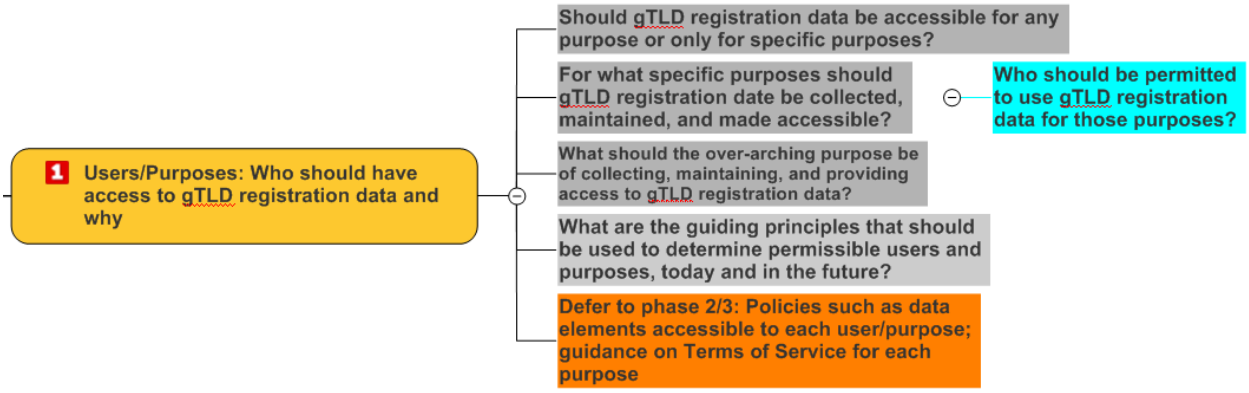
Key Concepts Deliberation Approach, guided by
RDS PDP WG Mind Map – 3 Fundamental Questions, mapped to EWG Report Excerpts

Charter Question: Users and Purposes



The following excerpts are taken from EWG Report (except as noted) as a starting point for deliberation.

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

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.

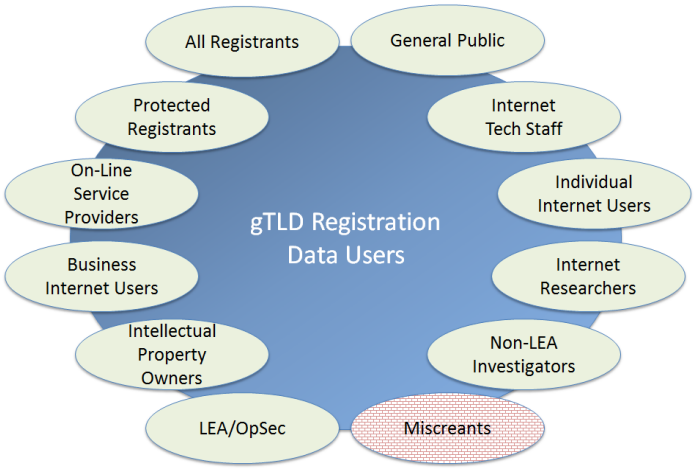
Instead, the EWG recommends a paradigm shift to a next-generation RDS that collects, validates and discloses gTLD registration data for permissible purposes only.

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.

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?

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.

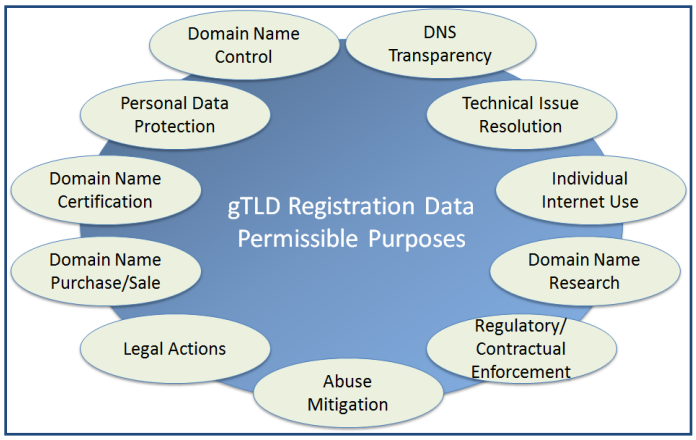
The EWG considered the totality of these use cases and the lessons learned from them, as well as reference material and community input, to derive a consolidated set of users and permissible purposes that must be accommodated by the RDS and potential misuses that must be deterred.



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.*

Purpose	***Includes tasks such as…***
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 instill 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 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.*

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

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.*

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 (v10):

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. To ensure that the purposes are understood in the appropriate context, a list of goals for each RDS purpose is also provided.

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.]

