|  |  |
| --- | --- |
| [UP-D01-R01] | “In support of ICANN’s mission to coordinate the global Internet’s system of unique identifiers, and to ensure the stable and secure operation of the Internet’s unique identifier system, information about gTLD domain names is necessary to promote trust and confidence in the Internet for all stakeholders.” (p. 16, Section IIb, Purpose) |
|  | Similar to:  Draft Statement of Purpose  Goals for each RDS Purpose include “Consistency with ICANN’s mission”  Specific Purposes include “A purpose of RDS is to provide information about domain contacts, domain names and name servers for gTLDs, [based on approved policy].” |
|  | **Poll Questions to be posed to WG to inform further deliberation:**  Choose one of the following resolutions:   * Delete as possible requirement and treat as input to the Statement of Purpose * Retain to help shape specific policy requirements pertaining to information about gTLD domain names * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   Indicate level of support[[1]](#footnote-1) for each of the following draft recommendations, derived from initial deliberation at ICANN57:   1. Information about gTLD domain names is necessary to: promote trust and confidence in the Internet. 2. Information about gTLD domain names is necessary to: support ICANN’s mission to coordinate the global Internet’s system of unique identifiers. 3. Information about gTLD domain names is necessary to: ensure the stable and secure operation of the Internet’s unique identifier system. 4. Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [UP-D01-R02] | “gTLD registration data [must be] collected, validated and disclosed for permissible purposes only.” (p. 21, p. 31 Principle 6) |
|  | Similar to:  [UP-D01-R03]  gTLD registration directory services must “accommodate in some manner all identified permissible purposes”, including the following users and permissible purposes. (pp. 21-25, 27-29) – see [UP-D01-R04 to R14]  [UP-D19-R01]  Based on the ICANN Governmental Advisory Committee (GAC) proposed principles and recommendations related to gTLD WHOIS services on the basis of general public policy issues, gTLD WHOIS [that is, registration directory] services should reflect and respect the following functions: detailed in [UP-D19-R02 to R09]  See also [DE-D01-R01]  The [gTLD registration directory service] must accommodate purpose-driven disclosure of data elements. |
|  | **Poll Questions to be posed to WG to inform further deliberation:**  Choose one of the following resolutions:   * Delete as possible requirement * Retain to help shape specific policy requirements pertaining to gTLD registration data * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   Indicate level of support1 for each of the following draft recommendations, derived from initial deliberation at ICANN57:   1. RDS policies may require collection of gTLD registration data *for specific permissible purposes only*; RDS policies must not require collection for other purposes. 2. RDS policies may require gTLD registration data to be validated to the level of accuracy needed by *any specific permissible purpose*; RDS policies must not require validation beyond that level. 3. RDS policies may require gTLD registration data be disclosed *for specific permissible purposes only*; RDS policies must not require disclosure for other purposes. 4. RDS policies must not prevent contracted parties from collecting data for other purposes; such data (if any) is beyond the scope of RDS policies. 5. RDS policies must present the purpose(s) for collection of gTLD registration data to the registrant and gain permission prior to collection. 6. Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [UP-D01-R04] | \* 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.” |
|  | Similar to: None |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R05] | \* 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.” |
|  | Similar to: None |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R06] | \* 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.” |
|  | Similar to:  [UP-D19-R03]  \* [Must reflect] "Providing contact points for network operators and administrators, including ISPs, and certified computer incident response teams" "to support the security and stability of the internet" (para 3.1 and para 2.1.1)  [UP-D21-R06]  “Article 29 WP acknowledges the legitimacy of the purpose of the making available of some personal data through the WHOIS services ...[t]his publicity is necessary in order to put the person running a Website in a position to face the legal and technical responsibilities which are inherent to the running of such a site.” |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R07] | \* 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.” |
|  | Similar to: None |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R08] | \* 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.” |
|  | Similar to:  [UP-D19-R08] \* [Must reflect] "Helping users to identify persons or entities responsible for content or services online" in contribution to user confidence in the Internet (para 3.1 and para 2.1.6)  [UP-D62-R03] When I buy something on the web, I would like to be able to access the registration data for the web page I am using to know it is the real company |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R09] | \* Business Domain Name Purchase or Sale – “Making purchase queries about a DN, acquiring a DN from another Registrant, and enabling due diligence research.” |
|  | Similar to:  [UP-D19-R04] \* [Must reflect] "Allowing users to determine the availability of domain names" (para 3.1 and para 2.1.2 |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R10] | \* Academic/Public-Interest DNS Research – “Academic public-interest research studies about domain names published in [gTLD registration directory services], including public information about the Registrant and designated contacts, the domain name’s history and status, and DNs registered by a given Registrant.” |
|  | Similar to: None |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R11] | \* 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. ” |
