RDS PDP Initial List of *Possible* Requirements Draft #3 – Triage In Progress as of 21 June 2016

The purpose of this document is to carry out Task 8 of the RDS PDP WG Phase 1 work plan. As noted in that plan, the bulk of the WG's work will involve recommending requirements for registration directory services.

Recognizing that the Board recommended that the EWG Final Report should be the starting point for this PDP and that EWG efforts, although not policy development, were very comprehensive with extensive and thorough consideration of public input, this document identifies *possible* requirements for registration data and directory services from the EWG Final Report along with *possible* requirements obtained from additional Key Inputs such as the sources identified by input-gathering sub-teams on Data, Purpose and Privacy and in the PDP Issue Report, and *possible* requirements suggested by SG/C/SO/AC Inputs and WG Members.

After *possible* requirements are gathered into a comprehensive and inclusive list, which is compiled without debate on the merits of each of the *possible* requirements, the WG will design a very systematic approach to maximize efficiency in discussing and attempting to reach consensus on recommended requirements for registration directory services. These requirements will help the WG reach an informed decision about if and why a next-generation system is needed to replace today's WHOIS system.

Organization

The *possible* requirements listed in this document are organized as follows:

1. *Possible* Requirements that map to one or more of the eleven (11) questions in the charter. Note that the same requirement may address multiple questions.
2. *Possible* Requirements that may not map to any question identified in the charter.
3. *Possible* Foundational Questions that must be answered based on all other requirements.

As stated above, all of the *possible* requirements in this document are derived from cited Key Input documents (listed in Annex A), supplemented by any additional *possible* requirements suggested by WG members or SGs, Cs, SOs and ACs during outreach.

After the WG confirms that this list of *possible* requirements is sufficiently complete to serve as the foundation for WG deliberation, the WG should continue through its work plan until reaching Task 12 where it will systematically consider each *possible* requirement individually with the goal of trying to reach as strong a consensus as possible as to whether the WG supports the *possible requirement*, including how it is worded.

The grouping of the requirements into the 11 charter questions should not be seen as fixed. The WG should feel free to move *possible* requirements under different questions and even to include a given requirement under more than one question if that seems useful, as long as the duplication is noted.

RDS PDP Initial List of *Possible* Requirements Draft #3 – Triage In Progress as of 21 June 2016

The order of the *possible* requirements within the various sections in this document is primarily based on the order in which the 11 questions are posed in the WG's charter. The WG may decide to change the order to provide a more useful presentation but this should be done with full consideration of the reasons why the order was established in the framework. Due to interdependencies, WG deliberation will likely be iterative, especially on fundamental questions pertaining to purpose, data, and privacy.

Notation

Possible requirements are numbered using the notation [QQ-D#-R#] for ease of use and scalability as this list evolves. Specifically, "QQ" identifies the associated question as follows:

- **FQ** Foundational Questions: Questions to be answered based on all other requirements
- **OQ** Other Questions: Questions that may not fit within the 11 charter questions
- **UP** Users/Purposes: Who should have access to gTLD registration data and why?
- **GA** Gated Access: What steps should be taken to control data access for each user/purpose?
- **DA** Data Accuracy: What steps should be taken to improve data accuracy?
- **DE** Data Elements: What data should be collected, stored, and disclosed?
- **PR** Privacy: What steps are needed to protect data and privacy?
- **CX** Coexistence: What steps should be taken to enable coexistence?
- **CM** Compliance: What steps are needed to enforce these policies?
- **SM** System Model: What system requirements must be satisfied by any implementation?
- **CS** Cost: What costs will be incurred and how must they be covered?
- **BE** Benefits: What benefits will be achieved and how will they be measured?
- **RI** Risks: What risks do stakeholders face and how will they be reconciled?

This "QQ" will be followed by "D##" which identifies by number a key input document from Annex A.

Finally, "R##" sequentially numbers within each document all *possible* requirements. For example, **[UP-D01-R03]** is the third *possible* user/purpose requirement extracted from the EWG Final Report **[01]**, while **[DE-D01-R04]** is the fourth *possible* data element requirement taken from that same document.

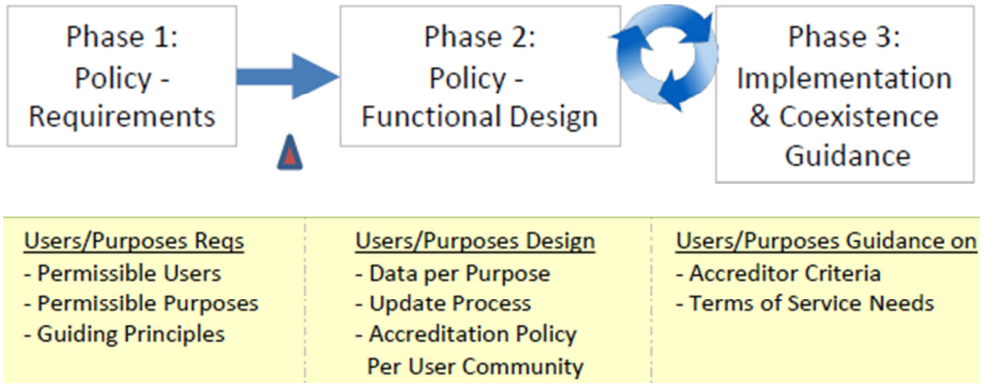
Possible requirements are not necessarily quoted verbatim from key input documents, but rather phrased as needed to describe a *possible* requirement for gTLD registration directory services or registration data. In particular, *possible* fundamental requirements should not be specific to today's WHOIS system or a next-generation replacement, since the goal is to enable WG deliberation and consensus as the basis for answering foundational questions posed by the WG charter.

RDS PDP Initial List of *Possible* Requirements Draft #3 – Triage In Progress as of 21 June 2016

Users/Purposes (UP)

The following *possible* requirements address the charter question on Users and Purposes (UP):
Who should have access to gTLD registration data & why?

The process framework for this question (below) can be applied to categorize ***possible requirements*** into three phases:



In the grid below, we identify the ***possible requirement*** for WG deliberation, any **pre-requisites or dependencies** contained in that ***possible requirement***, and whether the ***possible requirement*** therefore falls into Phase 1, 2, or 3. Policies designed to meet **Phase 1** policy requirements should be considered in **Phase 2**, while implementation or coexistence guidance for Phase 2 policies should be considered in **Phase 3**. In addition, an initial attempt has been made to **group similar requirements**, allowing the table to be easily re-sorted by Group. These initial groups are defined below the grid and may be revamped by the WG during deliberation.

