RDS PDP Initial List of *Possible* Requirements Draft #3 - 10 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.

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.

RDS PDP Initial List of *Possible* Requirements Draft #3 - 10 June 2016)

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.

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?

[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

Users/Purposes Reqs	Users/Purposes Design	Users/Purposes Guidance on
- Permissible Users	- Data per Purpose	- Accreditor Criteria
- Permissible Purposes	- Update Process	- Terms of Service Needs
- Guiding Principles	- Accreditation Policy Per User Community	

[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)

[UP-D01-R02] – "gTLD registration data [must be] collected, validated and disclosed for permissible purposes only." (p. 21, p. 31 Principle 6)

[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)

[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."

[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."

[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."

[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."

[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."

[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."

[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."

[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. "

[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."

[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."

[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."

[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.)

[UP-D01-R16] – "All purposes/contacts must be codified by policymakers through a defined process for adding, changing, or deleting purposes." (p.37)

[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.

[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)

[UP-D01-R19] – gTLD registration directory services must provide the "The ability to determine historical domain name registration information (commonly referred to as WhoWas)."

[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.

[UP-D01-R21] – There must be clearly defined permissible/impermissible uses of gTLD registration data and directory services.

[UP-D01-R22] – gTLD registration directory services must support defined permissible purposes, including uses that involve:
[UP-D01-R23] – Identifying the Registrant and contacts designated for a given purpose;
[UP-D01-R24] – Communicating with contacts designated for a given purpose;
[UP-D01-R25] – Using data published by Registries about Domain Names; and
[UP-D01-R26] – Searching portions of registration data required for a given purpose.

[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-R28] – An application process must be defined.
[UP-D01-R29] – Applications must be reviewed against defined criteria.
[UP-D01-R30] – Applications that pass review must be evaluated and approved by a multistakeholder review board as determined by a policy development process.
[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.

[UP-D01-R33] – All permissible purposes must be mapped to specific contact data needed for that specific purpose. (p.36)

[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.

[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.]

[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.

[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.

[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.

[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].

[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.

[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.

[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.

[UP-D01-R43] – ". . . the [gTLD registration directory service] portal [must] make the definitions for every 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."

[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-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.

[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.

[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:

[UP-D06-R03] – Registrar shall make a complete electronic copy of the data available at least one (1) time per week for download by third parties who have entered into a bulk access agreement with Registrar.

[UP-D06-R04] – Registrar may charge an annual fee, not to exceed US$10,000, for such bulk access to the data.

[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.

[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.

[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.

[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.

[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 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.

[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.

[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.

[UP-D07-R02] – From Section 1.10.1: Registry Operator will offer searchability on the web-based Directory Service.

[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.).

[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).

[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.

[UP-D07-R06] – From Section 1.10.5: Search results will include domain names matching the search criteria.

[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.

[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. (Related to **[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. (Related to **[UP-D01-R14]**)

[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.

[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.

[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.

[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.

[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.

[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.

[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."

[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 ICANNRADAR 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."

[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."

[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 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:

[UP-D19-R02] – Providing "a lookup service to internet users" (para 3.1 and para 2.1)

[UP-D19-R03] – "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-R04] – "Allowing users to determine the availability of domain names" (para 3.1 and para 2.1.2)

[UP-D19-R05] – "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-D19-R06] – "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)

[UP-D19-R07] – "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-D19-R08] – "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-D19-R09] – "Assisting businesses, other organizations and users in combating fraud and general compliance with relevant laws" (para 3.1 and para 2.1.7)

[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:

[UP-D21-R02] – Need a well-defined purpose for processing/use of data;

[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

[UP-D21-R04] – Bulk access to WHOIS data for direct marketing should be limited.

[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."

[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-D22-R01] – In sum, from the Article 29 WP's Opinion 2/2003, we could draw out the following *possible* Purpose requirements:

[UP-D22-R02] – Need a well-defined purpose;

[UP-D22-R03] – Data collected should be relevant (and not excessive) for defined purpose;

[UP-D22-R04] – Bulk access to WHOIS data for direct marketing should be limited;

[UP-D22-R05] – Data subjects should be provided with unambiguous and informed consent.

[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."

[UP-D22-R07] – In the Article 29 WP's Opinion 2/2003, the WP states "its support for ... limitation of bulk access for direct marketing issues."

[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

[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

[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

[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

[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.

[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, 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

[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

[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

[UP-D23-R09] – "First building block: purpose specification. Collection for 'specified, explicit and legitimate' purpose"

[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

[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

[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

[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

[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 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

[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

[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."

[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] – protects the collection and processing of personal data.

[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.)

[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."

[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

[UP-D26-R02] – According to the Directive (20), whereas the fact that the processing of data is carried out by a 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;

[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;

[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;

[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;

[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 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;

[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;

[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;

[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;

[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;

[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 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;

[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;

[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;

[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;

[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.

[UP-D26-R19] – According to the Directive, Member States shall provide that personal data must be:

[UP-D26-R20] – processed fairly and lawfully;

[UP-D26-R21] – 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;

[UP-D26-R22] – adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

[UP-D26-R23] – 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;

[UP-D26-R24] – kept in a form which permits identification of data subjects for no 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.

[UP-D26-R25] – According to the Directive Article 7, Member States shall provide that personal data may be processed only if:

[UP-D26-R26] – the data subject has unambiguously given his consent; or

[UP-D26-R27] – 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; or

[UP-D26-R28] – processing is necessary for compliance with a legal obligation to which the controller is subject; or

[UP-D26-R29] – processing is necessary in order to protect the vital interests of the data subject; or

[UP-D26-R30] – 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; or

[UP-D26-R31] – 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).

[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:

- 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
- (d) 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
- (e) the processing relates to data which are manifestly made public by the data subject or is 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.

[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.

[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.

[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 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."

[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.)

[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."

[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.

[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."

[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.
  (note: highlights are in the original)

[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

[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

[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

[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

[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:

[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;

[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;

[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;

[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

[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 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

[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

[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

[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

[UP-D30-R15] – It should be clarified that in any case, the Choice principle cannot be used to circumvent the 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

[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

[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

[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

[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

[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

[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 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

[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

[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

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?

