



Next-Generation gTLD Registration
Directory Service (RDS) to replace WHOIS
ICANN57 F2F Meeting Slides

RDP PDP WG | ICANN58 | 11 March 2017

Agenda

1

Introductions
& SOI Updates

2

PDP Work Plan,
Progress, &
Status

3

PDP Working
Session


4

Confirm action
items & proposed
decision points

5


Links to
Meeting Materials





WG Member Introductions and SOI Updates

Agenda Item #1



**PDP Work Plan, Progress,
and Status**
Agenda Item #2

Phase 1 Work Plan

Currently, we are working on Task 12.a: Deliberate on Possible Fundamental Requirements for these charter questions:

- **Users/Purposes:** Who should have access to gTLD registration data and why?
- **Data Elements:** What data should be collected, stored, and disclosed?
- **Privacy:** What steps are needed to protect data and privacy?

Since ICANN57, we have focused on **Key Concepts** for “**thin data**” and **collection** only, using polls to confirm informal rough consensus on **19 agreements** (see next slide)

- 1 • Form WG leadership team
- 2 • Review WG membership for gaps
- 3 • Establish WG meeting schedule
- 4 • Review, identify, & summarize key inputs to PDP
- 5 • Review PDP Rules of Engagement
- 6 • Develop PDP WG Work Plan
- 7 • Formal Early Outreach to ICANN SOs/ACs/SGs/Cs
- 8 • Develop Initial Possible Requirements List
- 9 • Informal Outreach on Initial Possible Requirements List
- 10 • Finalize Initial Possible Requirements List
- 11 • Decide how to reach consensus during deliberation
- 12 • Deliberate on possible Fundamental Requirements
- 13 • Publish First Initial Report for Phase 1 Public Comment
- 14 • Review/analyze Public Comments on First Initial Report
- 15 • Expand Phase 1 Work Plan based on Task 12 outcome
- 16 • Deliberate on possible Cross-cutting Requirements for NG RDS or WHOIS
- 17 • Finalize Draft Recommendations
- 18 • Publish Second Initial Report for Phase 1 for Public Comment
- 19 • Review/analyze Public Comments on Second Initial Report
- 20 • Publish Final Report for Phase 1

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

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

1. The WG should continue deliberation on the purpose(s) of "thin data."
2. Every "thin data" element should have at least one legitimate purpose.
3. Every existing "thin data" element does have at least one legitimate purpose for collection.

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

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

From Key Concepts Working Document:
<https://community.icann.org/x/p4xlAw>.

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

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?

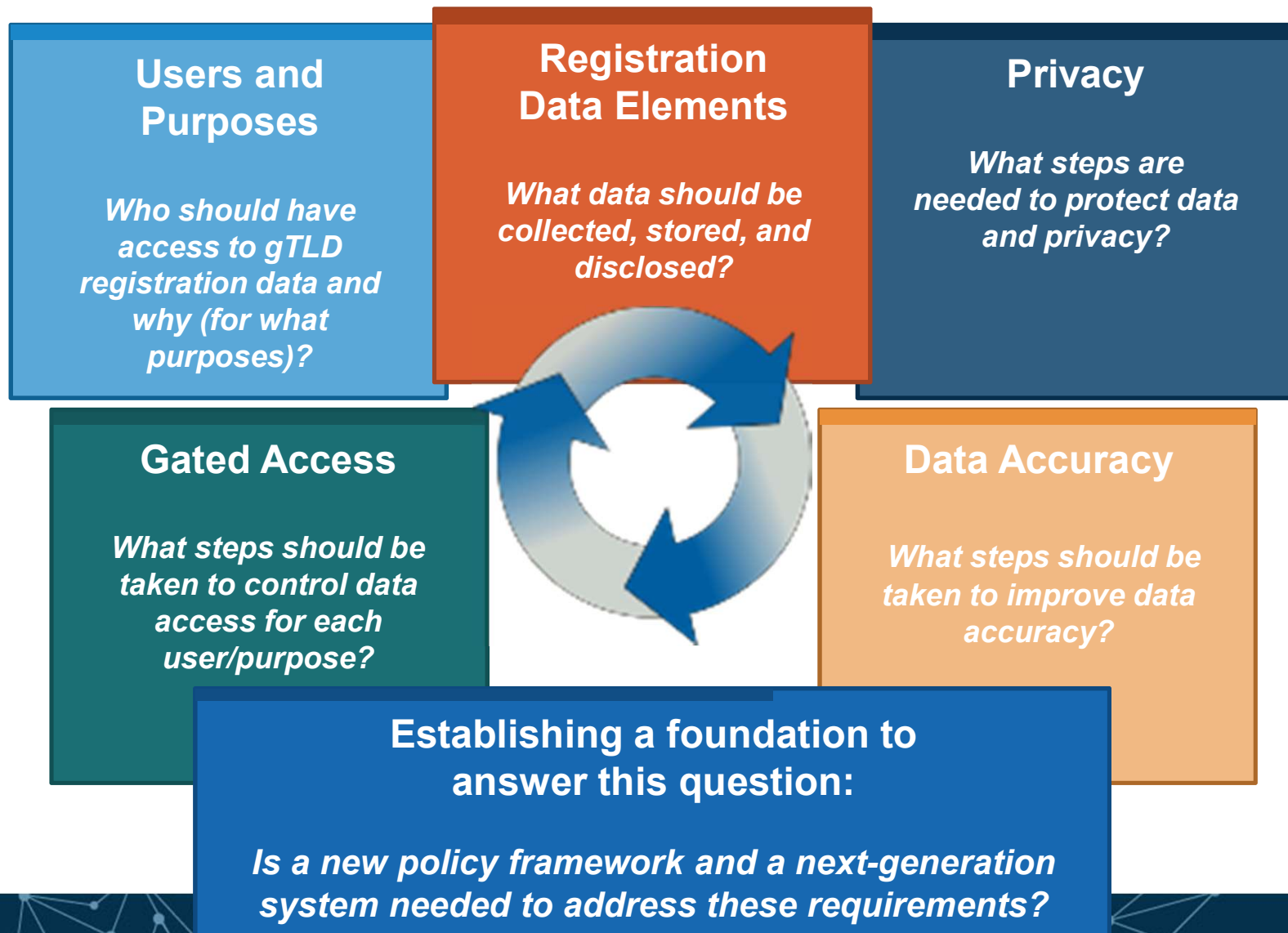
14. Existing gTLD RDS policies do NOT sufficiently address compliance with applicable data protection, privacy, and free speech laws about purpose.
15. As a WG, we need to agree upon a purpose statement for the RDS.