|  | Similar to:  [UP-D08-R01] gTLD directory services must support] Legal Actions --- investigating possible legal claims arising from use  of a domain name, including contacting registrant or its legal representative.  [UP-D19-R07] \* [Must reflect] "Facilitating clearance of trademarks and countering intellectual property infringements in accordance with applicable national laws and international treaties" (para 3.1 and para 2.1.5)  [UP-D62-R04] There are a lot of third parties (not just LEAs) who have legitimate reasons for access to avoid their rights being infringed upon  [DE-D32-R01]  The specifications below are recommended requirements for dispute resolution and other procedures related to trademarks. These include: [DE-D32-R02 to R04] |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R12] | \* Regulatory and Contractual Enforcement – “Tax authority investigation of businesses with online presence, UDRP investigation, contractual compliance investigation, and registration data escrow audits.” |
|  | Similar to:  [UP-D19-R09]  \* [Must reflect] "Assisting businesses, other organizations and users in combating fraud and general compliance with relevant laws" (para 3.1 and para 2.1.7) |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R13] | \* 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.” |
|  | Similar to:  [UP-D02-R02] "Law enforcement has a legitimate need to access the real identity of the responsible party(ies) for a domain name."  [UP-D02-R03] "Security practitioners have a legitimate need to access the real identity of those responsible for a domain name."  [UP-D19-R03] \* [Must reflect] "Providing contact points for network operators and administrators, including ISPs, and certified computer incident response teams" "to support the security and stability of the internet" (para 3.1 and para 2.1.1)  [UP-D19-R05] \* [Must reflect] "Assisting law enforcement authorities (which may include non-governmental entities) in investigations, in enforcing national and international law" (para 3.1 and para 2.1.3) |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R14] | \* DNS Transparency – “Querying the registration data made public by Registrants to satisfy a wide variety of needs to inform the general public.” |
|  | Similar to:  [UP-D08-R02]  [gTLD directory services must support] Providing a public record of domain name ownership, accessible by the public for any lawful use.  [UP-D19-R08]  \* [Must reflect] "Helping users to identify persons or entities responsible for content or services online" in contribution to user confidence in the Internet (para 3.1 and para 2.1.6) |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R15] | \* gTLD registration directory services must support active deterrence of known malicious activities to the extent other requirements are satisfied. (See paragraph c on page 25.) |
|  | Similar to: None |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D01-R17] | Since it is likely that further [permissible purposes] will be identified over time, any [gTLD registration directory service] must be designed with extensibility in mind. |
|  | Similar to:  [UP-D01-R27] gTLD registration directory services must be designed with the ability to accommodate new users and permissible purposes that are likely to emerge over time |
|  | **Pending initial deliberation on additional guiding principles** |
| [UP-D01-R27] | gTLD registration directory services must be designed with the ability to accommodate new users and permissible purposes that are likely to emerge over time. |
|  | **Pending initial deliberation on [UP-D01-R17]** |
| [UP-D02-R02] | "Law enforcement has a legitimate need to access the real identity of the responsible party(ies) for a domain name." |
|  | **Pending initial deliberation on [UP-D01-R13]** |
| [UP-D02-R03] | "Security practitioners have a legitimate need to access the real identity of those responsible for a domain name." |
|  | **Pending initial deliberation on** **[UP-D01-R13]** |
| [UP-D08-R01] | [gTLD directory services must support] Legal Actions --- investigating possible legal claims arising from use  of a domain name, including contacting registrant or its legal representative. |
|  | **Pending initial deliberation on** **[UP-D01-R11]** |
| [UP-D08-R02] | [gTLD directory services must support] Providing a public record of domain name ownership, accessible by the public for any lawful use. |
|  | **Pending initial deliberation on UP-D01-R14]** |
| [UP-D14-R03] | According to the 2013 RAA Data Retention Waiver and Discussion Document, registrars should have access to and be able to collect records of communications with the registrant regarding the registration (log files including communication sources, IP, ISP, behaviour on the website, method of transmission, source IP address, HTTP header, email, Skype handle associated with communication) in order to mitigate fraud prevention, for billing disputes, for commercial purposes. |
|  | Similar to: None |
|  | **Pending initial deliberation on specific permissible purposes** |
| [UP-D21-R06] | “Article 29 WP acknowledges the legitimacy of the purpose of the making available of some personal data through the WHOIS services ...[t]his publicity is necessary in order to put the person running a Website in a position to face the legal and technical responsibilities which are inherent to the running of such a site.” |
|  | **Pending initial deliberation on** **[UP-D01-R06]** |
| [UP-D26-R17] | As used in the Directive, [data] 'recipient' means a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients; |
|  | Similar to: None |
|  | **Pending initial deliberation on additional guiding principles** |
| [UP-D30-R02] | The requirement for a third country to ensure an adequate level of data protection was further defined by the CJEU in Schrems…It also indicated that the wording ‘adequate level of protection’ must be understood as “requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the Directive read in the light of the Charter” pg.10 |
|  | Similar to:  [GA-D30-R01] (duplicate) [PR-D30-R05] (duplicate) |
|  | **To be addressed through further deliberation on [PR-D30-R05] (duplicate)** |
| [UP-D62-R03] | When I buy something on the web, I would like to be able to access the registration data for the web page I am using to know it is the real company |
|  | **Pending initial deliberation on** **[UP-D01-R08]** |
| [UP-D62-R04] | There are a lot of third parties (not just LEAs) who have legitimate reasons for access to avoid their rights being infringed upon |
|  | **Pending initial deliberation on** **[UP-D01-R11]** |
| [UP-D62-R05] | Related to TM Clearinghouse notices, when notices are received, analysis that is performed includes going to see who is the registrant - this often eliminates the need for further action (~60-70%) |
|  | Similar to: None |
|  | **Pending initial deliberation on specific permissible purposes** |