[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

Gated Access Reqs	Gated Access Design	Gated Access Guidance on
- Levels of Access (e.g., Public/Gated)	- Authorized Levels Per User/Purpose	- Access Protocol Needs
- Criteria for each Level	- Credentialing Policy	- Authentication Needs
- LE Access Principles	- Anti-Abuse Policy	- Credential Admin Needs
		- Training Needs

[GA-D01-R01] – "gTLD registration data must be collected, validated, and disclosed for permissible purposes only, with some data elements being accessible only to authenticated requestors that are then held accountable for appropriate use." (Permissible Purpose Principle 6 on page 31, relevant to both UP and GA Questions)

[GA-D01-R02] – "Every Registrant must have the ability to access all public and gated information published in the [gTLD registration directory services] about their domain name, including designated contact data." (Permissible Purpose Principle 7 on page 31, relevant to both UP and GA Questions)

[GA-D01-R03] – To maximize Registrant privacy, Registrant-supplied data must be gated by default, except where there is a compelling need for public access that exceeds resulting risk.

[GA-D01-R04] – Registrants can opt into making any gated Registrant-supplied data public with informed consent. (Data Disclosure Principle 35 on page 45)

[GA-D01-R05] – gTLD registration directory services must make data accessible only in conformance with specified Data Access Principles (41-55 on pages 58-61), as follows:

[GA-D01-R06] – A minimum set of data elements, at least in line with the most stringent privacy regime, must be accessible by unauthenticated users.

[GA-D01-R07] – Multiple levels of authenticated data access must be supported, consistent with stated permissible purposes.

[GA-D01-R08] – gTLD registration directory services user access credentials must be tied to an auditable accreditation process.

[GA-D01-R09] – Access must be non-discriminatory (i.e., the process must create a level playing field for all requestors, within the same purpose).

[GA-D01-R10] – The gTLD registration directory service must deter misuse and promote accountability:

[GA-D01-R11] – All gTLD registration data element access must be based on a stated purpose;

[GA-D01-R12] – Access to gated data elements must be limited to authenticated requestors that assert a permissible purpose; and

[GA-D01-R13] – Requestors must be able to apply for and receive credentials for use in future authenticated data access queries.

[GA-D01-R14] – Some type of accreditation must be applied to requestors of gated access to gTLD registration data:

[GA-D01-R15] – When accredited Requestors query data, their purpose must be stated every time a request is made.

[GA-D01-R16] – Different terms and conditions may be applied to different purposes.

[GA-D01-R17] – If accredited requestors violate terms and conditions, penalties must apply.

[GA-D01-R18] – To raise the standard of gTLD registration data protection, all directory services queries/responses must make use of commonly-available message encryption and authentication measures to protect the confidentiality and integrity of data in transit.

[GA-D01-R19] – To meet the needs of authenticated users with permissible purposes, the gTLD registration directory must provide a Reverse Query service that searches public and gated data elements for a specified value and returns a list of all domain names that reference that value.

[GA-D01-R20] – To meet the needs of authenticated users with permissible purposes, the directory service must provide a WhoWas service that returns historical snapshots of public and gated data elements for specified domain names, limited to the historical data available.

[GA-D01-R21] – The gTLD registration directory service must support innovative services that make use of gTLD registration data elements, as follows.

[GA-D01-R22] - Third parties must be able to provide existing and future innovative services – including Reverse Queries and WhoWas – using public data elements and held to terms and conditions of gTLD registration data use.

[GA-D01-R23] In the event that third parties offer innovative services involving gated data elements, those third parties must be accredited and held to terms and conditions of gTLD registration data use.

[GA-D01-R24] – All disclosures of gated data elements must occur through defined gTLD registration directory service access methods (including those described above). The entire registration data set for all gTLDs (or the entire Registry data set for a single gTLD) must not be exported in bulk form for uncontrolled access.

[GA-D01-R25] – Disclosures may occur through interactive display and other gTLD registration directory service access methods.

[GA-D01-R26] – To make data easier to find and access in a consistent manner, a central point of access (e.g., web portal) must be offered.

[GA-D01-R27] – Secure access to public gTLD registration data must be available to all requestors through an unauthenticated query method (at minimum, via secure website).

[GA-D01-R28] – Secure access to gated gTLD registration data must be supported through secure web and other access methods and formats based on authenticated requestor and purpose.

[GA-D01-R29] – Requestors must be able to obtain authoritative data from the gTLD registration directory service in real-time when needed.

[GA-D01-R30] – The gTLD registration directory service must accommodate automation for large-scale lookups for various use cases and permissible purposes.

[GA-D01-R31] – To be truly global, the gTLD registration directory service must accommodate the display of registration data in multiple languages, scripts and character sets, including Internationalized domain names (IDNs).

[GA-D01-R32] – The gTLD registration directory service should support all future GNSO-defined transliteration policies for gTLDs.

[GA-D01-R33] – The gTLD registration directory service should enable collection and display of registration data elements in local languages.

[GA-D01-R34] – "All access must be purpose-based, returning only data elements permitted for the stated purpose." (bottom of p.62)

[GA-D01-R35] – ". . for each [gTLD registration directory services] user community identified [under the Charter question on Users/Purposes] desiring access to gated data for permissible purposes, community experts must be consulted to confirm EWG-identified registration data purposes, the data elements that must be accessible for that purpose, and possible User Accreditors." (top of p.63)

[GA-D01-R36] – "Non-accredited, unauthenticated access to non-gated (i.e., public) data must be possible in real-time."

[GA-D01-R37] – "Accreditation of [gTLD registration directory service] users for access to [registration data] does not have to happen in real-time for all use cases and/or requesters."

[GA-D01-R38] – "[gTLD registration directory services] must only apply the minimum accreditation scheme necessary to provide users access to gated data elements for the stated purpose."

[GA-D01-R39] – "There must be no requirement to pre-approve or provide credentials to every potential user of [gTLD registration directory services.] A request and fulfilment process can be created for each type of accredited user (i.e., [gTLD registration directory services] user community)."

[GA-D01-R40] – Accreditation for [gTLD registration directory services] users seeking access to data for permissible purposes could be granted in various ways as determined by data access policy. For

example, None (i.e., unauthenticated access to public data only), self-accreditation by the person/entity requesting the data, or accreditation by some trusted third party.

[GA-D01-R41] – Whenever possible, any third party accreditation process must leverage existing accreditation processes within each user community that needs credentialing.

[GA-D01-R42] – "Third party accreditation processes must be vetted by an authority responsible for implementing and enforcing [gTLD registration directory services] user accreditation policy (for example, ICANN, a multistakeholder panel) and reviewed on a periodic basis."

[GA-D01-R43] – "Any organization serving as a [gTLD registration directory service] user accreditor must have a signed agreement with ICANN and/or the registration directory service provider to offer such accreditation processes under agreed-upon guidelines, and establish a framework to allow for due process, accountability, security, fair access, and adherence to applicable law."