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

16. A purpose of gTLD registration data is to provide info about the lifecycle of a domain name.
17. A purpose of RDS is to identify domain contacts and facilitate communication with domain contacts associated with gTLDs, [based on approved policy]
18. A purpose of gTLD registration data is to provide a record of domain name registrations
19. A purpose of RDS policy is to facilitate the accuracy of gTLD registration data

From Key Concepts Working Document:
<https://community.icann.org/x/p4xlAw>.

Our first Initial Report will use rough consensus on fundamental requirements in 5 areas to answer one big question





PDP Working Session

Agenda Item #3

a. Finalize prep for sessions with Data Commissioners

- See [RDSPDP-QuestionsForDataCommissioners-7March2017.pdf](#)
 - Purpose
 - Registration Data Elements
 - Access to Registration Data for Criminal and Abuse Investigations
 - Personal Privacy/Human Rights
 - Jurisdiction
 - Compliance with Applicable Laws
 - Consumer Protection
- Some may be covered in the cross-community discussion with Data Commissioners on Monday 13 March at 15:15 CET: <http://sched.co/9nnl>
- Others can be covered in our WG's Wednesday F2F meeting with data protection experts: <https://community.icann.org/x/HbLRAw>
- Goal is to sharpen our understanding of data protection concepts, to inform our deliberation on registration data and RDS requirements

Need 7 volunteers (one per category) to listen for and ask our questions

b. Continue our deliberation on Purpose

- Continue our deliberation on Purpose, starting with Question 2.3:

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

- Review results of 7 March Poll on Purpose
- Finalize Statement of Purpose
- Move on to next topic of deliberation by returning to Question 2.2, expanding our focus from “thin data” collection to “thin data” access:

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

Summary of Poll Results: Q2

Q2 To arrive at an alternative wording that better reflects rough consensus, please indicate which of the following alternatives (if any) that you prefer

Answer Choices	Responses
<ul style="list-style-type: none"> A purpose of RDS is to provide authoritative gTLD registration data, such as domain names and their domain contacts and name servers, in accordance with applicable policy. 	27.78% 5
<ul style="list-style-type: none"> A purpose of RDS is to provide authoritative gTLD registration data, such as domain names and their domain contacts and name servers, as authorized by applicable policy. 	16.67% 3
<ul style="list-style-type: none"> A purpose of RDS is to facilitate dissemination of authoritative gTLD registration data, such as domain names and their domain contacts and name servers, in accordance with applicable policy. 	16.67% 3
<ul style="list-style-type: none"> A purpose of RDS is to facilitate dissemination of authoritative gTLD registration data, such as domain names and their domain contacts and name servers, as authorized by applicable policy. 	16.67% 3
<ul style="list-style-type: none"> A purpose of RDS is to facilitate dissemination of gTLD registration data, such as domain names and their domain contacts and name servers, in accordance with applicable policy. 	50.00% 9
<ul style="list-style-type: none"> A purpose of RDS is to facilitate dissemination of gTLD registration data, such as domain names and their domain contacts and name servers, as authorized by applicable policy. 	11.11% 2
Total Respondents: 18	