|  |  |
| --- | --- |
| [DE-D01-R01] | The [gTLD registration directory service] must accommodate purpose-driven disclosure of data elements. |
|  | Similar to:  [UP-D01-R35]  \* Purpose-based contact data must be provided for every registered domain name which makes public the union of data elements that are mandatory. [See DE possible requirements.]  [DE-D01-R07]  Each [gTLD registration] data element must be associated with a set of permissible purposes.  See also [UP-D01-R02] “gTLD registration data [must be] collected, validated and disclosed for permissible purposes only.” (p. 21, p. 31 Principle 6) |
|  | **Poll Questions to be posed to WG to inform further deliberation:**  Choose one of the following resolutions:   * Delete as possible requirement * Retain to help shape specific policy requirements pertaining to *disclosure* of gTLD registration data elements * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   Indicate level of support1 for each of the following draft recommendations, derived from initial deliberation at ICANN57:   1. RDS policies may require that disclosure of gTLD registration data elements be controlled and based upon the user’s declared specific purpose. 2. RDS policies must be precise about which (if any) gTLD registration data elements are public (that is, disclosed to all users, for all permissible purposes). 3. RDS policies must be precise about which (if any) gTLD registration data elements are not public (that is, disclosed only to some users and/or for some permissible purposes). 4. RDS policies must be precise about the set of permissible purposes associated with each gTLD registration data element. 5. Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [DE-D01-R22] | Validators, Registries and Registrars may collect, store, or disclose additional data elements for internal use that is never shared with the [gTLD registration directory service]. |
|  | Similar to:  [DE-D01-R19]  To avoid collecting more data than necessary, all other Registrant-supplied data not enumerated above and used for at least one permissible purpose must be optionally collected at the Registrant’s discretion. Validators, Registries and Registrars must allow for this data to be collected and stored if the Registrant so chooses. |
|  | **Poll Questions to be posed to WG to inform further deliberation:**  Choose one of the following resolutions:   * Delete as possible requirement * Retain to help shape specific policy requirements pertaining to *collection* of gTLD registration data elements * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   Indicate level of support1 for each of the following draft recommendations, derived from initial deliberation at ICANN57:   1. RDS policies may require specific mandatory data elements to be collected from Registrants and shared with the RDS. 2. RDS policies may allow specific optional data elements to be collected from Registrants and shared with the RDS, at the Registrant’s discretion. 3. RDS policies must not require all data elements shared with the RDS to be disclosed. [Note: Refer to DE-D01-R01 for recommendations about disclosure.] 4. RDS policies must allow gTLD-specific data elements to be collected from Registrants, as defined by the Registry’s policies for that gTLD. 5. RDS policies must not prevent contracted parties from collecting, storing, or disclosing data elements that are never shared with the RDS and thus out of scope. 6. Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [DE-D12-R02] | The [gTLD registration directory service] should collect and display uniform sets of data regardless of the registry involved. (sec. 5.2) |
|  | Similar to:  [DE-D12-R01] Registration information from all registries should follow consistent rules for labeling and display, as per the model outlined in specification 3 of the 2013 RAA. (Rec. #1) |
|  | **Poll Questions to be posed to WG to inform further deliberation:**  Choose one of the following resolutions:   * Delete as possible requirement * Retain to help shape specific policy requirements pertaining to *consistent labeling and display* of gTLD registration data elements * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   Indicate level of support1 for each of the following draft recommendations, derived from initial deliberation at ICANN57:   1. RDS policies must require *uniform* labeling and display of *common* gTLD registration   data, regardless of the registry involved.   1. RDS policies must require *consistent* labeling and display of *common* gTLD registration data, regardless of the registry involved. 2. RDS policies must allow for labeling and display of *gTLD-specific* registration data as defined by the Registry's policies for that gTLD. 3. RDS policies for consistent labeling and display of gTLD registration data should not constrain policies for data collection and disclosure. 4. Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [DE-D19-R01] | Based on the ICANN Governmental Advisory Committee (GAC) proposed principles, gTLD [registration directory] services "should provide sufficient and accurate data about domain name registrations and registrants (…)" (para 3.3) |