[GA-D01-R44] – Accreditors must take on defined sets of responsibilities, such as establishing criteria for membership, setting credentialing requirements, defining and enforcing terms and conditions of membership, providing functions such as user account creation, credential issuance, suspension and revocation, lifecycle user account management, and associated processes such as dispute handling and ToC enforcement.

[GA-D01-R45] – Accreditors that wish to participate in handling gTLD registration directory services requests for data on behalf of their members must be able to do so in ways that enable auditing and abuse complaint resolution and hold parties responsible for compliant usage and accountable in the event of abuse.

[GA-D01-R46] – [gTLD registration directory services] must provide real-time access to credentialed requestors via multiple methods. Access credentials issued during accreditation must be suitable for use with all defined access methods.

[GA-D01-R47] – "Best practices may be defined for credential management; Accreditors must be expected to adhere to best practices."

[GA-D01-R48] – gTLD registration directory services "must require individual credentials for authenticated access."

[GA-D01-R49] – "Authenticated access [to gTLD registration data] must not be transitive (i.e., an authenticated user shall not share gated data with others outside of its accreditation)."

[GA-D01-R50] – "A process for responsible revelation of gated data to further the original purpose it was requested for must be created and enforced."

[GA-D01-R51] – "An organization seeking access to [gTLD registration] data must be able to apply for user accreditation and have all people using the registration directory service in their organization covered by that one accreditation, [accepting responsibility] for managing accredited access within its own organization."

[GA-D01-R52] –"Audits and data analytics must be used to identify abuse of the system and access credentials."

[GA-D01-R53] – "An appeals process must be defined to allow [gTLD registration directory services] users to refute abuse allegations when seeking to reactive/reinstate access credentials."

[GA-D01-R54] – "Every Registrant must receive a credential to be able to examine their own contact data as stored by the [gTLD registration directory service] in relation to domain names that are registered to them."

[GA-D01-R55] – "A process for adding additional accreditors that either supplement current processes or offer new, innovative ways to provide user accreditation for approved purposes of the [gTLD registration directory service] must be established."

[GA-D04-R01] – If there is gated access, the [gTLD registration directory service] must feature strong encryption.

[GA-D04-R02] – The [gTLD registration directory service] must not be engineered to contain any back-doors. By introducing a technical input into an encryption product that would enable any party, even authorities, access to data, would also make encrypted data vulnerable to criminals, terrorists and foreign intelligence services, among others. This would have an undesirable consequence for the security of data stored in the [gTLD registration directory service].

[GA-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.

[GA-D08-R01] – Accredited Requestors may pre-identify purposes that will apply to all or some of their queries over a specified time frame. (Related **to [GA-D01-R15]**)

[GA-D08-R02] – Other than in exceptional circumstances, accreditation of users for access to [gTLD registration] data should take place in real time. (Related to **[GA-D01-R37])**

[GA-D08-R03] – A process for responsible sharing of gated [gTLD registration] data within an accredited requester organization, with its affiliates, with its clients, or with similar third parties must be created and enforced. (Related to **[GA-D01-R50]**)

[GA-D18-R01] – Based on the WHOIS Inter-Registrar Transfer Policy, Section I.A.1.1: "The Administrative Contact and the Registered Name Holder, as listed in the Losing Registrar's or applicable Registry's (where available) publicly accessible WHOIS service are the only parties that have the authority to approve or deny a transfer request to the Gaining Registrar. Registrars may use WHOIS data from either the Registrar of Record or the relevant Registry for the purpose of verifying the authenticity of a transfer request; or from another data source as determined by a consensus policy."

[GA-D19-R01] – Based on the ICANN Governmental Advisory Committee (GAC) proposed principles, gTLD [registration directory] services "should provide (…) data (…) in a manner that (…) facilitates continuous, timely and world-wide access" (para 3.3, sub 2)

[GA-D26-R01] – According to the Directive (18), whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

[GA-D26-R02] – 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;

[GA-D26-R03] – 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;

[GA-D26-R04] – 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 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;

[GA-D26-R05] – According to the Directive (57), whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

[GA-D26-R06] – According to the Directive (58), whereas, provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

[GA-D26-R07] – 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.

[GA-D28-R01] – The definition of a Data Controller under the EU Privacy Directive requires that the Data Controller ensure that "the privacy rights of individuals supplying their personal data must be respected by anyone collecting and processing that data." [This definition requires that any] gates created [must] ensure that a Registrant in the EU or other data protection country has their data processed through the gates in accordance with their national laws, e.g., EU Data Protection Directive.

[GA-D29-R01] – Each data controller must respect the following rules as set out in the Directive: Personal Data must be processed legally and fairly.

[GA-D30-R01] – 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

[GA-D30-R02] – 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

[GA-D30-R03] – 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

[GA-D30-R04] – 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 listed in **[UP-D30-R05]**

[GA-D30-R05] – Privacy Shield documents make use of terminology that is not consistent with the vocabulary generally used in the EU when dealing with data protection. This is not necessarily a problem, as long as it is clear what the corresponding terminology under EU law (and under U.S. law) would be. The WP29 regrets to note however this is not the case, including in the draft adequacy decision. For example, the word 'access' is used in chapter 3 of the draft adequacy decision in a sense that implies the collection of personal data, instead of allowing someone to see data that is already collected. Access by companies to the data and the individuals' right of access are two separate notions that should not be confused. pg. 13

[GA-D30-R06] – The Privacy Shield does not provide any legal guarantees where individuals are subject to a decision which produces legal effects concerning or significantly affecting them and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to them, such as their performance at work, creditworthiness, reliability, conduct, etc. The necessity to provide for legal guarantees for automated decisions (producing legal effects or significantly affecting the individual) in order to provide an adequate level of protection has already been underlined by the WP29 in its Working Document 12.pg 18

[GA-D30-R07] – 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

[GA-D30-R08] – 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 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

[GA-D30-R09] – 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

[GA-D32-R01] – The specifications below are recommended requirements for registries. These requirements include an independently-tested, functioning Database and Communications System that:

[GA-D32-R02] – Allows multiple competing registrars to have secure access (with encryption and authentication) to the database on an equal (first-come, first-served) basis. (may also apply to System Model)

[GA-D32-R03] – Provides free access to the software and customer interface that a registrar would need to register new second-level domain names. (may also apply to System Model charter question)

[GA-D32-R04] – The specifications below are recommended requirements for registrars. These requirements include a functioning Database and Communications System that supports secure access (with encryption and authentication) to the registry. (may also apply to Privacy charter question)

[GA-D34-R01] – [gTLD registration directory services policies must consider this question:] How can we ensure in a centralized [or any other] Gated Access environment that law enforcement and lawyers and others seeking access to personal and/or sensitive data who are operating legally within the scope of their jurisdiction and authority?