Q2 Comments

- a) (1) Any of these would likely work, as would the one checked with "provide" swapped in (that option was not provided). (2) In our current RDS, this data is made available both by registrars and (thick) registries. They sometimes differ. Only one can be authoritative. But the system provides both. This is my hesitancy about "authoritative."
- b) I'm not comfortable with including "authoritative" unless we have a corresponding definition of the word. My concern is based on a belief that people may associate possession with authority and I do not believe that association is always correct.
- c) My definition of "authoritative" is "the data that's in the registry." That's the standard industry and the historical understanding. It means that contact data in the registry (and thus the RDS) can be inaccurate, but it's what's on the record. "Facilitate dissemination" is a poor substitute that doesn't add anything and may even be inaccurate. "Facilitate" means "to make (an action or process) easy or easier." But either RDS provides registration data or it does not, and a basic purpose of RDS is certainly to provide registration data. "Facilitate dissemination" is more about the HOW or TO WHOM, and those issues are covered under "applicable policy."
- d) don't think domain-contacts should be in the 'such as' as the WG has not yet decided if 'thick' data is appropriate
- e) RDS in its simplest form is a data set. It needs to be authoritative and set up in accordance with applicable policy. "As authorized by" is redundant and unnecessary. The "to facilitate dissemination of" is a separate issue. First, what data set to assemble as authoritative. Second, what are the policies around facilitating dissemination (how about simply saying "access").

Summary of Poll Results: Q3

Q3 Is there anything missing from the latest draft statement of purpose (below) that you suggest be added?

Answer Choices	Responses
▼ No, not at this time	72.22% 13
▼ Yes (please describe below)	27.78% 5
Total	18

- a. As I mentioned before, as worded it seems like the second paragraph of above statement is defining an RDS incorrectly as a system that collects and maintains data. This paragraph is trying to make the distinction between registration data and directory services but as worded I don't think it draws a clear line.
- b. actually, I think we are not ready to decide on this statement at this time. It is not clear to me that we are talking about the same things when we discuss the purpose of RDS. More work required.
- c. I would reworded to say: the purpose of a RDS is to facilitate dissemination of gTLD registration data
- d. A purpose of RDS policy is to protect the privacy of individuals and ensure that gTLD registration data is disseminated only as authorized by applicable policy.
- e. as authorized by applicable policy

Finalize 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 elements¹ 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.*
- 2. A purpose of RDS is to provide an authoritative source of information about, for example, domain contacts², 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 facilitate the accuracy of gTLD registration data.*

Note: (2) above will be revised, based on the results of this poll.

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.

Next: Purposes for Providing Access to “Thin Data”

Previously, we reached informal rough consensus on a narrowed Question 2.2:

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

Next, let’s return to Question 2.2 and expand our focus as follows:

*For what specific (legitimate) purposes should gTLD registration **thin data elements** be made accessible?*

PURPOSES FOR “THIN DATA” COLLECTION

- Domain Name Control
- Technical Issue Resolution
- Domain Name Certification
- Business DN Purchase or Sale
- Academic/Public Interest DNS Research
- Regulatory and Contractual Enforcement
- Criminal Investigation & DNS Abuse Mitigation
- Legal Actions
- Individual Internet Use

Example of Thin WHOIS record

Domain Name: CNN.COM
Registrar: CSC CORPORATE DOMAINS, INC.
WHOIS Server: whois.corporatedomains.com
Referral URL: <http://www.cscglobal.com>
Name Server: NS1.TIMEWARNER.NET
Name Server: NS3.TIMEWARNER.NET
Name Server: NS5.TIMEWARNER.NET
Status: clientTransferProhibited
Updated Date: 04-feb-2010
Creation Date: 22-sep-1993
Expiration Date: 21-sep-20184

Source: [GNSO PDP on Thick WHOIS Final Report](#)

Purposes for collection? Purposes for providing access?