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
[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)	None	1	A
[UP-D01-R02]	"gTLD registration data [must be] collected, validated and disclosed for permissible purposes only." (p. 21, p. 31 Principle 6)	None	1	A
[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)	Permissible purposes Permissible Users	1	A

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
		Precedes [UP-D01-R04 to R14]		
[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."	Supports [UP-D01-R03]	1	E
[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."	Supports [UP-D01-R03]	1	G
[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."	Supports [UP-D01-R03]	1	B
[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."	Supports [UP-D01-R03]	1	AC
[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."	Supports [UP-D01-R03]	1	E F
[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."	Supports [UP-D01-R03]	1	J
[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."	Supports [UP-D01-R03]	1	I
[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. "	Supports [UP-D01-R03]	1	J
[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."	Supports [UP-D01-R03]	1	I
[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."	Supports [UP-D01-R03]	1	B Q

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
[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."	Supports [UP-D01-R03]	1	C
[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.)	None	1	B
[UP-D01-R16]	"All purposes/contacts must be codified by policymakers through a defined process for adding, changing, or deleting purposes." (p.37)	None	1	D H
[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.	None	1	A H
[UP-D01-R18]	gTLD registration directory services must provide the "ability to determine all domains registered by a given entity (commonly referred to as Reverse WHOIS)." (p. 26)	Permissible purposes that require this functionality	2	C E
[UP-D01-R19]	gTLD registration directory services must provide the "The ability to determine historical domain name registration information (commonly referred to as WhoWas)."	Permissible purposes that require this functionality	2	C I
[UP-D01-R20]	ICANN must publish, in one place, a user-friendly policy describing the purpose and permissible uses of registration data, to clearly inform Registrants why this data is being collected and how it will be handled and used.	Permissible purposes Why data is collected How data will be handled/ used Policies to be defined in P2	3	A D
[UP-D01-R21]	There must be clearly defined permissible/impermissible uses of gTLD registration data and directory services.	None	1	D
[UP-D01-R22]	gTLD registration directory services must support defined permissible purposes, including uses that involve [UP-D01-R23 to R26]	Permissible purposes Precedes [UP-D01-R23 to R26]	2	
[UP-D01-R23]	* [Must support] Identifying the Registrant and contacts designated for a given purpose;	Permissible purposes that require this functionality Supports [UP-D01-R22]	2	E
[UP-D01-R24]	* [Must support] Communicating with contacts designated for a given purpose;	Permissible purposes that require this functionality Supports [UP-D01-R22]	2	F
[UP-D01-R25]	* [Must support] Using data published by Registries about Domain Names; and	Permissible purposes that require this functionality Supports [UP-D01-R22]	2	C
[UP-D01-R26]	* [Must support] Searching portions of registration data required for a given purpose.	Permissible purposes that require this functionality Supports [UP-D01-R22]	2	C
[UP-D01-R27]	gTLD registration directory services must be designed with the ability to accommodate new users	Precedes [UP-D01-R26 to R31]	1	H

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	and permissible purposes that are likely to emerge over time.			
[UP-D01-R28]	* An application process must be defined.	Supports [UP-D01-R27]	2	H
[UP-D01-R29]	* Applications must be reviewed against defined criteria.	Supports [UP-D01-R27]	2	H
[UP-D01-R30]	* Applications that pass review must be evaluated and approved by a multistakeholder review board as determined by a policy development process.	Supports [UP-D01-R27]	3	H
[UP-D01-R31]	* Approved applications must be added to the gTLD registration directory services privacy policy and scheduled for implementation periodically (e.g., quarterly, annually) as defined by policy.	Supports [UP-D01-R27] Policies to be defined in P2	3	H
[UP-D01-R33]	All permissible purposes must be mapped to specific contact data needed for that specific purpose. (p.36)	Permissible purposes Data Element PR(s) for Contacts	2	A
[UP-D01-R34]	gTLD registration directory services must meet contact data requirements associated with permissible purposes through the following principles 8-14 on pp. 35-36.	Permissible purposes Precedes [UP-D01-R35 to R41]	1	A
[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.]	Data Element PR(s) for Contacts Supports [UP-D01-R34]	1	A
[UP-D01-R36]	* All mandatory purpose-based contact data must be syntactically accurate and operationally reachable to meet the needs of every codified permissible purpose.	Data Accuracy PR(s) for Contacts Supports [UP-D01-R34]	1	F
[UP-D01-R37]	* During domain name registration, the Registrant must be informed of all permissible purposes and given an opportunity to publish contact data for each purpose, including replacing the Registrant's contact data for any or all purposes.	Data Element PR(s) for Contacts Supports [UP-D01-R34]	1	E
[UP-D01-R38]	* A domain name must not be activated (put into the global DNS) until valid contact data is provided for every applicable purpose.	Data Accuracy PR(s) for Contacts Supports [UP-D01-R34]	1	F
[UP-D01-R39]	* If contact data becomes invalid for its designated purpose, a process that provides the Registrant with the ability to specify a new valid contact must ensue, allowing reasonable notification and time for update to occur. [See DA possible requirements].	Data Element PR(s) for Contacts Supports [UP-D01-R34]	1	F
[UP-D01-R40]	* A process and policies must be developed enabling Registrant-designated contacts to opt-in/opt-out of having their data published as contacts for domain names, to support the rights of persons and entities to accept or reject responsibility for serving in specific roles for particular domain registrations.	Data Element PR(s) for Contacts Supports [UP-D01-R34]	2	A D
[UP-D01-R41]	* Any system for providing purpose-based contact data must be flexible and allow for new purposes and contact types to be created and published.	Data Element PR(s) for Contacts Supports [UP-D01-R34]	1	A H
[UP-D01-R42]	gTLD registration directory services must allow registrants to optionally supply "designated administrative, technical, accredited Privacy/Proxy Provider, and business contacts" to be made accessible when appropriate for those specific purposes.	Permissible purposes Privacy PR(s) for P/P Providers	2	G
[UP-D01-R43]	". . . the [gTLD registration directory service] portal [must] make the definitions for every	Permissible purposes	2/3	A

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	purpose-based contact type readily accessible to users (for example, using hover-over pop-up definitions) to clearly indicate that contacts are published to handle inquiries for permissible purposes, and that a point of contact must be designated to cover those purposes." (p.57)			
[UP-D02-R01]	"There is a critical need for a policy asserting the purpose of collecting and maintaining registration data. This policy should address the operational concerns of the parties who collect, maintain or use this data as it relates to ICANN's remit."	None	1	D
[UP-D02-R02]	"Law enforcement has a legitimate need to access the real identity of the responsible party(ies) for a domain name."	None	1	B
[UP-D02-R03]	"Security practitioners have a legitimate need to access the real identity of those responsible for a domain name."	None	1	B
[UP-D05-R01]	"The WHOIS protocol has no provisions for strong security. WHOIS lacks mechanisms for access control, integrity, and confidentiality. Accordingly, WHOIS-based services should only be used for information which is non-sensitive and intended to be accessible to everyone." (From Section 5: Security Considerations) This text implies that there should be a requirement to provide services for access control, integrity, and confidentiality. It also suggests that [gTLD registration directory services] should not be used to access sensitive information.	Access PR(s) requiring Public Access	1	U L D
[UP-D06-R01]	In providing query-based public access to registration data as required by [RAA] Subsections 3.3.1 and 3.3.4, Registrar shall not impose terms and conditions on use of the data provided, except as permitted by any Specification or Policy established by ICANN. Unless and until ICANN establishes a different Consensus Policy, Registrar shall permit use of data it provides in response to queries for any lawful purposes except to: (a) allow, enable, or otherwise support the transmission by e-mail, telephone, postal mail, facsimile or other means of mass unsolicited, commercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations.	Lawful Permissible Purposes	1	D
[UP-D06-R02]	In the event that ICANN determines, following analysis of economic data by an economist(s) retained by ICANN (which data has been made available to Registrar), that an individual or entity is able to exercise market power with respect to registrations or with respect to registration data used for development of value-added products and services by third parties, Registrar shall provide third-party bulk access to the data subject to public access under [RAA] Subsection 3.3.1 under the following terms and conditions: [detailed in [UP-D06-R03 to R07]	Access PR(s) requiring Bulk Access Precedes [UP-D06-R03 to R07]	1	I C
[UP-D06-R03]	* Registrar shall make a complete electronic copy of the data available at least one (1) time per	Access PR(s) requiring	2/3	I