[GA-D34-R02] – [gTLD registration directory services policies must consider this question:] In a Gated Access environment, how can we prevent access to the personal and/or sensitive data by those seeking to investigate matters that are not crimes or illegalities in the country of the Registrant or Registrar?

[GA-D34-R03] – [gTLD registration directory services policies must consider this question:] In a Gated Access environment, how can we ensure that those who abuse their access to massive amounts of data are prosecuted, and by someone other than the Registrant, who is unlikely to have the resources to address such matters. How does ICANN take on responsibility for the gTLD registration directory service, and liability for any abuses or misuses?

[GA-D42-R01] – RFC 7482, Section 7, Security Considerations, specifies "Search functionality typically requires more server resources (such as memory, CPU cycles, and network bandwidth) when compared to basic lookup functionality. This increases the risk of server resource exhaustion and subsequent denial of service due to abuse. This risk can be mitigated by developing and implementing controls to restrict search functionality to identified and authorized clients." This provides a *possible* requirement: A registration directory service must provide features to identify and authorize clients.

[GA-D42-R02] – RFC 7482, Section 7, Security Considerations, specifies "Search functionality also increases the privacy risk of disclosing object relationships that might not otherwise be obvious." This provides a *possible* requirement: A registration directory service must provide features to restrict information returned to clients on a "need to know" basis.

[GA-D42-R01] – RFC 7482: Registration Data Access Protocol (RDAP) Query Format, specifies a protocol "intended to address deficiencies with the WHOIS protocol [RFC3912] that have been identified over time." "The intent of the patterns described here are to enable queries of: (...) reverse DNS metadata by domain, name servers by name, registrars by name, and entities (such as contacts) by identifier." This provides *possible* requirements:

[GA-D42-R03] – A registration directory service must include features that address the deficiencies of WHOIS, including lack of standardized command structures, lack of standardized output and error structures, lack of support for internationalization and localization, and lack of support for user identification, authentication, and access control.

[GA-D42-R04] – A registration directory service must be able to support queries for reverse DNS metadata by domain, name servers by name, registrars by name, and entities (such as contacts) by identifier.

[GA-D41-R01] – RFC 7481: Security Services for the Registration Data Access Protocol (RDAP), Section 3.1, Access Control, specifies that "Information returned to a client can be clearly marked with a status value (see Section 10.2.2 of [RFC7483]) that identifies the access granted to the client." This provides a *possible* requirement: A registration directory service must be able to return information that identifies the access granted to the client. (May also be related to Users/Purposes**)**

[GA-D41-R02] – RFC 7481, Section 3.2, Authentication, specifies that "RDAP clients and servers MUST implement the authentication framework specified in "Hypertext Transfer Protocol (HTTP/1.1): Authentication" [RFC7235]." This provides a *possible* requirement: Registration directory service servers must be able to authenticate themselves to clients using HTTPS or a mechanism that provides an equivalent level of server authentication. (May also be related to Privacy)

[GA-D41-R03] – RFC 7481, Section 3.2, Authentication, specifies that "If the "basic" scheme is used, HTTP over TLS [RFC2818] MUST be used to protect the client's credentials from disclosure while in transit..." This provides a *possible* requirement: Connections between registration directory service clients and registration directory service servers must be encrypted to prevent inadvertent disclosure of information to passive eavesdropping attacks. (May also be related to Privacy)

[GA-D41-R04] – RFC 7481, Section 3.2, Authentication, specifies that "Servers MUST support either Basic or Digest authentication; they are not required to support both. Clients MUST support both to interoperate with servers that support one or the other." (May also be related to Privacy)

[GA-D41-R05] – RFC 7481, Section 3.2, Authentication, specifies that "transports for RDAP must either provide a TLS-protected transport (e.g., HTTPS) or a mechanism that provides an equivalent level of server authentication." This provides a *possible* requirement: A registration directory service must be able to support client authentication using HTTP Basic and Digest authentication. (May also be related to Privacy)

[GA-D41-R06] – RFC 7481, Section 3.2.1, Federated Authentication, specifies that "Federated authentication mechanisms used by RDAP MUST be fully supported by HTTP." This provides a *possible* requirement: Federated authentication systems used by A registration directory service must be fully supported by HTTP. (May also be related to Privacy)

[GA-D41-R07] – RFC 7481, Section 3.3, Authorization, specifies that "If such varying degrees of access are supported, an RDAP server MUST provide granular access controls (that is, per registration data object) in order to implement authorization policies." This provides a *possible* requirement: A registration directory service must provide granular access controls in order to implement authorization policies. (May also be related to Privacy)

[GA-D41-R08] – RFC 7481, Section 3.5, Data Confidentiality, specifies that “HTTP over TLS MUST be used to protect all client-server exchanges unless operational constraints make it impossible to meet

this requirement." This provides a *possible* requirement: A registration directory service must use HTTP over TLS to protect all client-server exchanges. (May also be related to Privacy)

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.

Data Accuracy (DA)

The following *possible* requirements address the charter question on Data Accuracy (DA):
What steps should be taken to improve data accuracy?

[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

Data Accuracy Reqs	Data Accuracy Design	Data Accuracy Guidance on
- Accuracy Principles - Contact Data Validation Needs	- Validation Levels - Contact Management - Remediation Policy	- Validator Criteria - Contact Auth Needs - Interface Needs (RDS/Validator/RR/Ry)

[DA-D01-R01] – "Standard validation [must be applied] to all gTLD registration data. In addition to periodic checks, validation would occur at the time of collection, with an option to pre-validate blocks of contact data for reuse in multiple domain name registrations." (top of p.69)

[DA-D01-R02] – "The [gTLD registration directory services] ecosystem must include a pre-validated Contact Directory, conceptually separate from the Domain Name Directory, to promote the quality and reusability of data elements used to contact domain name Registrants and people or organizations that can be designated by Registrants as contacts for various purposes associated with a domain name registration, and to deter the fraudulent use of personal data." (top of p.69)

[DA-D01-R03] – [gTLD registration directory services must support a] Pre-validation process (Section b on pp.71-72)

[**DA-D01-R05]** – [gTLD registration directory services must support an] Accuracy, Audit & Remediation Process (Section c on pp. 72-73)

[DA-D01-R06] – [gTLD registration directory services must include an] Operational Framework for Contact IDs (Section d on pp. 74-75)

[DA-D01-R07]– [gTLD registration directory services must have specified] Principles for Interaction between Contact Holders & Validators 83-89 (pp. 75-76)

[DA-D01-R08]– [To create and maintain] any given Contact, a Contact Holder may choose any Validator.