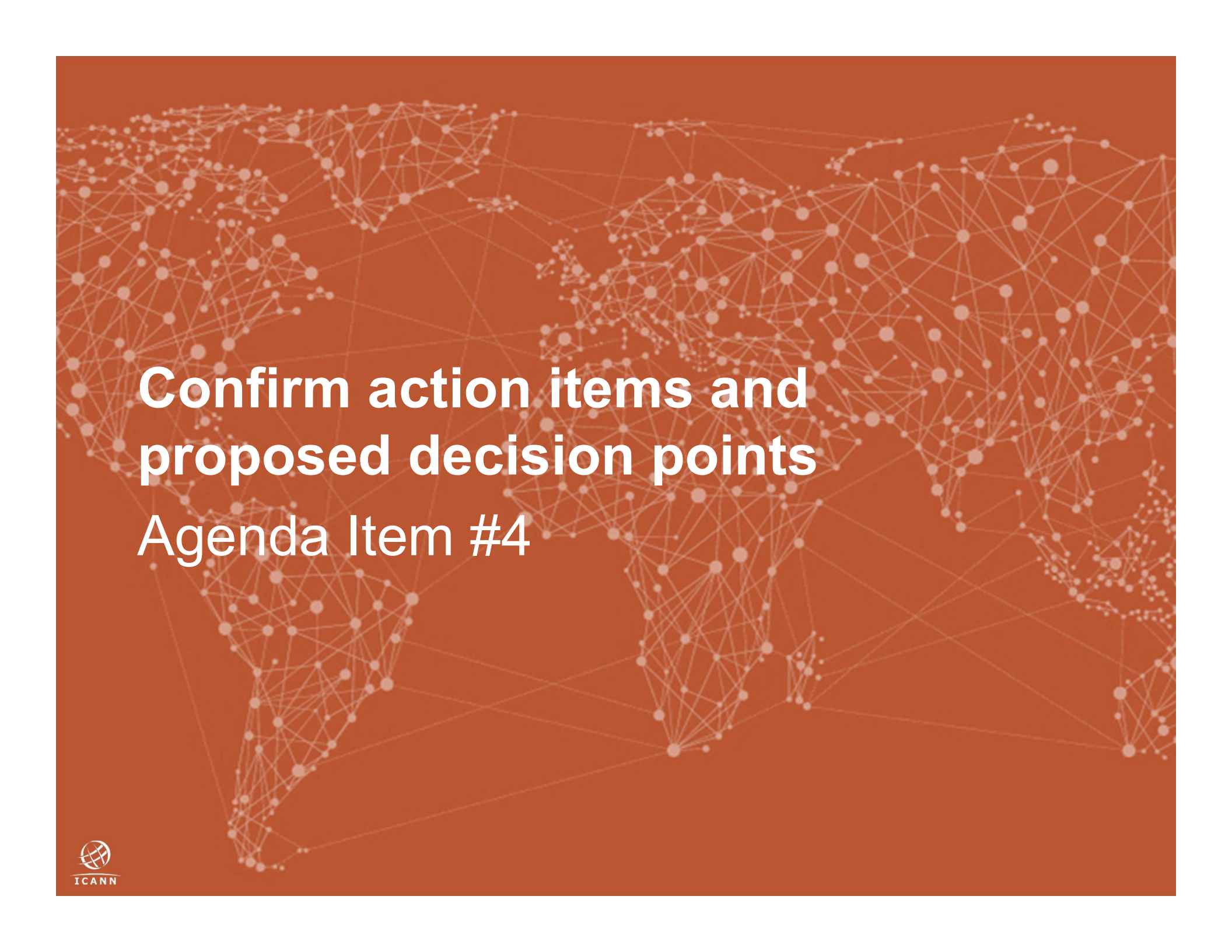
Purposes identified for Thin Data	Includes tasks such as... (Note: may involve more than thin data)	Related Thin Data Elements	Example Use Cases developed by PDP WG (Note: may involve more than thin data)
Domain Name Control	Creating, managing and monitoring a Registrant's own domain name (DN), including 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.	Domain Name [Name Servers] Sponsoring Registrar Registrar's RDS/WHOIS URL Registration Status(es) Registration Creation Date Registration Expiration Date RDS/WHOIS Last Updated Date	DN maintenance - Transfer DN maintenance - Deletions DN maintenance - DNS Changes DN maintenance - Renewal
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 [Name Servers] Sponsoring Registrar Registrar's RDS/WHOIS URL Registration Status(es) Registration Creation Date Registration Expiration Date RDS/WHOIS Last Updated Date	Technical Issue Resolution Technical Issue Resolution (specific examples)
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.	Domain Name Name Servers	Certification Authority
Business Domain Name Purchase or Sale	Making purchase queries about a DN, acquiring a DN from another Registrant, and enabling due diligence research.	Domain Name Name Servers Sponsoring Registrar Registrar's RDS/WHOIS URL Registration Status(es) Registration Creation Date Registration Expiration Date RDS/WHOIS Last Updated Date	Business DNs - Bankruptcy Asset Purchase Business DNs - Mergers and Acquisitions Business Intelligence

Purposes for collection? Purposes for providing access?

