[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]."
[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.
[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
[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
[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.”
[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

[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
[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
[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

[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]
[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)

[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)
[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)

[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
[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
[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.
	See [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."
	See [UP-D01-R13]
[UP-D02-R03]	"Security practitioners have a legitimate need to access the real identity of those responsible for a domain name."

	See [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.
	See [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.
	See 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
[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."

	See [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
[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)
[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
	See [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
	See [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
[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)
[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.
[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)
[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] (duplicated)
[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)

Sources - From Annex A. Key Input Documents

[01] EWG Final Report

[02] SAC061, SSAC Comment on ICANN's Initial Report from the Expert Working Group (2013)

[08] Steve Metalitz: Additional Possible Requirements

[12] GNSO PDP on Thick WHOIS Final Report (2013)

[14] 2013 RAA's Data Retention Specification Waiver and Discussion Document (2014)

[19] GAC Principles regarding gTLD WHOIS Services (28 March 2007)

[21] Article 29 WP on ICANN Procedure for Handling WHOIS Conflicts with Privacy Law (2007)

[26] European Data Protection Directive (1995)

[30] Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision of the Article 29 WP 238

[32] Green Paper: Improvement of Technical Management of Internet Names and Addresses (1998)

[62] Possible Requirements identified during the ICANN56 Cross-Community Session on RDS

We will be tracking the status of each PR discussed, for example

- D – Discussed in one WG meeting
- I – Initial WG support with no strong opposition
- E – Ready to edit
- R - Rough consensus in support of PR
- X – Rough consensus to delete PR