[DA-D01-R09]– Oversight and accountability policies related to the management of Contacts must be developed.

[DA-D01-R10]– Contact Holders must be able to modify the contact information…through the issuing Validator.

[DA-D01-R11]– Validators must use Contact Holder authentication to deter unauthorized modification of contact information. Validators may offer multiple levels of Contact Holder authentication.

[DA-D01-R12]– Contact Holders must be able to choose providers based on cost/benefit propositions tied to ease-of-use, security, costs, and other logical business factors.

[DA-D01-R13]– Validators must publish their policies on authentication in a manner that can be utilized globally for reputation management [to] encourage better accuracy and accountability.

[DA-D01-R14]– Validators must be able to validate contact information submitted in the Contact Holder's native language [to] improve accuracy of native-language data and support scalability of the domain name registration system into a multi-lingual environment.

[DA-D01-R15] – [gTLD registration directory services must have specified] Principles for Contact Validation 90-104 (pp.76-78)

[DA-D01-R16] – All contact data elements must be validated at a syntactic level. This represents a base-level of validation that must be achievable by any entity in the industry.

[DA-D01-R17] – All mandatory contact data elements for a particular purpose must be validated operationally before that contact can be included in domain name registration data for that purpose.

[DA-D01-R18] – A Contact Holder must be able to voluntarily seek optional higher levels of validation (e.g., optional identity validation), bearing associated costs in return for perceived benefits (e.g., greater consumer confidence in domain names registered to identity-validated entities).

[DA-D01-R19] – Given costs involved with optional identity validation, a low-cost mechanism for economically disadvantaged Contact Holders to receive optional identity validation is desirable.

[DA-D01-R20] – In order to preserve associations and allow for a correction process, contact data can have a status of "inaccurate" and remain in the system.

[DA-D01-R21] – Validation Status of contact data must be tracked and published as appropriate [in the registration directory service], along with the most recent time the validation status was determined.

[DA-D01-R22] – Third parties may file inaccuracy reports to challenge the Validation Status of contact data, triggering a standard remediation process that may result in the contact being flagged as "inaccurate" and in further consequences for domain names using that contact data.

[DA-D01-R23] – Active domains cannot have a mandatory contact with an "inaccurate" status without some sort of remediation.

[DA-D01-R24] – A minimum level of cross-field validation must be checked for all contact data elements associated with contacts where cross-field validation is applicable (e.g. physical address).

[DA-D01-R25] – Revalidation of contact data must be carried out on a regular basis to ensure data is accurate at the declared level.

[DA-D01-R26] – If a Contact Holder provides optional data elements, those elements must be at least syntactically validated. Optional data elements must not be validated beyond syntax unless the Contact requests and presumably pays for any costs associated with such validation.

[DA-D01-R27] – The level of validation achieved beyond syntactical validation for data elements that can be operationally- or (optionally) identity-validated must be recorded and maintained by the Validator.

[DA-D01-R28] – The Validator must determine and publish [in the gTLD registration directory service] the overall validation status achieved by each contact.

[DA-D01-R29] – For any data element that has undergone validation, the timestamp of that validation must also be recorded and maintained.

[DA-D01-R30] – [gTLD registration directory services must offer an optional] Unique Contact Data Capability (Section g on p.78)

[DA-D01-R31] – "To allow for much greater accuracy across such a diverse space and ease-of-use for such contacts, it is desirable to provide mechanisms to allow easy use of such contacts by multiple Registrants; for example, a web hosting company providing their NOC's unique ID for "technical" and "abuse" contacts for domains controlled by their customers." (Bottom of p.69) [Also included as a *possible* Benefits requirement]

[DA-D01-R32] – ". . when such an entity needs to update their contact information to reflect a new address/phone number or a merger/acquisition, it must be easy to update that information in one place and have that reflected to all domains associated with that contact data set (as designated by a unique identifier)." (Top of p.70) [Also included as a *possible* Benefits requirement]

[DA-D02-R01] – "An accuracy policy should define each data element and require that it be examined and indicate for each element a method for determining the level of accuracy of the data."

[DA-D02-R02] – "Policies with respect to the accuracy of registration data should apply equally to all registration data without regard to whether it is internationalized or ASCII registration data."

[DA-D06-R01] – Upon receiving any updates to the data elements listed in [RAA] Subsections 3.3.1.2, 3.3.1.3, and 3.3.1.5 through 3.3.1.8 from the Registered Name Holder, Registrar shall promptly update its database used to provide the public access described in [RAA] Subsection 3.3.1.

[DA-D06-R02] – Registrar shall comply with the obligations specified in the [gTLD registration directory service] Accuracy Program Specification. In addition, notwithstanding anything in the Accuracy Program Specification to the contrary, Registrar shall abide by any Consensus Policy requiring

reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with a Registered Name sponsored by Registrar or (b) periodic re-verification of such information. Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy.

[DA-D08-R01] – All mandatory contact data elements for a particular purpose must be validated operationally before the corresponding registration is activated. (Related to **[DA-D01-R17]**)

[DA-D09-R01] – The WHOIS RT recommends fulfillment of data accuracy objectives over time. Specifically:

[DA-D09-R02] – The [WHOIS RT] notes that the focus of its recommendations is on the desired outcome that ICANN work to improve the accuracy of [gTLD registration] data. [Data] validation or verification would be one possible means to achieve this objective, whereas our intention is to allow latitude in how the objective is achieved.

[DA-D09-R03] – Based on review of a study on data accuracy that ICANN asked the National Opinion Research Council of the University of Chicago to provide ("NORC WHOIS Data Accuracy Study 2009/10"), the WHOIS RT recommended that ICANN pursue a "contactability standard" for data accuracy in the WHOIS – enough accurate data elements for the Registrant to be contacted (minimal data elements).

[DA-D09-R04] – In Recommendation 6, the WHOIS RT recommended that ICANN should take appropriate measures to reduce the number of WHOIS registrations that fall into the accuracy groups Substantial Failure and Full Failure (as defined by the NORC Data Accuracy Study, 2009/10) by 50% within 12 months and by 50% again over the following 12 months. (Refer to the NORC study for definitions of Substantial and Full Failure.)

[DA-D10-R01] – In SAC058, a report to the ICANN Board from the Security and Stability Advisory Committee (SSAC) concerning the issue of domain name registration data quality, the SSAC examines the feasibility and suitability of improving registration data accuracy through validation, offering the following *possible* Data Accuracy requirements.