Purposes identified for Thin Data	Includes tasks such as... (Note: may involve more than thin data)	Related Thin Data Elements	Example Use Cases developed by PDP WG (Note: may involve more than thin data)
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 DNSs registered by a given Registrant.	Domain Name Name Servers Sponsoring Registrar Registrar's RDS/WHOIS URL Registration Status(es) Registration Creation Date Registration Expiration Date RDS/WHOIS Last Updated Date	None developed by PDP WG EWG example cases include: DN Registration History DNs for Specified Contact Survey DN Registrant or Contact
Regulatory and Contractual Enforcement	Tax authority investigation of businesses with online presence, UDRP [and URS] investigation, contractual compliance investigation, and registration data escrow audits.	Domain Name Name Servers Sponsoring Registrar Registrar's RDS/WHOIS URL Registration Status(es) Registration Creation Date Registration Expiration Date RDS/WHOIS Last Updated Date	Services required by Registry Agreement
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.	Domain Name Name Servers Sponsoring Registrar Registrar's RDS/WHOIS URL Registration Status(es) Registration Creation Date Registration Expiration Date RDS/WHOIS Last Updated Date	Investigate Abusive Domain Find Domains Registered by Miscreant Reputation Services Law Enforcement - Compromised websites WHOIS queries for compliance purposes

Purposes for collection? Purposes for providing access?

Purposes identified for Thin Data	Includes tasks such as... (Note: may involve more than thin data)	Related Thin Data Elements	Example Use Cases developed by PDP WG (Note: may involve more than thin data)
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.	Domain Name Other Thin Data Elements?	Obtain DN holder details for legal action Fraudulent contact information Trademark Infringement
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.	Domain Name Other Thin Data Elements?	Real-World Contact



**Confirm action items and
proposed decision points**
Agenda Item #4



Links to Meeting Materials

Agenda Item #5

Sessions at ICANN58 and Further Information

- Open Working Group meeting/community sessions:
Saturday 11 March 13:45 CET: <http://sched.co/9npN> and
Wednesday 15 March 13:45 CET: <http://sched.co/9npc>
- Background information:
Background Docs: <https://community.icann.org/x/QlxlAw>
Phase 1 Docs: <https://community.icann.org/x/p4xlAw>
- ICANN58 Background Briefing Paper:
<http://gnso.icann.org/en/issues/policy-briefing-next-gen-rds-27feb17-en.pdf>
- Working Group Charter:
<https://community.icann.org/x/E4xlAw>
- Working Group online wiki space (with meeting transcripts,
call recordings, draft documents and background materials):
<https://community.icann.org/x/rjJ-Ag>

To learn more



Thank You and Questions

Reach us at:

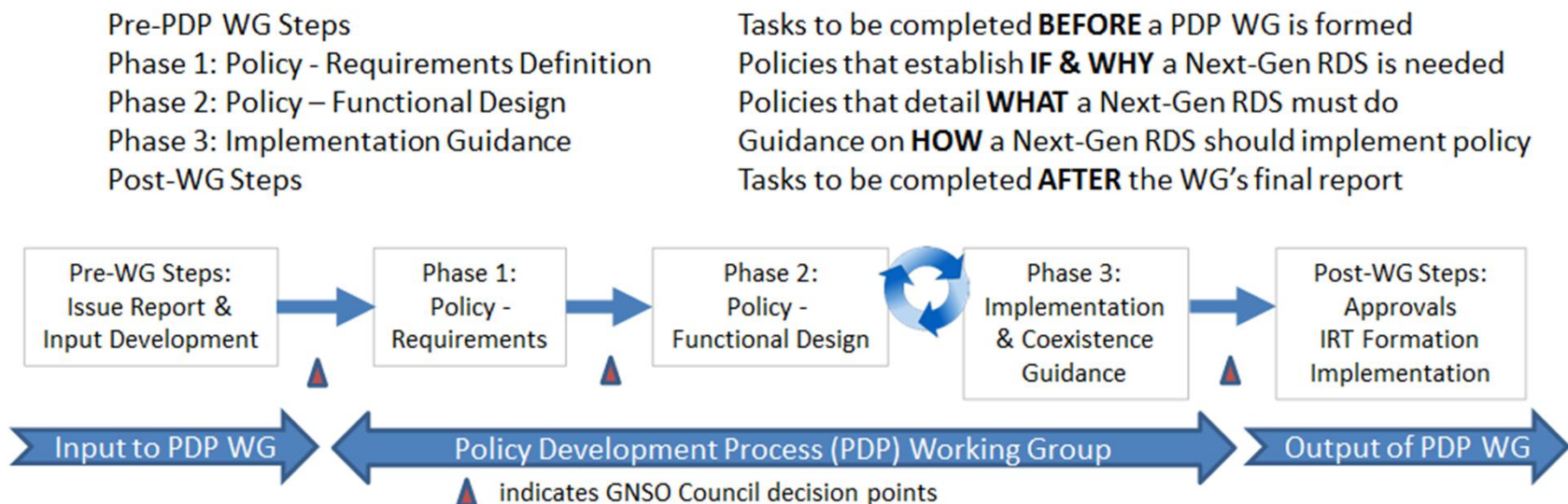
Email: gns0-rds-pdp-wg@icann.org

Website: <http://tinyurl.com/ng-rds>



Background on this PDP

- ⦿ This PDP has been tasked with defining the purpose of collecting, maintaining and providing access to gTLD registration data and considering safeguards for protecting that data, determining if and why a next-generation Registration Directory Service (RDS) is needed to replace WHOIS, and creating policies and coexistence and implementation guidance to meet those needs.