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	week for download by third parties who have entered into a bulk access agreement with Registrar.	Bulk Access Supports [UP-D06-R02]		C
[UP-D06-R04]	* Registrar may charge an annual fee, not to exceed US$10,000, for such bulk access to the data.	Access PR(s) requiring Bulk Access Supports [UP-D06-R02]	2/3	I C
[UP-D06-R05]	* Registrar's access agreement shall require the third party to agree not to use the data to allow, enable, or otherwise support any marketing activities, regardless of the medium used. Such media include but are not limited to e-mail, telephone, facsimile, postal mail, SMS, and wireless alerts	Access PR(s) requiring Bulk Access Supports [UP-D06-R02]	2	I C
[UP-D06-R06]	* Registrar's access agreement shall require the third party to agree not to use the data to enable high-volume, automated, electronic processes that send queries or data to the systems of any Registry Operator or ICANN-Accredited registrar, except as reasonably necessary to register domain names or modify existing registrations.	Access PR(s) requiring Bulk Access Supports [UP-D06-R02]	2	I C
[UP-D06-R07]	* Registrar's access agreement must require the third party to agree not to sell or redistribute the data except insofar as it has been incorporated by the third party into a value-added product or service that does not permit the extraction of a substantial portion of the bulk data from the value-added product or service for use by other parties.	Access PR(s) requiring Bulk Access Supports [UP-D06-R02]	2	I C
[UP-D06-R08]	From 3.3.7: To comply with applicable statutes and regulations and for other reasons, ICANN may adopt a Consensus Policy establishing limits (a) on the Personal Data concerning Registered Names that Registrar may make available to the public through a public-access service described in [RAA] Subsection 3.3 and (b) on the manner in which Registrar may make such data available. Registrar shall comply with any such Consensus Policy.	Access PR(s) requiring Public Access	2	D
[UP-D06-R09]	Rights in Data. Registrar disclaims all rights to exclusive ownership or use of the data elements listed in [RAA] Subsections 3.2.1.1 through 3.2.1.3 for all Registered Names submitted by Registrar to the Registry Database for, or sponsored by Registrar in, each gTLD for which it is Accredited. Registrar does not disclaim rights in the data elements listed in [RAA] Subsections 3.2.1.4 through 3.2.1.6 and Subsections 3.3.1.3 through 3.3.1.8 concerning active Registered Names sponsored by it in each gTLD for which it is Accredited, and agrees to grant non-exclusive, irrevocable, royalty-free licenses to make use of and disclose the data elements listed in [RAA] Subsections 3.2.1.4 through 3.2.1.6 and 3.3.1.3 through 3.3.1.8 for the purpose of providing a service or services (such as a Whois service under Subsection 3.3.4) providing interactive, query-based public access. Upon a change in sponsorship from Registrar of any Registered Name in each gTLD for which it is Accredited, Registrar acknowledges that the registrar gaining sponsorship shall have the rights of an owner to the data elements listed in [RAA] Subsections 3.2.1.4 through 3.2.1.6 and 3.3.1.3	Access PR(s) requiring Public Access Data Element PR(s) requiring collection of listed elements	2	M

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	through 3.3.1.8 concerning that Registered Name, with Registrar also retaining the rights of an owner in that data. Nothing in this Subsection prohibits Registrar from (1) restricting bulk public access to data elements in a manner consistent with this Agreement and any Specifications or Policies or (2) transferring rights it claims in data elements subject to the provisions of this Subsection 3.5.			
[UP-D06-R10]	From 3.7.7.7: Registrar shall agree that it will not process the Personal Data collected from the Registered Name Holder in a way incompatible with the purposes and other limitations about which it has provided notice to the Registered Name Holder in accordance with [RAA] Subsection 3.7.7.4.	Permissible purposes Data Element PR(s) requiring collection of Personal Data Privacy PR(s) stating limitations	1	A
[UP-D06-R11]	Handling by ICANN of Registrar-Supplied Data. Before receiving any Personal Data from Registrar, ICANN shall specify to Registrar in writing the purposes for and conditions under which ICANN intends to use the Personal Data. ICANN may from time to time provide Registrar with a revised specification of such purposes and conditions, which specification shall become effective no fewer than thirty (30) days after it is provided to Registrar. ICANN shall not use Personal Data provided by Registrar for a purpose or under conditions inconsistent with the specification in effect when the Personal Data was provided. ICANN shall take reasonable steps to avoid uses of the Personal Data by third parties inconsistent with the specification.	Permissible purposes Data Element PR(s) requiring collection of Personal Data Privacy PR(s) stating conditions	2/3	A
[UP-D07-R01]	From Specification 4, Section 1.10: "Offering searchability capabilities on the Directory Services is optional but if offered by the Registry Operator it shall comply with the specification described in this [New gTLD Registry Agreement] section [as detailed in [UP-D07-R02 to R07]	Precedes [UP-D07-R02 to R07] Permissible purposes requiring this functionality	2	I
[UP-D07-R02]	* From Section 1.10.1: Registry Operator will offer searchability on the web-based Directory Service.	Supports [UP-D07-R01] Permissible purposes requiring this functionality	2	I
[UP-D07-R03]	* From Section 1.10.2: Registry Operator will offer partial match capabilities, at least, on the following fields: domain name, contacts and registrant's name, and contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state or province, etc.).	Supports [UP-D07-R01] Permissible purposes requiring this functionality	2	I
[UP-D07-R04]	* From Section 1.10.3: Registry Operator will offer exact-match capabilities, at least, on the following fields: registrar id, name server name, and name server's IP address (only applies to IP addresses stored by the registry, i.e., glue records).	Supports [UP-D07-R01] Permissible purposes requiring this functionality	2	I
[UP-D07-R05]	* From Section 1.10.4: Registry Operator will offer Boolean search capabilities supporting, at least, the following logical operators to join a set of search criteria: AND, OR, NOT.	Supports [UP-D07-R01] Permissible purposes requiring this functionality	2	I