[DA-D10-R02] – [ICANN should] identify [registration data] validation techniques that can be automated and develop policies that incent the development and deployment of those techniques. (Page 4)

[DA-D10-R03] – To improve registration data accuracy, there needs to be 1) an incentive for the registrant to submit accurate data, or 2) efforts by registry / registrar to follow up and check the accuracy of the submitted data; or 3) both. (Page 5)

[DA-D10-R04] – [As further detailed below, registration data should undergo] Syntactic Validation: Assess [registration] data with the intent to ensure that they satisfy specified syntactic constraints,

conform to specified data standards, and are transformed and formatted properly for their intended use. (Page 7)

[DA-D10-R05] – [As further detailed below, registration data should undergo] Operational Validation: Assess that [registration] data correspond to the intended use in their routine functions (e.g. check that an email address or phone number can receive email or phone calls, check that a postal address can receive postal mail, etc.). (Page 8)

[DA-D10-R06] – [As further detailed below, registration data should undergo] Identity Validation: Assess that [registration] data corresponds to the real world identity of the registrant entity. (Page 8)

[DA-D10-R07] – [ICANN should] Determine the length of time before the validation of changes to contact information must be repeated. (Page 8-9)

[DA-D10-R08] – Name validation should be implemented as follows:

- Syntactic Validation: To achieve effective syntactic validation of a name as one of the contact information elements, the script (or writing system) used for a name element must be known. If it is, confirming that the syntax conforms to the script is possible and can be automated. However, the language of a name cannot be determined precisely as many languages share the same script. (Page 9)
- Operational Validation: Create exception lists for auditing purposes in order to facilitate the process of operational validation of names because names in the world are diverse and it may not be possible to operationally verify a name automatically. (Page 10)
- Identity Validation: Require the submission of physical documentation issued by a government authority to verify that registration data contact information corresponds to a real world entity. (Page 10)

[DA-D10-R09] – Email address validation should be implemented as follows:

- Syntactic Validation: Syntax for a valid email address (defined as per RFC 5322) and syntax for a valid internationalized email address (defined as per PRFs 6530-33) should be checked automatically. (Page 10)
- Operational Validation: Having in mind that an email address is defined as a string composed of a Left Hand Side (LHS) and Right Hand Side (RHS) separated by the at-symbol (@), verify that an email address is operational implementing several checks (e.g. with respect to the RHS check that the domain name exist in the DNS while with respect to the LHS check that the endpoint SMTP accepts an email message for the recipient specified at the LHS). (Page 10)
- An effective verification technique of an email address is to attempt to deliver an email message that requires explicit user action. In this technique, an email address should not be considered valid until the user receives and performs some action described in the email, such as clicking on a web link or replying to the message in a specified way. Note that sometimes anti-spam measures could still block these verification emails. (Page 11)
- Identity Validation: In order to verify that an email address is used exclusively by a particular registrant, contact the registrant using an out-of-band method, i.e., contacting the registrant

without using email (e.g. two possibilities are using the postal information or the telephone information to contact the registrant). (Page 11)

[DA-D10-R10] – Telephone number validation should be implemented as follows:

- Syntactic Validation: Perform automatic checks to determine if a telephone number complies with the E.164 standard (E.164 is an ITU-T recommendation that defines the international public telecommunication numbering plan used in the PSTN and some other data networks). (Page 11)
- Operational Validation: Verify E.164 formatted PSTN addresses (telephone numbers) by leveraging PSTN databases. (Page 11)
- Use the Short Message Service (SMS) to verify a phone number (works only for cellular numbers). (Page 12)
- Identity Validation: In order to verify that a telephone number is used exclusively by a particular registrant, contact the registrant using an out-of-band method, i.e., contacting the registrant without using the telephone number (e.g. two possibilities are using the postal information or the email address to contact the registrant). (Page 12)

[DA-D10-R11] – Postal address validation should be implemented as follows:

- Syntactic Validation: The EPP standard defines an opaque container and loose constraints that can support internationalized postal addresses.
- Operational Validation: Verify postal addresses by leveraging postal databases. There are about 200 such databases in the world with about 20 (G20 major economies) being highly accurate. (Page 13)
- Deliver a postal message to a postal address in order to verify with a high level of certainty that the postal address is valid. (Page 13)
- Identity Validation: In order to verify that a postal address is used exclusively by a particular registrant, contact the registrant using an out-of-band method, i.e., contacting the registrant without using the postal address (e.g. two possibilities are using the telephone number or the email address to contact the registrant). (Page 13)

[DA-D11-R01] – The accuracy of [gTLD registration data] must be assessed by asking the following questions. Answers in the negative indicate inaccurate data. The criteria are based on the obligations contained in the 2009 and 2013 RAA.

[**DA-D11-R02]** – Phase One: Syntax Validation must be performed on gTLD registration data elements that are email addresses, as follows:

- Does the email address only contain permissible characters? (i.e., as provided for within the RFC 5322)
- Is there presence of an "@" symbol in the email address?
- Is there presence of a domain component?
- Is the domain component in a TLD, which is resolvable on the Internet? (see IANA's Root Zone Database: http://www.iana.org/domains/root/db)

- Is the domain component syntactically valid? (i.e., the component following the "@" symbol meets requirements)
- Is there presence of local component? (i.e., the characters preceding the "@" symbol)

[**DA-D11-R03]** – Phase One: Syntax Validation must be performed on gTLD registration data elements that are telephone numbers, as follows:

- Is there presence of a phone number? (not required for registrant field for 2009 RAA)
- Is there presence of a country code?
- Is the country code syntactically valid? (not required for 2009 RAA)
- Does the phone number contain at least the minimum allowed digits based on the country code?
- Does the phone number contain an appropriate amount of digits based on the country code?
- Does the phone number only contain permissible numbers and formatting characters?
- if there is an extension does it only contain permissible numbers and formatting characters?

[DA-D11-R04] – Phase One: Syntax Validation must be performed on gTLD registration data elements that are postal addresses, as follows:

- Is there presence of a postal address?
- Is there presence of a country?
- Is the country identifiable?
- Is the country provided in the Country field? (not required for 2009 RAA)
- Is the country syntactically valid? (i.e., meets ISO 3166-1: Alpha 2-code format) (not required for 2009 RAA)
- If the country uses a postal code system, is the code syntactically valid and in the right field?
- If a country requires a state or province, is a state listed and is it syntactically valid? (not required for 2009 RAA)
- Is there presence of a city?
- Is there presence of a street?