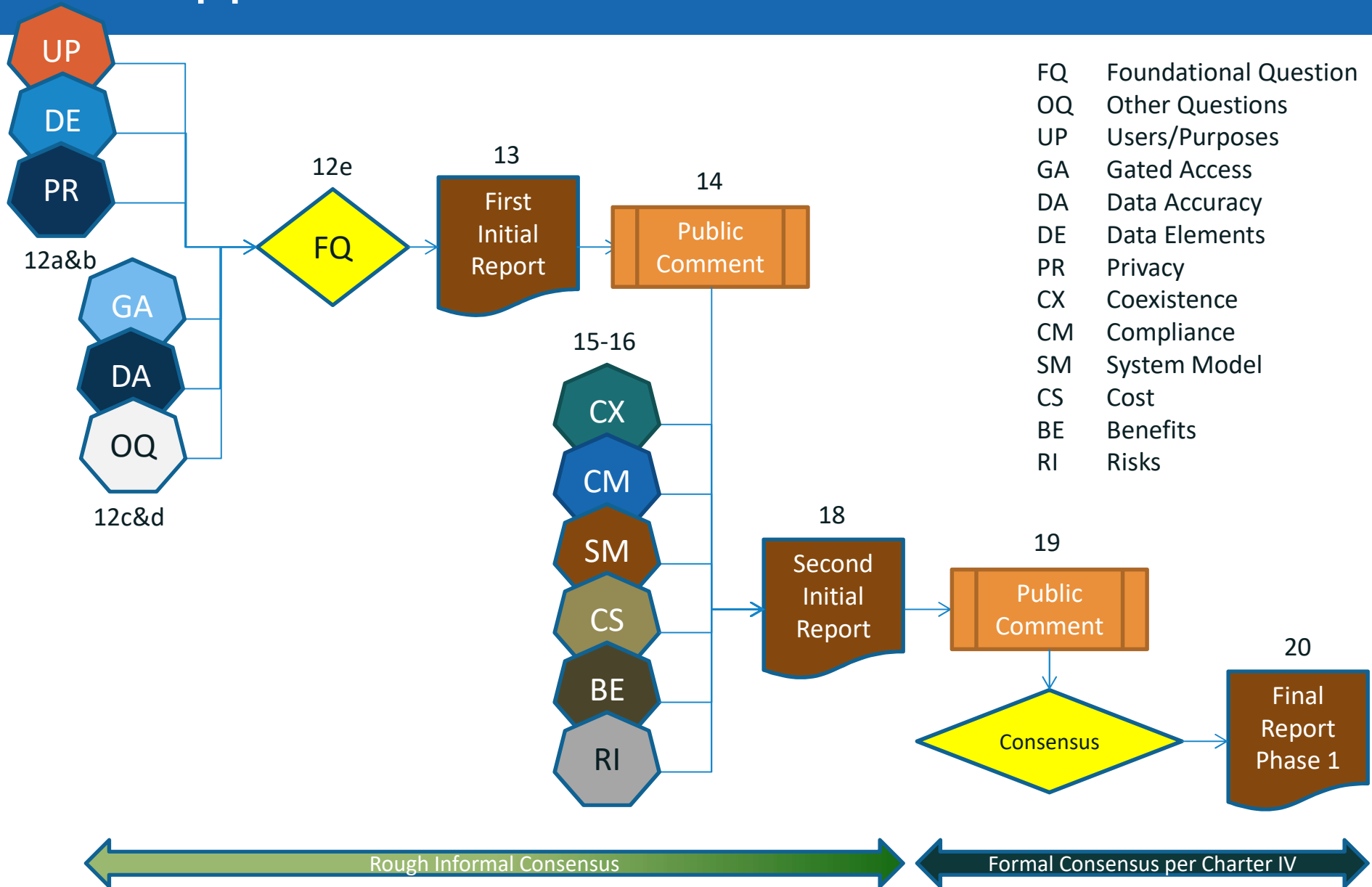


During Phase 1, this WG will



- Attempt to reach consensus on the following (*at a minimum*):
- **What are the fundamental requirements for gTLD registration data?**
When addressing this, the PDP WG should consider, at a minimum, *users & purposes, access, accuracy, data elements, and privacy*
- **Is a new policy framework and a next-generation system needed to address these requirements?**
 - **If yes, what cross-cutting requirements must any 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?

Approach to reach consensus in Phase 1



Task #s are taken from Work Plan @ <https://community.icann.org/x/olxlAw>

Starting with Task 12a (3 charter questions)

1 Users/Purposes: Who should have access to gTLD registration data and why

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

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

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?

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

Defer to phase 2/3: Policies such as data elements accessible to each user/purpose; guidance on Terms of Service for each purpose

Iterating in a randomized manner



4 Data Elements: What data should be collected, stored, and disclosed?

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?