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*

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.*
2. *A purpose of RDS is to provide an authoritative source of information about, for example, domain contacts[2], domain names and name servers for gTLDs, [based on approved 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.*
5. *A purpose of RDS [policy] is to promote the accuracy of gTLD registration data.*

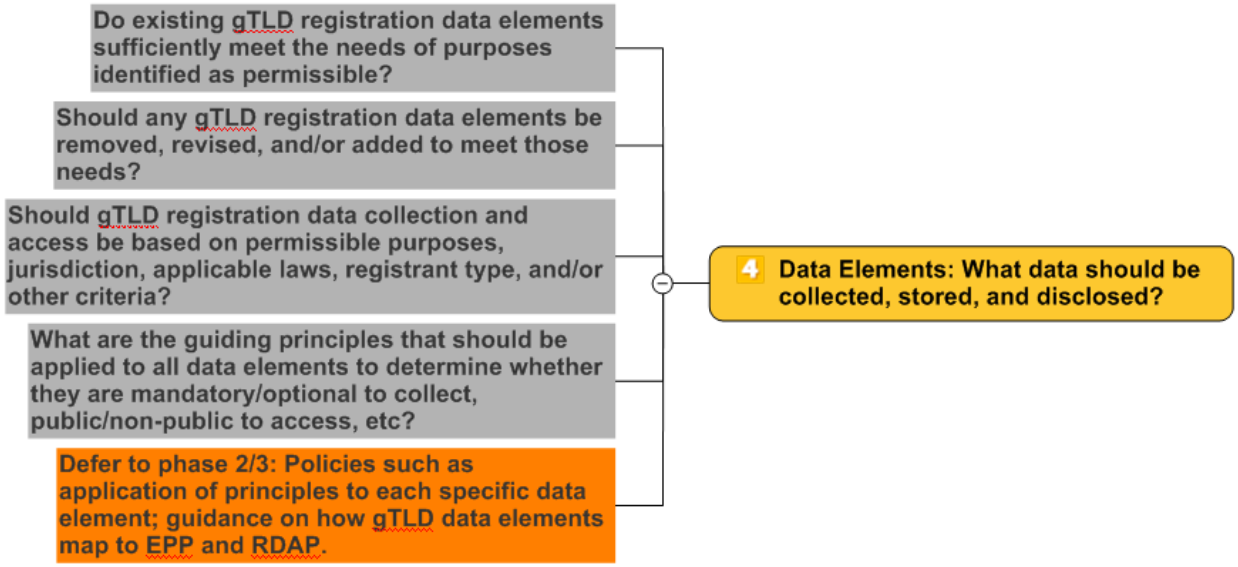
[1] Here, "registration data elements" refers to data about generic top-level domain names collected in the relationship between registrars to registries and in the relationship between registrars/registries and ICANN.
[2] Contacts related to the domain name, including those directly related to the domain name and also those involved in the registration system as relevant. Further specification may occur at a later stage in the [RDS PDP] process.

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

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.*

Charter Question: Data Elements



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

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

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

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

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.

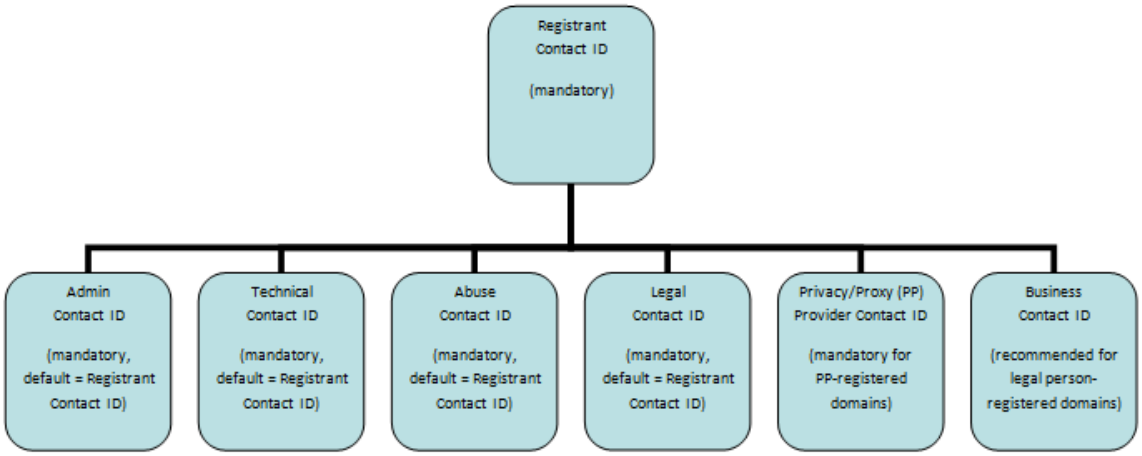


Figure 4. RDS Contact Types

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.