[DA-D12-R01] – Data in the [gTLD registration directory service] must be synchronized, i.e., updated in an immediate and accurate manner so that all data sets (e.g., registrar and registry) are exact duplicates. (sec. 5.7)

[DA-D12-R02] – The [gTLD registration directory service] must include features to reduce the risk of inconsistencies between data sets held by different parties (i.e., synchronization failures). (sec. 5.7)

[DA-D12-R03] – The [gTLD registration directory service] must specify the single data set (among multiple data sets) to be relied upon in case of doubt (i.e., the authoritative data). (sec. 5.8) [may also relate to Users/Purposes]

[DA-D12-R04] – To the extent the [gTLD registration directory service] involves a hierarchical database structure, it must specify the single database within that structure that holds the data that is assumed to be the final authority regarding the question of which record shall be considered

accurate and reliable in case of conflicting records (i.e., the authoritative data). (sec. 5.8) [may also relate to Users/Purposes]

[DA-D15-R01] – ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) requires registrant information taken from [gTLD registration directory services] for the disputed domain name to be accurate to meet UDRP-related Data Element requirements - see **[DE-D15-R01]** through **[DE-D15-R03]**.

[DA-D15-R02] – ICANN's UDRP makes Domain Registrant liable to provide complete & accurate statements, including contact information, which forms part of Domain WHOIS, by default. Specifically, registrants who apply "to register a domain name, or to maintain or renew a domain name registration, [must] represent and warrant... that (a) the statements ... made in [their] Registration Agreement are complete and accurate." (UDRP policy, Paragraph 20)

[DA-D16-R01] – ICANN's Uniform Rapid Suspension (URS) policy requires registrant information taken from [gTLD registration directory services] for the disputed domain name to be accurate for proper completion of the Complaint, for proper service of hard copy Notice, and to meet additional URS-related Data Element requirements - see **[DE-D16-R01]** through **[DE-D16-R09]**.

[DA-D18-R01] – Based on the WHOIS Inter-Registrar Transfer Policy, **Section I.A.3.7**: "Upon denying a transfer request for any of the following reasons, the Registrar of Record must provide the Registered Name Holder and the potential Gaining Registrar with the reason for denial. The Registrar of Record may deny a transfer request only in the following specific instances:

- Reasonable dispute over the identity of the Registered Name Holder or Administrative Contact.
- The transfer was requested within 60 days of the creation date as shown in the registry WHOIS record for the domain name."

[DA-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)

[DA-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* requirement: Data should be accurate. Specifically, Article 29 expresses "support for earlier proposals concerning accuracy of the data (which is also one of the principles of the Data Protection Directive) published in WHOIS directories ..."

[DA-D22-R01] – In sum, from the Article 29 WP's Opinion 2/2003, we could draw out the following *possible* requirement: Data should be accurate. Specifically, the WP states "its support for the proposals concerning accuracy of the data (which is also one of the principles of the European Data Protection Directive) ..."

[DA-D25-R01] – Council of Europe's Treaty 108 on Data Protections enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected.

[DA-D26-R01] – According to the Directive (38), whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

[DA-D26-R02] – 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;

[DA-D30-R01] – The Data Integrity and Purpose Limitation principle (Annex II, II.5) also states: "To the extent necessary for those purposes, an organisation must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete and current". The WP29 notes that this is exactly the same wording as used in the Safe Harbour arrangement. The WP29 doubts that the wording "to the extent necessary to these purposes" should be included, since the accuracy of the data in its view should not depend on the purpose of the processing. The WP29 would prefer if this connection is not made in the final adequacy decision.pg24

[DA-D32-R06] – Updated Ownership, Contact and Use Information. At any time there is a change in ownership, the domain name owner must submit the following information:

- Up-to-date contact and ownership information; and
- A description of how the owner is using the domain name, or, if the domain name is not in use, a statement to that effect. (may also apply to Data Elements charter question)

[DA-D41-R01] – RFC 7481, Section 3.6, Data Integrity, specifies that "If the policy of the server operator requires message integrity for client-server data exchanges, HTTP over TLS MUST be used to protect those exchanges." This provides a *possible* requirement: A registration directory service must be able to provide message integrity for client-server data exchanges using HTTP over TLS. (May also be related to Privacy)

[DA-D45-R01] – Incentives for registrants to input accurate gTLD registration data must be provided. These may include:

[DA-D45-R02] – Building a 'gate' between private data and the public. "Make it harder for criminals to access sensitive data by putting all sensitive data behind a series of 'gates' which are only accessible to authenticated users with permissible purposes. Registrants [should be] able to control their own personal data [and] determine which data they want behind each gate and which data can be publicly displayed to anonymous requestors."

[DA-D45-R03] – Making contact data updates easier and more automatic. "Updating contacts [should be] greatly simplified [by] allowing contact holders to easily update their data and such updates to be automatically applied to every affected domain own by the registrant."

[DA-D45-R04] – Mechanisms to detect invalid gTLD registration data must be provided. These may include:

[DA-D45-R05] – Validators [to] validate the contact data and give an unique contact ID to contact data which registries or registrars can use obtain [validated] data. "Validators would specialize in collecting, validating, and storing contact data (postal address, email address, phone, fax, SMS numbers, etc.) which shall be made available by the [gTLD registration directory service] only to authorized requestors."

[DA-D45-R06] – Official proof validation [should be] optional to registrants. "The EWG did not propose that identity validation be required, or that contacts be forced to show government IDs or any other proof of identity when creating a contact. In fact, [the EWG's] final report supports use of contacts created by accredited privacy and proxy services, so that registrants would still have the option of not entering their own contact data, instead designating a third party willing to serve as a contact for that domain name."

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.

Data Elements (DE)

The following *possible* requirements address the charter question on Data Elements (DE):
What data should be collected, stored, and disclosed?

[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

Data Element Reqs	Data Element Design	Data Element Guidance on
- Data Collection Needs - Data Access Needs - Guiding Principles	- RR/Ry Data Elements - Registrant Data Elements - PBC Data Elements - Update Process	- EPP/RDAP Mapping Needs - WHOIS Data Migration Needs

[DE-D01-R01] – The [gTLD registration directory service] must accommodate purpose-driven disclosure of data elements.

[DE-D01-R02] – Not all [gTLD registration] data collected is to be public; disclosure must depend upon Requestor and Purpose.

[DE-D01-R03] – Public access to an identified minimum data set must be made available [by the gTLD registration directory service], including contact data published expressly to facilitate communication for this purpose.