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

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

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

Defer to phase 2/3: Policies such as application of principles to each specific data element; guidance on how gTLD data elements map to EPP and RDAP.

5 Privacy: What steps are needed to protect data and privacy?

What are the guiding principles that should be applied?

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

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

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?

Defer to phase 2/3: Policies such as specific over-arching privacy policy for gTLD registration directory services or enhanced privacy options that may be build upon policies specified by the PPSAI PDP; guidance on application of data protection laws in each jurisdiction and how they apply to each registration data element.

Charter Questions

Sub-Questions

Sub-sub questions

Examples of topics to be considered in phase 2/3

Questions for Data Commissioners - Purpose

Purpose

1. Our working group is now deliberating upon the purpose of domain name registration data and the registration directory system that provides public access to that data. Can you please help us understand what the data protection supervisors have meant over the years when they have told ICANN to specify the purpose of WHOIS? How would you assess the purpose of collecting, processing, maintaining and providing access to gTLD registration data? For example, can you help us understand what a purpose applies to when it comes to registration data or directory services? Where will purpose be applied (and not be applied) in registration data and directory services policies? What criteria should be used to determine legitimate purpose(s)? What is the difference between “primary” and “secondary” purposes and how does that affect all of the above?

2. Article 6(1)(b) Directive provides that personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (Article 7). Processing of personal data is allowed to a limited number of legitimate grounds, specified in Article 7 Directive. Under what circumstances might the publication of registration data elements that are personal data be allowable?

Questions for Data Commissioners – Registration Data

Registration Data Elements

3. Considering that gTLD registration data elements may refer to mere technical information, information that may relate to legal persons and information that may directly relate to an identified or identifiable natural person, only the last one of which has consequences from a data protection perspective, how do you think consistent policies for a Registration Directory Service could best be developed?

For example, it is our understanding that “personal data” under the EU Data Protection Directive and the General Data Protection Regulation is specified if data relates to an identified or identifiable natural person. Currently, Registrars and Registries display the following info through a public directory service called WHOIS without any access restrictions: the domain name registrant’s full name, street address, zip code, country code, telephone number and email address. Is this “personal data” as specified by the Directive and the General Data Protection Regulation, regardless of whether the registrant is a legal person or a natural person?

4. Article 5 of the EU commerce directive requires service providers to disclose their contact information. Does this directive apply to domain name registrants? Does that mean that registrants that are service providers in the EU could be required to have their contact data displayed in a registration directory service?

Questions for Data Commissioners – Registration Data

Registration Data Elements

5. Below is an example of “thin data” elements made publicly accessible in today’s WHOIS system for every registered gTLD domain name. Do you believe that any of the following data elements are considered personal information under the General Data Protection Directive, and why?

Domain Name: CNN.COM

Registrar: CSC CORPORATE DOMAINS, INC.

Sponsoring Registrar IANA ID: 299

Whois Server: whois.corporatedomains.com

Referral URL: <http://www.cscglobal.com/global/web/csc/digital-brand-services.html>

Name Server: NS-1086.AWSDNS-07.ORG

Name Server: NS-1630.AWSDNS-11.CO.UK

Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>

Status: serverDeleteProhibited <https://icann.org/epp#serverDeleteProhibited>

Status: serverTransferProhibited <https://icann.org/epp#serverTransferProhibited>

Status: serverUpdateProhibited <https://icann.org/epp#serverUpdateProhibited>

Updated Date: 15-feb-2017

Creation Date: 22-sep-1993

Expiration Date: 21-sep-2018

Questions for Data Commissioners – Access

Access to Registration Data for Criminal and Abuse Investigations

6. It is our understanding that the suppression of criminal offences is an exemption to the application of the General Data Protection Regulation. If or when could this exemption apply to private cybersecurity firms investigating crime, civil offenses, or abuses in general by using data obtained through a registration data directory service?

7. If the application of General Data Protection Regulation provisions led to a completely private domain name registration database, where the vast majority of registrants refused to give access to their data, should the economic repercussions of closing the database be taken into account, to evaluate whether or not to apply the General Data Protection Regulation? For example, would economic repercussions be seen as threatening the 'monetary interests of the State' or the economic rights of private cybersecurity firms and the IP industry?

Questions for Data Commissioners – Personal Privacy/HR

Personal Privacy/Human Rights

8. Today, a public access WHOIS directory service enables anyone who may be the victim of defamation, threats, harassment, etc., to look up the name of a domain name registrant (which may or may not correspond to the owner of a website hosted at that domain name), as a deterrent to such attacks. Do you believe this deterrent effect can constitute a public service, instead of protecting the privacy rights of the perpetrators? This effectively contributes to the fight against online violence against women, who are often the victims in such cases.