|  | Similar to:  [DA-D19-R01] (duplicate) |
|  | **Poll Questions to be posed to WG to inform further deliberation:**  Choose one of the following resolutions:   * Delete as possible requirement * Retain to help shape specific policy requirements pertaining to gTLD registration data elements * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   Indicate level of support1 for each of the following draft recommendations, derived from initial deliberation at ICANN57:   1. RDS policies must include a definition of "sufficient" registration data about domain names and Registrants 2. RDS policies must include a definition of "accurate" registration data about domain names and Registrants 3. RDS policies must require *sufficient* registration data about domain names and Registrants 4. RDS policies must require *accurate* registration data about domain names and Registrants 5. Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [DE-D01-R02] | Not all [gTLD registration] data collected is to be public; disclosure must depend upon Requestor and Purpose. |
|  | Similar to:  [DE-D01-R04] 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, and Auditing/Compliance to ensure that gated access is not abused.  [DE-D01-R05]  Only the data elements permissible for the declared purpose must be disclosed (i.e., returned in responses or searched by Reverse and WhoWas queries). |
|  | **Pending initial deliberation – added for Week 2** |
| [DE-D01-R03] | Public access to an identified minimum data set must be made available [by the gTLD registration directory service], including contact data published expressly to facilitate communication for this purpose. |
|  | Similar to:  [DE-D01-R24] 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.  [DE-D01-R20]  To maximize Internet stability, the following mandatory data elements must be provided by Registries and Registrars:  a. Registration Status  b. Client Status (Set by Registrar)  c. Server Status (Set by Registry)  d. Registrar  e. Registrar Jurisdiction  f. Registry Jurisdiction  g. Registration Agreement Language  h. Creation Date  i. Registrar Expiration Date  j. Updated Date  k. Registrar URL  l. Registrar IANA Number  m. Registrar  [DE-D01-R26]  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:  a. Domain Name  b. DNS Servers  c. Registrant Type  d. Registrant Contact ID  e. Registrant Email Address  f. Tech Contact ID  g. Admin Contact ID  h. Legal Contact ID  i. Abuse Contact ID  j. Privacy/Proxy Provider Contact ID (mandatory only if Registrant Type = Privacy/Proxy Provider)  k. Business Contact ID (mandatory only if Registrant Type = Legal Person) |
|  | **Pending initial deliberation – added for Week 2** |
| [PR-D30-R05] | The requirement for a third country to ensure an adequate level of data protection was further defined by the CJEU in Schrems…It also indicated that the wording ‘adequate level of protection’ must be understood as “requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of the Directive read in the light of the Charter” pg.10 |
|  | See [UP-D30-R02] (duplicate) |
|  | **Poll Questions to be posed to WG to inform further deliberation:**  Choose one of the following resolutions:   * Delete as possible requirement * Retain as possible guiding principle(s) to help shape specific policy requirements  pertaining to gTLD registration data privacy * Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   Indicate level of support1 for each of the following draft recommendations, derived from initial deliberation at ICANN57:   1. RDS policies must include a definition of "adequate level of protection" for gTLD registration data 2. RDS policies must include a definition of "third country" as it pertains to gTLD registration data 3. When gTLD registration data is transferred across national borders, RDS policies must require the third country to ensure an adequate level of protection for that data 4. RDS policies must allow contracted parties to comply with applicable law 5. RDS polices must provide an adequate level of protection for gTLD registration data 6. Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [PR-D25-R03] | Council of Europe's Treaty 108 on Data Protections, Article 5, Quality of data, restricts the collection of data under its privacy laws to only that data that is: a. obtained and processed fairly and lawfully; b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c. adequate, relevant and not excessive in relation to the purposes for which they are stored; d. accurate and, where necessary, kept up to date; e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.” |
|  | Same as [UP-D25-R03] (duplicate) |
|  | **Pending initial deliberation – added for Week 2** |
| [PR-D26-R04] | According to the Directive (26), whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible; |
|  | Same as [UP-D26-R03] (duplicate) |
|  | **Pending initial deliberation – added for Week 2** |
| [PR-D26-R05] | According to the Directive (30), whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons; |
|  | Same as [UP-D26-R06] |
|  | **Pending initial deliberation – added for Week 2** |

