RDS PDP Phase 1: Key Concepts Deliberation – Working Draft Excerpt:
List of Initial Rough Consensus Agreements To-Date

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

1. The WG should continue deliberation on the purpose(s) of the "Minimum Public Data Set."

2. Every data element in the "Minimum Public Data Set" should have at least one legitimate purpose.

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

45. *There must be at least one purpose for collecting each data element in the MPDS, and that purpose must be sufficient for making that data element public.*

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

4. EWG-identified purposes apply to at least one data element in the "Minimum Public Data Set."

5. Domain name control is a legitimate purpose for "Minimum Public Data Set" collection.

6. Technical Issue Resolution is a legitimate purpose for "Minimum Public Data Set" collection.

7. Domain Name Certification is a legitimate purpose for "Minimum Public Data Set" collection.

8. Business Domain Name Purchase or Sale is a legitimate purpose for "Minimum Public Data Set" collection.

9. Academic / Public Interest DNS Research is a legitimate purpose for "Minimum Public Data Set" collection.

10. Regulatory and Contractual Enforcement is a legitimate purpose for "Minimum Public Data Set" collection.

11. Criminal Investigation & DNS Abuse Mitigation is a legitimate purpose for "Minimum Public Data Set" collection.

12. Legal Actions is a legitimate purpose for "Minimum Public Data Set" collection.

13. Individual Internet Use is a legitimate purpose for "Minimum Public Data Set" collection.

46. Technical Issue Resolution for issues associated with Domain Name Resolution is a legitimate purpose, based on the following definition: Information collected to enable contact of the relevant contacts to facilitate tracing, identification and resolution of incidents related to issues associated with domain name resolution by persons who are affected by such issues, or persons tasked (directly or indirectly) with the resolution of such issues on their behalf.

47. The following information is to be collected for the purpose of Technical Issue Resolution associated with Domain Name Resolution:

- *Technical Contact(s) or (if no Technical Contact is provided) Registrant Contact(s),*
- *Nameservers,*
- *Domain Status,*
- *Expiry Date and Time,*
- *Sponsoring Registrar.*

48. Domain Name Management is a legitimate purpose for collecting some registration data, based on the definition: Information collected to create a domain name registration, enabling management of the domain name registration, and ensuring that the domain registration records are under the control of the authorized party and that no unauthorized changes or transfers are made in the record.

49. The following registration data is needed for the purpose of Domain Name Management:

- *Domain Name*
- *Registrant Name*
- *Registrant Organization*
- *Registrant Email*
- *Registrar Name*
- *Creation Date*
- *Updated Date*
- *Expiration Date*
- *Nameservers*
- *Domain Status*
- *Administrative Contact*

Table: Summary of Data Required and Collected for each Legitimate Purpose

Data Required/Collected	For the following Legitimate Purposes
Nameservers	Technical Issue Resolution, Domain Name Management
Domain Status	Technical Issue Resolution, Domain Name Management
Expiry Date and Time	Technical Issue Resolution, Domain Name Management
Creation Date	Domain Name Management
Updated Date	Domain Name Management
Sponsoring Registrar	Technical Issue Resolution, Domain Name Management
Registrant Contact(s)	Technical Issue Resolution (if no Tech Contact is provided)
Registrant Name	Domain Name Management
Registrant Organization	Domain Name Management
Registrant Email	Domain Name Management
Technical Contact(s)	Technical Issue Resolution
Administrative Contact	Domain Name Management

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

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

15. As a WG, we need to agree upon a purpose statement for the RDS. (refer to WG Agreements #16 – 19 in the Statement of Purpose)

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

16. A purpose of gTLD registration data is to provide info about the lifecycle of a domain name and its resolution on the Internet.

17. A purpose of RDS is to facilitate dissemination of gTLD registration data of record[2], such as domain names and their domain contacts[3] and name servers, in accordance with applicable policy.[4]

18. A purpose of RDS is to identify domain contacts and facilitate communication with domain contacts associated with generic top-level domain names, [based on approved policy].

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

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

The following draft criteria for determining whether purposes are legitimate for processing registration data were deliberated upon without reaching rough consensus:

- *Draft Criterion #1: Any purpose for processing registration data must be [consistent with / not inconsistent] with ICANN's mission.*
- *Draft Criterion #2: If applicable data protection laws require a [legal /lawful] basis for processing, then any purpose must satisfy at least one such basis for processing.*
- *Draft Criterion #3: One criterion the WG will consider when determining whether a purpose for processing is legitimate is whether the purpose is inherent to the functionality of the DNS. This will not be the only criterion considered and is not a requirement that all purposes must satisfy*.

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

20. gTLD registration data in the "Minimum Public Data Set" must be accessible without requestor identification, authentication, or stated purpose.

21. There must be no RDS policies that prevent RDS operators from applying operational controls such as rate limiting and CAPTCHA, provided that they do not unreasonably restrict legitimate access.
[Rough consensus in 2 May poll, but pending action item]

Question: What guiding principles should be applied to "Minimum Public Data Set" access?

22. At least a defined set of data elements must be accessible by unauthenticated RDS users.

23. RDS policy must state purpose(s) for public access to the "Minimum Public Data Set."

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

25. "Minimum Public Data Set" to be used as a replacement term (within WG Agreements to date) for what had previously been referred to as "thin data."

26. The DNSSEC data element should be added to the "Minimum Public Data Set."

27. Today's gTLD WHOIS registration data elements classified as "thin" are sufficient at this time, to be referred to within WG Agreements hereafter as the "Minimum Public Data Set."

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

28. Registrant Country must be included in RDS data elements; it must be mandatory to collect for every domain name registration.

29. RDS policy must include a definition for every gTLD registration data element including both a semantic definition and (by reference to appropriate standards) a syntax definition.

30. At least one element identifying the domain name registrant (i.e., registered name holder) must be collected and included in the RDS.

31. Data enabling at least one way to contact the registrant must be collected and included in the RDS.

32. At a minimum, one or more e-mail addresses must be collected for every domain name included in the RDS, for contact roles that require an e-mail address for contactability.

33. For resiliency, data enabling alternative or preferred method(s) of contact should be included in the RDS; further deliberation to determine whether such data element(s) should be optional or mandatory to collect.

34. At least one element enabling contact must be based on an open standard and not a proprietary communication method.

35. To improve contactability with the domain name registrant (or authorized agent of the registrant), the RDS must be capable of supporting at least one alternative contact method as an optional field.

36. Purpose-based contact (PBC) types identified (Admin, Legal, Technical, Abuse, Proxy/Privacy, Business) must be supported by the RDS but optional for registrants to provide.

37. The URL of the Internic Complaint Site must be supported for inclusion in the RDS.

38. The Registrar Abuse Contact Email Address must be supported for inclusion in the RDS, and must be provided by Registrars.

39. Reseller Name MUST be supported by the RDS. Note: There may be a chain or Resellers identified by Reseller Name.

40. Per recently-approved consensus policy on consistent labeling and display, BOTH the Registrar Abuse Contact Email and Registrar Abuse Contact Phone must be supported for inclusion in the RDS, and MUST be provided by Registrars.

41. In the interest of maximizing contactability, additional contact methods MUST be supported by the RDS as an open-ended list and be optional for Registrants to provide. This does not preclude agreements on requirements to include other contact methods.

42. The RDS must support Registrant Postal Address data elements: Registrant Street Address, City, State/Province, and Postal Code.

43. The RDS must support Registrant Phone + Registrant Phone Ext (extension) data elements.

44. There is no requirement for the Original Registration Date as proposed by the EWG Final Report.