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
[UP-D07-R06]	* From Section 1.10.5: Search results will include domain names matching the search criteria.	Supports [UP-D07-R01] Permissible purposes requiring this functionality	2	I
[UP-D07-R07]	* From Section 1.10.6: Registry Operator will: 1) implement appropriate measures to avoid abuse of this feature (e.g., permitting access only to legitimate authorized users); and 2) ensure the feature is in compliance with any applicable privacy laws or policies.	Supports [UP-D07-R01] Permissible purposes requiring this functionality	2	J
[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.	Variant of [UP-D01-R11]	1	A D
[UP-D08-R02]	[gTLD directory services must support] Providing a public record of domain name ownership, accessible by the public for any lawful use.	Variant of [UP-D01-R14]	1	A
[UP-D09-R01]	In Recommendations 2 -4, the WHOIS Policy Review Team (WHOIS RT) recommends that the ICANN Board oversee the creation of a single [gTLD registration data] policy document, and reference it in subsequent versions of agreements with Contracted Parties. In doing so, ICANN should clearly document the current [and recommended next-generation?] gTLD WHOIS policy as set out in the gTLD Registry and Registrar contracts and GNSO Consensus Policies and Procedure.	Policies to be defined in P2	3	A
[UP-D13-R01]	Based on the review of ICANN's procedure for handling WHOIS conflicts with privacy law, the following User/Purpose-related requirements from past accreditation agreements are unchanged: Registrars must notify registrants of: 1) the purposes for the collection of any personal data, and 2) the intended recipients of the data.	Permissible purposes Permissible users Data Element PR(s)	1	B
[UP-D14-R01]	The 2013 RAA Data Retention Waiver and Discussion Document lists and describes all data elements that can be collected by the registrars in accordance with the 2013 RAA and it provides reasons / legitimate purposes for that collection and retention. The following possible User/Purpose requirement stems from this document: Registrars should have access to standard data elements (see [DE-D14-R01]) for billing and billing disputes.	[DE-D14-R01]	1	A
[UP-D14-R02]	According to the 2013 RAA Data Retention Waiver and Discussion Document, the public community should have access to WHOIS Information (described in the WHOIS Specification) in order to mitigate abuse, address hijacking, theft and slamming.	None	1	J
[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.	None	1	M A

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
[UP-D16-R01]	Under the current ICANN UDRP and URS policies for new gTLDs, contact data published in WHOIS is required to identify registrants for legal purposes. The UDRP and URS policies rely on contact data that is published publicly in [gTLD registration directory services], where potential complainants can see it, and so UDRP and URS dispute resolution service providers can use the data to administrate required communications.	Access PR(s) requiring Public Access Data Element PR(s) for Contacts	1	K
[UP-D18-R01]	Based on the WHOIS Inter-Registrar Transfer Policy, Section I.A.4.5: "For purposes of facilitating transfer requests, Registrars should provide and maintain a unique and private email address for use only by other Registrars and the Registry: • 4.5.1 This email address is for issue related to transfer requests and the procedures set forth in this policy only. • 4.5.2 The email address should be managed to ensure messages are received by someone who can respond to the transfer issue. • 4.5.3 Messages received at such email address must be responded to within a commercial reasonable timeframe not to exceed seven (7) calendar days."	Data Element PR(s)	2	K
[UP-D18-R02]	Based on the WHOIS Inter-Registrar Transfer Policy, Section I.A.4.6: • 4.6.1 "Registrars will establish a Transfer Emergency Action Contact ("TEAC") for urgent communications relating to transfers. The goal of the TEAC is to quickly establish a real-time conversation between registrars (in a language that both parties can understand) in an emergency. Further actions can then be taken towards a resolution, including initiating existing (or future) transfer dispute or undo processes." • 4.6.2 "Communications to TEACs will be reserved for use by ICANN-Accredited Registrars, gTLD Registry Operators and ICANN Staff. The TEAC point of contact may be designated as a telephone number or some other real-time communication channel and will be recorded in, and protected by, the ICANN RADAR system. Communications to a TEAC must be initiated in a timely manner, within a reasonable period of time following the alleged unauthorized loss of a domain."	Data Element PR(s)	2	K
[UP-D18-R03]	Based on the WHOIS Inter-Registrar Transfer Policy, Section I.A.5.5 to I.A.5.6: • 5.5 "Registrar-generated "AuthInfo" codes must be unique on a per-domain basis." • 5.6 "The "AuthInfo" codes must be used solely to identify a Registered Name Holder, whereas the FOAs still need to be used for authorization or confirmation of a transfer request, as described in Section 2 and Section 4 of [the Inter-Registrar Transfer] policy."	Data Element PR(s)	2	K
[UP-D18-R04]	Based on the WHOIS Inter-Registrar Transfer Policy, Section I.B.1.1: "In general, registrants must be permitted to update their registration/WHOIS data and transfer their registration rights to	Data Element PR(s) Data Accuracy PR(s)?	1	K

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	other registrants freely."			
[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]	Precedes [UP-D19-R02 to R09]	1	C?
[UP-D19-R02]	* [Must reflect] Providing "a lookup service to internet users" (para 3.1 and para 2.1)	Supports [UP-D19-R01] Permissible purposes that require this functionality	1	F
[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)	Supports [UP-D19-R01] Permissible purposes that require this functionality Data Element PR(s) for Contact	1	B
[UP-D19-R04]	* [Must reflect] "Allowing users to determine the availability of domain names" (para 3.1 and para 2.1.2)	Supports [UP-D19-R01] Permissible purposes that require this functionality Data Element PR(s) for Ops	1	C
[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)	Supports [UP-D19-R01] Permissible purposes that require this functionality	1	J
[UP-D19-R06]	* [Must reflect] "Assisting in combating against abusive use of ICTs, such as illegal and other acts motivated by racisms (…) including child pornography (…)" (para 3.1 and para 2.1.4)	Supports [UP-D19-R01] Permissible purposes that require this functionality	1	J
[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)	Supports [UP-D19-R01] Permissible purposes that require this functionality	1	J
[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)	Supports [UP-D19-R01] Permissible purposes that require this functionality Data Element PR(s) for RegID	1	C B
[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)	Supports [UP-D19-R01] Permissible purposes that require this functionality Data Accuracy PR(s) antifraud	1	J

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
[UP-D21-R01]	In sum, from the Article 29 WP's comments on ICANN's procedures for handling WHOIS conflicts with privacy law (and related correspondence), we could draw out the following possible Purpose requirements: [detailed in [UP-D21-R02 to R04]	Precedes [UP-D21-R02 to R04]	1	A
[UP-D21-R02]	* Need a well-defined purpose for processing/use of data;	Supports [UP-D21-R01] Privacy PR(s) for processing/use	1	A J
[UP-D21-R03]	* Domain name Point of Contact needs to be in a position to face the legal and technical responsibilities of domain operation; and	Supports [UP-D21-R01] Data Element PR(s) for contact	1	C B
[UP-D21-R04]	* Bulk access to WHOIS data for direct marketing should be limited.	Supports [UP-D21-R01] Access PR(s) requiring Bulk Access	1	I J
[UP-D21-R05]	According to Article 29 WP's comments on ICANN's procedures for handling WHOIS conflicts with privacy law (and related correspondence), "Purpose definition is a central element in determining whether a specific processing or use of personal data is in accordance with EU data protection legislation."	Privacy PR(s) for Personal Data Protection, Jurisdiction	1	A
[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."	None	1	B E
[UP-D22-R01]	In sum, from the Article 29 WP's Opinion 2/2003, we could draw out the following possible Purpose requirements: [detailed in [UP-D22-R02 to R05]	Precedes [UP-D22-R02 to R05]	1	A
[UP-D22-R02]	* Need a well-defined purpose;	Supports [UP-D22-R01] Privacy PR(s) for Processing/Use	1	A J
[UP-D22-R03]	* Data collected should be relevant (and not excessive) for defined purpose;	Supports [UP-D22-R01] Data Element PR(s)	1	A
[UP-D22-R04]	* Bulk access to WHOIS data for direct marketing should be limited;	Supports [UP-D22-R01] Access PR(s) requiring Bulk Access	1	I J
[UP-D22-R05]	* Data subjects should be provided with unambiguous and informed consent.	Supports [UP-D22-R01] Privacy PR(s) for Consent	1	L
[UP-D22-R06]	According to the Article 29 WP's Opinion 2/2003, "From the data protection viewpoint it is essential to determine in very clear terms what is the purpose of the WHOIS and which purpose(s) can be considered as legitimate and compatible to the original purpose."	Original Purpose	1	A
[UP-D22-R07]	In the Article 29 WP's Opinion 2/2003, the WP states "its support for ... limitation of bulk access	Access PR(s) requiring	1	I