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

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*

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?

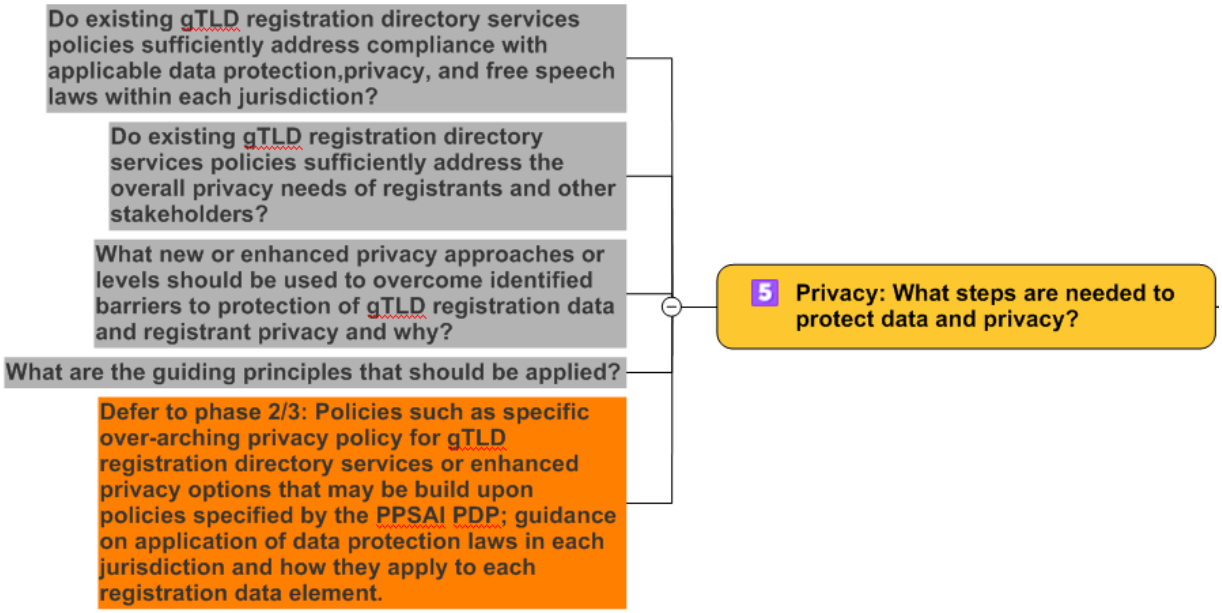
From Pages 41-42:

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).)*

No.	*Data Element Principles*
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.* • *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)

Charter Question: Privacy



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

Do existing gTLD registration directory services policies sufficiently address compliance with applicable data protection, privacy, and free speech laws within each jurisdiction?

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.*

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

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.

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?

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.

What are the guiding principles that should be applied?

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.

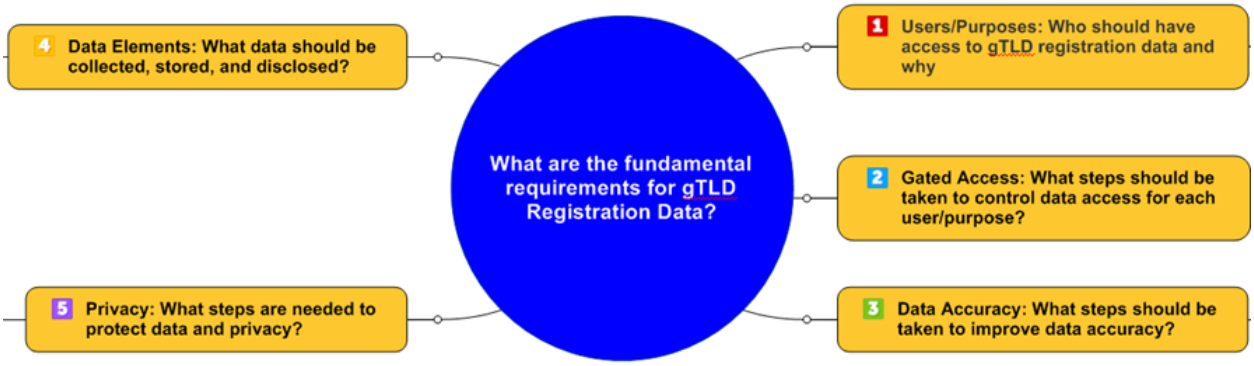
From Pages 88-90:

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).

Key Concepts Deliberation Approach, guided by
RDS PDP WG Mind Map – 3 Fundamental Questions, mapped to EWG Report Excerpts

<u>These are 3 of the 5 Fundamental Questions posed by the WG's Charter</u>



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).