**All Possible Requirements copied in their entirety verbatim from:**[RDS PDP Initial List of Possible Requirements Draft #5 – as of 28 October 2016](https://community.icann.org/download/attachments/41890478/RDS%20PDP%20List%20of%20Possible%20Requirements%20D5%20-%20TriageInProgress%20-%2028%20October.pdf)

**Source Documents for Possible Requirements referenced in this Initial Deliberation List  
From RDS PDP Initial List of Possible Requirements Draft #5, Annex A. Key Input Documents**

**[01]** [EWG Final Report](https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf)

**[02]** [SAC061, SSAC Comment on ICANN’s Initial Report from the Expert Working Group](https://www.icann.org/en/system/files/files/sac-061-en.pdf) (2013)

**[08]** [Steve Metalitz: Additional Possible Requirements](http://mm.icann.org/pipermail/gnso-rds-pdp-wg/2016-May/000719.html)

**[12]** [GNSO PDP on Thick WHOIS Final Report](http://gnso.icann.org/en/issues/whois/thick-final-21oct13-en.pdf) (2013)

**[14]** 2013 RAA's [Data Retention Specification Waiver](https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#data-retention) and [Discussion Document](https://www.icann.org/en/system/files/files/draft-data-retention-spec-elements-21mar14-en.pdf) (2014)

**[19]** [GAC Principles regarding gTLD WHOIS Services](http://whois.icann.org/en/link/gac-principles-regarding-gtld-whois-services) (28 March 2007)

**[21]** [Article 29 WP on ICANN Procedure for Handling WHOIS Conflicts with Privacy Law](https://www.icann.org/en/correspondence/schaar-to-cerf-12mar07.pdf) (2007)

**[25]** [Council of Europe's Treaty 108 on Data Protection](http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108) (1985)

**[26]** [European Data Protection Directive (1995](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al14012))

**[30]** [Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision of the Article 29 WP 238](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf)

**[32]** [Green Paper: Improvement of Technical Management of Internet Names and Addresses (1998)](https://www.ntia.doc.gov/legacy/ntiahome/domainname/022098fedreg.htm)

**[62]** [Possible Requirements identified during the ICANN56 Cross-Community Session on RDS](http://mm.icann.org/pipermail/gnso-rds-pdp-wg/2016-June/000933.html)

**As deliberations proceed, we will be tracking the status of each PR discussed, for example**

* I – Initial deliberation underway for this possible requirement and similar possible requirements
* P – Polling on draft recommendation(s) derived from initial deliberation at ICANN57
* F – Further WG deliberation underway, informed by poll results
* R – Deliberation completed with rough consensus in support of draft recommendation(s)
* X – Deliberation completed with rough consensus to delete PR

1. “Level of support” choices: Could support as-is, Might support with refinement, Could not support in any form, No opinion [↑](#footnote-ref-1)