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	for direct marketing issues."	Bulk Access		
[UP-D23-R01]	"Specification of purpose is an essential first step in applying data protection laws and designing data protection safeguards for any processing operation. Indeed, specification of the purpose is a pre-requisite for applying other data quality requirements, including the adequacy, relevance, proportionality and accuracy of the data collected and the requirements regarding the period of data retention. The principle of purpose limitation is designed to establish the boundaries within which personal data collected for a given purpose may be processed and may be put to further use. The principle has two components: the data controller must only collect data for specified, explicit and legitimate purposes, and once data are collected, they must not be further processed in a way incompatible with those purposes." p.4	Permissible purposes Data Accuracy PR(s) Data Element PR(s)	1	A
[UP-D23-R02]	"When we share personal data with others, we usually have an expectation about the purposes for which the data will be used. There is a value in honouring these expectations and preserving trust and legal certainty, which is why purpose limitation is such an important safeguard, a cornerstone of data protection. Indeed, the principle of purpose limitation inhibits 'mission creep', which could otherwise give rise to the usage of the available personal data beyond the purposes for which they were initially collected." p.4	Permissible purposes Privacy PR(s) on personal data	1	A
[UP-D23-R03]	"On the other hand, data that have already been gathered may also be genuinely useful for other purposes, not initially specified. Therefore, there is also a value in allowing, within carefully balanced limits, some degree of additional use. The prohibition of 'incompatibility' in Article 6(1)(b) does not altogether rule out new, different uses of the data – provided that this takes place within the parameters of compatibility." p.4	Permissible purposes Privacy PR(s) on personal data	1	A
[UP-D23-R04]	"The principle of purpose limitation - which includes the notion of compatible use - requires that in each situation where further use is considered, a distinction be made between additional uses that are 'compatible', and other uses, which should remain 'incompatible'. The principle of purpose limitation is designed to offer a balanced approach: an approach that aims to reconcile the need for predictability and legal certainty regarding the purposes of the processing on one hand, and the pragmatic need for some flexibility on the other." p.5	Permissible purposes Privacy PR(s) on personal data	1	A
[UP-D23-R05]	Council of Europe "CoE Resolution (73) 22 requires the information to be 'appropriate and relevant with regard to the purpose for which it has been stored' and - in the absence of 'appropriate authorisation' - prohibits its use 'for purposes other than those for which it has been stored' as well as its 'communication to third parties'." p.8.	Permissible purposes Access PR(s) for authorization Privacy PR(s) on personal data	1	A
[UP-D23-R06]	"When applying data protection law, it must first be ensured that the purpose is specific, explicit and legitimate. This is a prerequisite for other data quality requirements, including adequacy,	Permissible purposes Data Accuracy PR(s)	1	A

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	relevance and proportionality (Article 6(1)(c)), accuracy and completeness (Article 6(1)(d)) and requirements regarding the duration of retention (Article 6(1)(e)).” p. 12	authorization Privacy PR(s) on personal data		
[UP-D23-R07]	“In cases where different purposes exist from the beginning and different kinds of data are collected and processed simultaneously for these different purposes, the data quality requirements must be complied with separately for each purpose.” p. 12	Permissible purposes Data Accuracy PR(s) Data Element PR(s)	1	A
[UP-D23-R08]	“If personal data are further processed for a different purpose: the new purposes must be specified (Article 6(1)(b)), and it must be ensured that all data quality requirements (Articles 6(1)(a) to (e)) are also satisfied for the new purposes.” p. 12 [detailed in [UP-D23-R09 to R10]	Precedes [UP-D23-R09 to R10] Permissible purposes Data Accuracy PR(s)	1	H
[UP-D23-R09]	* “First building block: purpose specification. Collection for 'specified, explicit and legitimate' purpose”	Supports [UP-D23-R08] Permissible purposes	1	A
[UP-D23-R10]	* “Second building block: compatible use. Article 6(1)(b) of the Directive also introduces the notions of 'further processing' and 'incompatible' use, and requires that further processing must not be incompatible with the purposes for which personal data were collected.” In particular, Article 6(1)(b) requires that personal data should not be 'further processed in a way incompatible' with those purposes and recital 28 states that the 'purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified'.” p.12	Supports [UP-D23-R08] Permissible purposes Privacy PR(s) on personal data	1	H
[UP-D23-R11]	“Transparency: There is a strong connection between transparency and purpose specification. When the specified purpose is visible and shared with stakeholders such as data protection authorities and data subjects, safeguards can be fully effective. Transparency ensures predictability and enables user control.” p. 13	Permissible purposes Privacy PR(s)	1	AD
[UP-D23-R12]	“Predictability: If a purpose is sufficiently specific and clear, individuals will know what to expect: the way data are processed will be predictable. This brings legal certainty to the data subjects, and also to those processing personal data on behalf of the data controller. Predictability is also relevant when assessing the compatibility of further processing activities. In general, further processing cannot be considered predictable if it is not sufficiently related to the original purpose and does not meet the reasonable expectations of the data subjects at the time of collection, based on the context of the collection.” p. 13	Permissible purposes Privacy PR(s)	1	A D
[UP-D23-R13]	“User control: User control is only possible when the purpose of data processing is sufficiently clear and predictable. If data subjects fully understand the purposes of the processing, they can exercise their rights in the most effective way. For instance, they can object to the processing or request the correction or deletion of their data.” p. 14	Permissible purposes Privacy PR(s)	1	A E
[UP-D23-R14]	“Personal data must be collected for explicit purposes. The purposes of collection must not only be specified in the minds of the persons responsible for data collection. They must also be made	Permissible purposes Data Element PR(s) on Collection	1	A D

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	explicit. In other words, they must be clearly revealed, explained or expressed in some intelligible form. It follows from the previous analysis that this should happen no later than the time when the collection of personal data occurs." p.17	Privacy PR(s) on personal data		
[UP-D23-R15]	"Purpose limitation [in the EU Data Protection Directive] protects data subjects by setting limits on how data controllers are able to use their data while also offering some degree of flexibility for data controllers." Executive Summary, p. 3	Permissible purposes Privacy PR(s) for Processing/Use	1	D
[UP-D23-R16]	"Processing of personal data in a way incompatible with the purposes specified at collection is against the law and therefore prohibited. The data controller cannot legitimise incompatible processing by simply relying on a new legal ground in Article 7. The purpose limitation principle can only be restricted subject to the conditions set forth in Article 13 of the Directive."	Permissible purposes Privacy PR(s) for Processing/Use	1	A
[UP-D25-R01]	Council of Europe's Treaty 108 on Data Protections – Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (signed by 48 countries in Western and Eastern Europe and around the world) [could possibly confer requirements on a gTLD directory service]	Same as [PR-D25-R01]		D
[UP-D25-R02]	Council of Europe's Treaty 108 on Data Protections outlaws the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. (Note: this protects an array of groups and organizations with missions, mandates and projects around race, politics, heath, religion, sexual orientation, prison support and rehabilitation, etc.)	Privacy PR(s)	1	D
[UP-D25-R03]	Council of Europe's Treaty 108 on Data Protections specifies in Article 5, Quality of data that personal data undergoing automatic processing shall be: 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 [PR-D25-R03] Permissible purposes Data Accuracy PR(s) Privacy PR(s) for personal data	1	A M
[UP-D26-R01]	According to the European Data Protection Directive (1995), whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals; p.2	Privacy PR(s) for personal data	1	D
[UP-D26-R02]	According to the Directive (20), whereas the fact that the processing of data is carried out by a	To be continued		D