9. Under the General Data Protection Regulation, is consumer protection an objective pursued by the State which would fall into the category of protecting the rights and freedoms of others? If yes, do you consider anonymous public access to registration data an additional protection given to consumers, to help them avoid scams?

10. With regards to General Data Protection Regulation compliance by entities within the EU, would it be enough legally if ICANN consensus policies define a new Registration Directory Service which allows for controlled access to registration data, without requesting the data subject's formal consent for each use, especially uses that do not benefit him/her, but are lawful (for example, the suppression of criminal offenses)?

11. Numerous stakeholders at ICANN have suggested that asking end users or beneficial registrants to consent to further uses of their registration data would solve the debate over the privacy of registration data made accessible through WHOIS. What are your views on the use of consent in this context?

Questions for Data Commissioners – Jurisdiction

Jurisdiction

12. Can you explain to us how the data commissioners factor in the European Charter of Rights (or, for that matter, local or supra-national fundamental rights instruments in the case of countries outside Europe) in the assessment of data protection issues? Is this matter within their jurisdiction?

13. In view of the borderless nature of the internet and the fact that European Union citizens may freely acquire domain names from registries and registrars in third countries, how could potential conflicts of law based on the current and future European Union data protection framework best be avoided?

14. Can the EU enforce provisions of the General Data Protection Regulation on ICANN itself, or just the EU Registrars and EU Registries? Will there be such enforcement?

Questions for Data Commissioners – Applicable Law

Compliance with Applicable Laws

15. Article 6 of the General Data Protection Regulation provides that processing is lawful if, among other things, the processing is “necessary to protect the vital interests of . . . another natural person or for the legitimate interests pursued by . . . a third party.” Under these principles, and given the longstanding and historical use of registration data made available through WHOIS as a de-facto public resource, do you agree this information should continue to be made readily available to those who investigate fraud, consumer deception, intellectual property violations, or other violations of law?

16. Our working group deals with policies pertaining to generic top-level domains (gTLDs). However, each country establishes its own policies pertaining to country-code top-level domains (ccTLDs). Currently, all EU states have ccTLD registries which provide publicly available registration data through WHOIS, both for private individuals and commercial entities. Can you explain how these ccTLD registry policies are able to comply with EU data protection laws?

17. The gTLD ecosystem includes the Generic Names Supporting Organization which recommends policy, ICANN which implements that policy, registries which administer the domain name space under a given gTLD, and registrars which register domain names for use by registrants. Within this ecosystem, who do you see as the data controller, in terms of the EU definitions of data controller and data processors?

Questions for Data Commissioners – Consumer Protection

Consumer Protection

18. Can you comment on your understanding of the need for owners of trademarks/brands and IP to avoid and combat infringement, and this need's connection to consumer protection, in the context of the EU ePrivacy Directive and the General Data Protection Regulation?

19. Today, intellectual property and trademark rights holders depend on registration data obtained through the WHOIS directory service to police the misuse of their intellectual property on commercial websites, track down purveyors of counterfeit goods, and prevent fraudulent websites from engaging in illegal activity on the Internet. Is creating a repository of information for contactability to facilitate reaching those business registrants a valid purpose for this directory service and, if not, why not?

Questions for Data Commissioners – Additional

Proposed addition by Alex Deacon (15 March)

20. WHOIS is a key tool to enhance transparency and accountability in the online environment (under the condition of course that they are accurate).

- a. How can we ensure that tools such as WHOIS are given real/true meaning to help defend fundamental rights/the rule of law in general?
- b. How can we best reconcile the different fundamental rights in this context - fundamental rights such as authors' rights, the right to privacy, the right to property and other legitimate/internationally recognized fundamental rights?
- c. How do we ensure the required balance between the different fundamental rights as stipulated, for example, in the Court of Justice of the European Union in its Promusicae decision?

Online Workshop of possible interest to RDS PDP WG

PrivacyCheq GDPR Compliance Webinar Series :

Operationalizing Legitimate Interests as a basis for lawful processing under GDPR

Thursday, March 16th at 2:30 PM GMT and 1:00 PM EST (free, registration required)

<http://us14.campaign-archive2.com/?u=f7f06f709dff69f947397b77b&id=d418d6b2cf>

As part of our technical compliance education series, PrivacyCheq is pleased to offer this **free 30 minute webinar** which will explore the complexities of technical compliance with the European Union's General Data Protection Regulation.

Under GDPR, data controllers must choose one of six bases for legally processing a data subject's personal data. Recent proposals from the UK ICO have spotlighted one of these, "Legitimate Interests". Many digital marketers have believed that gathering informed affirmative consent from data subjects would adversely affect their business and are considering the Legitimate Interests basis as a [less disruptive option for their industry](#).

This webinar will provide deep insight into the actual **real world implementation of Legitimate Interests** as a basis for processing. It is intended **for DPOs, legal professionals and consulting firms** that will be responsible for delivering compliant user experiences by May 2018.