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;			
[UP-D26-R03]	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;			A D
[UP-D26-R04]	According to the Directive (28), whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;			A D
[UP-D26-R05]	According to the Directive (29), whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;			A D
[UP-D26-R06]	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….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;			A D
[UP-D26-R07]	According to the Directive (31), whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data			AB D

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	subject's life;			
[UP-D26-R08]	According to the Directive (33), whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;			D
[UP-D26-R09]	According to the Directive (39), whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;			C
[UP-D26-R10]	According to the Directive (41), whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;			E
[UP-D26-R11]	According to the Directive (50), whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;			C
[UP-D26-R12]	According to the Directive (51), whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;			L
[UP-D26-R13]	According to the Directive (56), whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of			M

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;			
[UP-D26-R14]	As used in the Directive, [data] 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;			M
[UP-D26-R15]	As used in the Directive, [data] 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;			M
[UP-D26-R16]	As used in the Directive, 'third party' means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;			M
[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;			C
[UP-D26-R18]	As used in the Directive, 'the data subject's consent' means any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.			L
[UP-D26-R19]	According to the Directive, Member States shall provide that personal data must be [handled as detailed in [UP-D26-R20 to R24]	Precedes [UP-D26-R20 to R24]		
[UP-D26-R20]	* [personal data must be] processed fairly and lawfully;	Supports [UP-D26-R19]		D
[UP-D26-R21]	* [personal data must be] collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;	Supports [UP-D26-R19]		A
[UP-D26-R22]	* [personal data must be] adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;	Supports [UP-D26-R19]		R
[UP-D26-R23]	* [personal data must be] accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;	Supports [UP-D26-R19]		N
[UP-D26-R24]	* [personal data must be] kept in a form which permits identification of data subjects for no	Supports [UP-D26-R19]		D

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.			M
[UP-D26-R25]	According to the Directive Article 7, Member States shall provide that personal data may be processed only if: [conditions detailed in [UP-D26-R26 to R31]	Precedes [UP-D26-R26 to R31]		M
[UP-D26-R26]	* [personal data may be processed only if] the data subject has unambiguously given his consent	Supports [UP-D26-R25]		L
[UP-D26-R27]	* [personal data may be processed only if] processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	Supports [UP-D26-R25]		L
[UP-D26-R28]	* [personal data may be processed only if] processing is necessary for compliance with a legal obligation to which the controller is subject	Supports [UP-D26-R25]		J
[UP-D26-R29]	* [personal data may be processed only if] processing is necessary in order to protect the vital interests of the data subject	Supports [UP-D26-R25]		B
[UP-D26-R30]	* [personal data may be processed only if] processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed	Supports [UP-D26-R25]		B
[UP-D26-R31]	* [personal data may be processed only if] processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under [the Directive] Article 1 (1).	Supports [UP-D26-R25]		M D
[UP-D26-R32]	According to the Directive, Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. [This requirement] shall not apply where:] (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or (b) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or (c) the processing relates to data which are manifestly made public by the data subject or is			AD ?

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	necessary for the establishment, exercise or defence of legal claims.			
[UP-D26-R33]	According to the Directive, processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.			A D
[UP-D26-R34]	According to the Directive, where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing; (c) any further information such as • the categories of data concerned, • the recipients or categories of recipients, • the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject. [The above requirement] shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.	Same as [GA-D26-R07]		M
[UP-D26-R35]	According to the Directive Article 25, Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.			M
[UP-D27-R01]	According to the European Data Protection Supervisor, Registrar Accreditation Agreement (RAA) gTLD registration data element specifications "should only require collection of personal data, which is genuinely necessary for the performance of the contract between the Registrar and the Registrant (e.g. billing) or for other compatible purposes such as fighting fraud related to domain			A D

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	name registration."			
[UP-D27-R02]	According to the European Data Protection Supervisor, personal data should only be collected to perform the contract between Registrar and Registrant, and that it should be retained no longer than is necessary for these purposes. "This data should be retained for no longer than is necessary for these purposes. It would not be acceptable for the data to be retained for longer periods or for other, incompatible purposes, such as law enforcement purposes or to enforce copyright."			O
[UP-D28-R01]	"The people or bodies that collect and manage personal data are called "data controllers". They must respect EU law when handling the data entrusted to them." (Note: they manage the data for the purpose for which it was collected.)			M
[UP-D28-R02]	"The privacy rights of individuals supplying their personal data must be respected by anyone collecting and processing that data. The Data Protection Directive lays down a series of rights and duties in relation to personal data when it is collected and processed."			A D
[UP-D28-R03]	The EU Privacy Directive "refers to the persons or entities which collect and process personal data as 'data controllers'. For instance, a medical practitioner is usually the controller of his patients' data; a company is the controller of data on its clients and employees; a sports club is controller of its members' data and a library of its borrowers' data." [gTLD registration directory services? must] ensure that Uses/Purposes are consistent with those allowed by law and the purpose for which the data was collected.			M
[UP-D28-R04]	"Data controllers determine 'the purposes and the means of the processing of personal data'. This applies to both public and private sectors."			M
[UP-D28-R05]	"Data controllers must respect the privacy and data protection rights of those whose personal data is entrusted to them. They must: collect and process personal data only when this is legally permitted; respect certain obligations regarding the processing of personal data; respond to complaints regarding breaches of data protection rules; collaborate with national data protection supervisory authorities.	Same as [PR-D28-R04]		M
[UP-D30-R01]	The WP29 recalls its long-standing position that massive and indiscriminate surveillance of individuals can never be considered as proportionate and strictly necessary in a democratic society, as is required under the protection offered by the applicable fundamental rights. Additionally, comprehensive oversight of all surveillance programmes is crucial. pg. 4			P
[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			A D

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	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			
[UP-D30-R03]	The WP29 has already explained the way it applied the core EU data protection principles to transfers of personal data to third countries in its Working Document 12 'Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive'. The WP29 tried to find the equivalent safeguards which ensure a level of protection equivalent to the principles guaranteed in the Directive, notably regarding purpose limitation, data quality and proportionality, transparency, security, rights of access, rectification and opposition, data retention and restrictions on onward transfers. pg. 11			M
[UP-D30-R04]	WP29 stresses that any interference with the fundamental rights to private life and data protection need to be justifiable in a democratic society. The CJEU criticised the fact that the Safe Harbour decision did not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference. Nor does it refer to the existence of effective legal protection against interference of that kind.pg 11			D
[UP-D30-R05]	In order to evaluate if any interference would be justifiable in a democratic society, the assessment was conducted in light of the European jurisprudence on fundamental rights which sets four essential guarantees for intelligence activities [as detailed in [UP-D30-R06 to R08]	Precedes [UP-D30-R06 to R08]		D
[UP-D30-R06]	* Processing should be in accordance with the law and based on clear, precise and accessible rules: this means that anyone who is reasonably informed should be able to foresee what might happen with her/his data where they are transferred;	Supports [UP-D30-R05]		A L
[UP-D30-R07]	* Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated: a balance needs to be found between the objective for which the data are collected and accessed and the rights of the individual;	Supports [UP-D30-R05]		R
[UP-D30-R08]	* An independent oversight mechanism should exist, that is both effective and impartial: this can either be a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks;	Supports [UP-D30-R05]		D
[UP-D30-R09]	Effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body. pg. 12			AB D
[UP-D30-R10]	Scope of application of the EU data protection framework and, in particular, of the Directive 95/46/EC principles: The WP29 recalls that under the EU data protection legal framework, and in particular under the Directive (Article 4(1)), Member States laws apply not only to the processing operations carried out by data controllers established on their territory, but also where data			AB

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	controllers (although not established in the EU), make use of equipment situated on EU territory, in particular for the collection of personal data. As a consequence, EU Member State law applies to any processing that takes place prior to the transfer to the U.S., either in the context of activities of an organisation established in the EU or through the use of equipment situated in the EU used by an organisation not established in the EU. pg. 12			
[UP-D30-R11]	It is therefore crucial to clarify in the Principles that in case of such contradiction, the provisions of the data processing contract and particularly the instructions of the organization transferring the data out of the EU will prevail. Without such clarification, the Principles could be interpreted and applied in a manner that offers too much control capacities to the Shield Agent and this would put the EU data exporter at risk of violating his obligations as a data controller under EU data protection law to which it is subject when transferring data to a Shield organisation acting as an Agent. In addition, this lack of clarity gives the impression that the processor might reuse the data as he wishes.pg 16			AB M
[UP-D30-R12]	Annex II, I.5. provides, among others, for exemptions from the Principles when data covered by the Privacy Shield is used for reasons of national security12, public interest, law enforcement, or following statute, government regulation or case law which creates conflicting obligations or explicit authorisations. Without full knowledge of U.S. law at both the Federal and at state level, it is difficult for the WP29 to assess the scope of this exemption and to consider whether those limitations are justifiable in a democratic society. It would be essential that the European Commission also includes in its draft adequacy decision an analysis of the level of protection where those exemptions would apply. pg. 17			G
[UP-D30-R13]	The Data Retention Limitation principle (Article 6(1)e of the Directive) is a fundamental principle in EU data protection law imposing that personal data must only be kept as long as necessary to achieve the purpose for which the data have been collected or for which they are further processed.pg 17			D
[UP-D30-R14]	Moreover, the WP29 emphasises that a general right to object (on compelling grounds relating to the data subject's particular situation), being understood as a right to ask to terminate the processing about one's data whenever the individual has compelling legitimate grounds relating to his particular situation, should be offered within the Privacy Shield. The WP29 strongly recommends that the draft adequacy decision makes clear that the right to object should exist at any given moment, and that this objection is not limited to the use of the data for direct marketing. pg. 20			M
[UP-D30-R15]	It should be clarified that in any case, the Choice principle cannot be used to circumvent the			D

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	Purpose limitation principle19. Choice should be applicable only where the purpose is materially different but still compatible since the processing for incompatible purpose is prohibited (Annex II, II.5.a). It has to be clarified that the right to opt-out cannot enable the organisation to use data for incompatible purposes.pg 20			
[UP-D30-R16]	The WP29 recommends also inserting a clear reference to the Purpose Limitation principle (Annex II, II.5) within the conditions for onward transfers to a third party controller (Annex II, II.3.a). This would make clear that onward transfers may not take place where the third party controller will process data for an incompatible purpose. pg. 21			M
[UP-D30-R17]	The WP29 notes that the Accountability for Onward Transfer principle (Annex II, II.3) explains that personal data may be transferred to a third party acting as an Agent only for limited and specified purposes, but does not explicitly say that these limited and specified purposes have to be compatible with the initial purposes for which the data were collected as well as with the instructions of the controller. More clarity is needed on this point. pg. 21			M
[UP-D30-R18]	PPD-28 imposes limits on the use of signals intelligence collected in bulk as regards the purpose of the use. These six purposes for which data can be collected in 'bulk', including counter-terrorism and other forms of serious (transnational) crimes. The WP29's analysis suggests that the purpose limitation is rather wide (and possibly too wide) to be considered as targeted.pg.38			A Q
[UP-D30-R19]	the WP29 recalls that it has consistently considered that massive and indiscriminate collection of data in any case cannot be regarded as proportionate.pg. 39			R
[UP-D30-R20]	WP29 notes that also targeted data processing, or processing that is 'as tailored as feasible', can still be considered to be massive. Whether or not such massive data collection should be allowed or not is currently subject to proceedings before the CJEU. For this reason, the WP29 shall not make a final assessment as to the legality of targeted, but massive data processing. However, it stresses that if targeted, but massive data processing would be allowed, the targeting principles should apply to both the collection and the subsequent use of the data, and cannot be limited to just the use…The WP29 is, at this stage, not convinced these purposes are sufficiently restricted to ensure the data collection is indeed restricted to what is necessary and proportional. pg.40			M
[UP-D30-R21]	4.2.1 Access by law enforcement authorities to personal data should be in accordance with the law and based on clear, precise and accessible rules. pg.53			Q
[UP-D30-R22]	Since all applicable rules to limit access by law enforcement authorities to data transferred under the Privacy Shield are based on the Constitution, on statutory law and on transparent policies of the Department of Justice, a presumption of accessibility of these rules is taken into account by the WP29. However, the clarity and precision of the rules can only be assessed in each individual			Q

QQ-D#-R#	Possible Requirement	Pre-Requisites/Dependencies	Ph	Gr
	type of procedure and request for access. The WP29 therefore regrets to note that, based on the available details in Annex VII to the Privacy Shield and the findings in the draft decision, such an assessment cannot be done at this momentpg.pg 53			
[UP-D30-R23]	Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated The WP29 duly notes that requesting access to data for law enforcement purposes can be considered to pursue a legitimate objective. For instance, Article 8(2) ECHR accepts interferences to the right to the protection for private life by a public authority "in the interests of (…) public safety, (…) for the prevention of disorder or crime". However, such interferences are only acceptable when they are necessary and proportionate pg.53			Q R
[UP-D30-R24]	According to the settled case-law of the CJEU, the principle of proportionality requires that the legislative measures proposing interferences with the rights to private life and to the protection of personal data "be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives." Therefore, the assessment of necessity and proportionality is always done in relation to a specific measure envisaged by legislation. pg. 54			R
[UP-D30-R25]	The first concern is that the language used in the draft adequacy decision does not oblige organisations to delete data if they are no longer necessary. This is an essential element of EU data protection law to ensure that data is kept for no longer than necessary to achieve the purpose for which the data were collected pg.57			O

Initial Group Key: (initial groupings may be reworked by WG during deliberation)

A = Purpose
B = Contact data for technical resolution
C = Registration data query, search and disclosure
D = Policy needs
E = Identifying own data and access
F = Contact data for other than technical resolution
G = Proxy
H = Extensibility
I = Research (other than for legal investigation)
J = Legal research
P = Use of data for surveillance
Q = Law Enforcement Investigation
R = Proportionality of use of the data
S = Gated Data Access
T = Public Data Access
U = Access Policies, including Authenticated Access
V = Access Violation
X = Encryption
Y = Internalization
Z = Audit or Logging

K = Registrar transfer policy
L = Consent
M = Controller/Processor/Processing or transfer of data
N = Accuracy of data
O = Retention of data

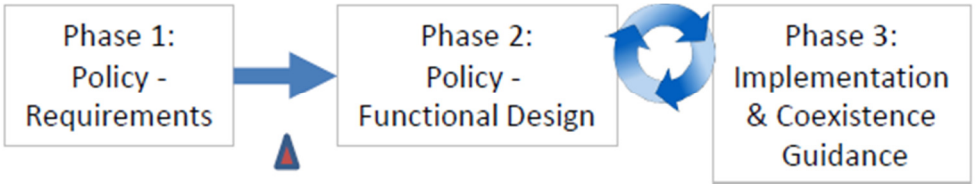
AA = Validation of Contact Data
AB = Applicable Law
AC = Cert Authority (or any third party that has duty to validate)
AD = Transparency

See Additional Key Inputs for this charter question (hyperlinked on this Wiki page) which may be consulted as a potential source of ***possible*** requirements. The PDP WG may also identify additional sources by themselves or through community outreach.

Gated Access (GA)

The following ***possible*** requirements address the charter question on Gated Access (GA):
What steps should be taken to control data access for each user/purpose?

The process framework for this question (below) can be applied to categorize ***possible requirements*** into three phases:



In the grid below, we identify the ***possible requirement*** for WG deliberation, any **pre-requisites or dependencies** contained in that ***possible requirement***, and whether the ***possible requirement*** therefore falls into Phase 1, 2, or 3. Policies designed to meet **Phase 1** policy requirements should be considered in **Phase 2**, while implementation or coexistence guidance for Phase 2 policies should be considered in **Phase 3**. In addition, an initial attempt has been made to **group similar requirements**, allowing the table to be easily re-sorted by Group. These initial groups are defined below the grid and may be revamped by the WG during deliberation.

Annex A. Key Input Documents

[01] EWG Final Report

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

[03] SAC055, WHOIS: Blind Men and an Elephant (September 2012)

[04] Human Rights Council - Report by the UN Special Rapporteur on the right to privacy (2016)

[05] Legacy WHOIS protocol (RFC 3912) (2004)

[06] 2013 Registrar Accreditation Agreement (RAA), including RAA WHOIS requirements for Registrants (2013)

[07] 2014 New gTLD Registry Agreement, including Specification 4 Registration Data Publication Services (2014)

[08] Steve Metalitz: Additional Possible Requirements

[09] WHOIS Policy Review Team Final Report (2012)

[10] SAC058, Report on Domain Name Registration Data Validation (2013)

[11] ARS Phase 1 Validation Criteria

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

[13] Review of the ICANN Procedure for Handling WHOIS Conflicts with Privacy Law (2014)

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

[15] WHOIS Uniform Domain Name Dispute Resolution Policy and Rules for Uniform Domain Name Dispute Resolution Policy

[16] WHOIS New gTLD URS Policy and Rules for URS Policy

[17] WHOIS Expired Domain Deletion Policy

[18] WHOIS Inter-Registrar Transfer Policy

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

[20] Article 29 WP statement on the data protection impact of the revision of the ICANN RAA (2013-2014)

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

[22] Article 29 WP 76 Opinion 2/2003

[23] Article 29 WP 203 Opinion 3/2013

[24] Article 29 WP 217 Opinion 4/2014

[25] Council of Europe's Treaty 108 on Data Protection (1985)

[26] European Data Protection Directive (1995)

[27] EDPS comments on ICANN's public consultation on 2013 RAA Data Retention Specification Data Elements and Legitimate Purposes for Collection and Retention (17 April 2014)

[28] Definition of Data Controllers

[29] Obligations of Data Controllers

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

[31] Africa Union Convention on Cybersecurity and Personal Data Protection

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

[33] White Paper: Management of Internet Names and Addresses, Statement of Policy (2012)

[34] Kathy Kleiman: Additional Possible Requirements

[35] The Constitution of the State of California (USA): Article 1, Section 1

[36] Massachusetts (USA) Right of Privacy, MGL c.214, s.1B

[37] U.S. Supreme Court Case - McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995)

[38] Ghana Protection Act, 2012

[39] South Africa's Act No. 4 of 2013: Protection of Personal Information Act (2013)

[40] RFC 7480: Registration Data Access Protocol (RDAP) (2015)

[41] RFC 7481: Security Services for the Registration Data Access Protocol (RDAP) (2015)

[42] RFC 7482: Registration Data Access Protocol (RDAP) Query Format (2015)

[43] Extensible Provisioning Protocol (EPP - RFC 5730) (2009)
Includes related RFCs 5731, 5732, 5733

[44] Article: Global data privacy laws 2015: 109 countries, with European laws now a minority (Greenleaf)

[45] How to Improve WHOIS Data Accuracy, by Lanre Ajayi, EWG Member

[46] Some Thoughts on the ICANN EWG Recommended Registration Directory Service (RDS), by Rod Rasmussen, EWG Member

Additional Key Input Documents (hyperlinked) to be inserted here as requirements are added.
Document titles and hyperlinks will be copied from (or as necessary, added to) these WG Wiki pages:
Key Input Documents and Questions posed by the Charter.

RDS PDP Initial List of *Possible* Requirements Draft #3 – Triage In Progress as of 21 June 2016

Note: This triaged draft in progress contains *possible* requirements for registration data and directory services submitted by RDS PDP WG members as of 10 June and published as Draft 3. WG members continue to work on possible requirements from several other key documents already identified, including the following submissions not yet incorporated into this triaged draft:

- WHOIS Misuse Study and Final Study Report (2014)
- Marrakech, Singapore, and Los Angeles GAC Communiqués (2014-2016)
- Article 29 WP 33 Opinion 5/2000
- U.S. Federal Communications Commission Proposed Rule FCC 16-39: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services

Assignments still underway as of 21 June include:

- WHOIS Privacy and Proxy Services Abuse Study and Final Study Report (2014)
- SAC051, Report on Domain Name WHOIS Terminology (2011)
- Final Report from the Working Group on Internationalized Registration Data (2015)
- Final Report from the Expert Working Group on Internationalized Registration Data (2015)
- GNSO PDP on Translation/Transliteration of Contact Information and Final Report (2015)
- GNSO PDP on Privacy & Proxy Services Accreditation Issues (PPSAI), Final Report, and GNSO Council Recommendations to Board (2015)
- Article 29 WP 41 Opinion 4/2001, and Article 29 WP 56 Working Document 5/2002
- Final Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)
- IWG Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet(Crete, 4./5.05.2000)
- Privacy Considerations for Internet Protocols (RFC 6973) (2013)
- Book: Global Tables of Data Privacy Laws and Bills (Greenleaf, 4rd Edition, January 2015)