[DE-D01-R04] – Data Elements determined to be more sensitive (after conducting the risk & impact assessment) must be protected by gated access, based upon:

- Identification of a permissible purpose,
- Disclosure of requestor/purpose, and
- Auditing/Compliance to ensure that gated access is not abused.

[DE-D01-R05] – Only the data elements permissible for the declared purpose must be disclosed (i.e., returned in responses or searched by Reverse and WhoWas queries).

[DE-D01-R06] – The only [gTLD registration] data elements that must be collected are those with at least one permissible purpose.

[DE-D01-R07] – Each [gTLD registration] data element must be associated with a set of permissible purposes.

[DE-D01-R08] – An initial set of acceptable uses, permissible purposes, and data element needs are identified [by *possible* requirements for Users/Purposes.]

[DE-D01-R09] – Each permissible purpose must be associated with clearly-defined data element access and use policies.

[DE-D01-R10] – An on-going review process must be defined to consider proposed new purposes and periodically update permissible purposes to reflect approved additions, mapping them to existing data elements.

[DE-D01-R11] – A Policy Definition process must be defined to consider proposed new data elements and, when necessary, update defined data elements, mapping them to existing permissible purposes.

[DE-D01-R12] – The list of minimum data elements to be collected, stored and disclosed must be based on known [permissible purpose] use cases and a risk assessment.

[DE-D01-R13] – In support of the overarching legal principles (see Privacy Question), Registrars and Validators should afford domain name Registrants and purpose-based contacts the opportunity, at the time of data collection, to consent to the use of their data for pre-disclosed permissible purposes, in accordance with the data protection laws of their jurisdiction. In formulating the policy, this principle must be addressed in the broader context of these overarching legal principles.

[DE-D01-R14] – To meet basic domain control needs, it must be mandatory for Registries and Registrars to collect and Registrants to provide the following data elements when a domain name is registered:

a. Domain Name
b. DNS Servers
c. Registrant Name
d. Registrant Type

Indicates the kind of entity identified by Registrant Name, for use in applying registration data requirements (e.g., undeclared, privacy/proxy provider, legal person, natural person – further described on pp 42-43)

e. Registrant Contact ID
   A unique ID assigned to each Registrant Contact [Name+Address] during validation
f. Registrant Postal Address
   Includes Street, City, State/Province, Postal Code, Country (as applicable)
g. Registrant Email Address
h. Registrant Phone
   Includes the following data elements: Number, Extension (when applicable)

[DE-D01-R15] – To improve both Registrant privacy and contactability, Registrars must collect and Registrants must provide purpose-based contacts for every registered domain name.

[DE-D01-R16] – Registrants may optionally designate Privacy/Proxy-supplied contacts or authorized third party contacts for specified permissible purposes.

[DE-D01-R17] – To meet the communication needs associated with each permissible purpose, contacts created through a Validator and subsequently associated with a domain name must satisfy minimum mandatory data element requirements.

[DE-D01-R18] – If a Registrant does not designate a contact for each mandatory permissible purpose, the Registrant's own contact data must be used by default. (Note that the Registrant can avoid this by using an accredited Privacy/Proxy service, or by designating other contacts.

[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-D01-R20] – To maximize Internet stability, the following mandatory data elements must be provided by Registries and Registrars:

a. Registration Status
b. Client Status (Set by Registrar)
c. Server Status (Set by Registry)
d. Registrar
e. Registrar Jurisdiction
f. Registry Jurisdiction
g. Registration Agreement Language
h. Creation Date
i. Registrar Expiration Date
j. Updated Date
k. Registrar URL
l. Registrar IANA Number

m. Registrar Abuse Contact Phone Number
n. Registrar Abuse Contact Email Address
o. URL of Internic Complaint Site

[DE-D01-R21] – For TLD-specific data elements, the TLD Registry must establish and publish a data collection policy (consistent with these over-arching principles) and be responsible for any validation of those TLD-specific data elements.

[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].

[DE-D01-R23] To maximize Registrant privacy, Registrant-supplied data must be gated by default, except where there is a compelling need for public access that exceeds resulting risk. Registrants can opt into making any gated Registrant-supplied data public with informed consent.

[DE-D01-R24] – To maximize Internet stability, all Registry or Registrar-supplied registration data must be always public, except where doing so results in unacceptable risk. Registrants can opt into making any public Registry/Registrar-supplied data gated, except as noted below to enable basic domain control.

[DE-D01-R25] – To maximize reachability, all purpose-based contacts must be public by default. Contact Holders can opt into making any contact data element gated, except [for data elements] required to satisfy the designated purpose.

[DE-D01-R26] – To meet basic domain control needs, the following Registrant-supplied data, which is mandatory to collect and low-risk to disclose, must be included in the minimum public data set:

a. Domain Name
b. DNS Servers
c. Registrant Type
d. Registrant Contact ID
e. Registrant Email Address
f. Tech Contact ID
g. Admin Contact ID
h. Legal Contact ID
i. Abuse Contact ID
j. Privacy/Proxy Provider Contact ID
(mandatory only if Registrant Type = Privacy/Proxy Provider)
k. Business Contact ID
(mandatory only if Registrant Type = Legal Person)

[DE-D01-R27] – To balance simplicity and reachability, if a Registrant does not supply a mandatory purpose-based contact, the Registrant must be informed that [Registrant data elements] will be used [for that purpose]. The Registrant can avoid this disclosure by specifying one or more third party contacts or by using an accredited Privacy/Proxy service.

[DE-D01-R28] – For TLD-specific data elements, the TLD Registry must establish and publish a data disclosure policy (consistent with these over-arching principles) and be responsible for identifying permissible purposes for any gated TLD-specific data elements.

[**DE-D01-R29]** – [gTLD registration directory services] must be expandable in the future to support "multiple contacts specified for each type of purpose-based contact, allowing direct contact with specific individuals with critical responsibilities."

[DE-D01-R30] – All purpose-based contacts "must be aware of and agree to fulfill the designated role(s) for each registered domain name." (p.39)

[DE-D01-R31] – Each contact's approval must be obtainable in a scalable, real-time or near real-time manner to avoid delaying domain name registrations or domain name updates.

[DE-D01-R32] – Policies and processes must prevent unauthorized use of contact data.

[DE-D01-R33] – Either the designated contact or the Registrant must be able to rescind approval at a later time.

[DE-D01-R34] – Registrants must be able to easily designate themselves as contacts for their domain names without external/third party approval.

[DE-D01-R35] – Contact management must be feasible separately from domain management, allowing contact portability and accountability separate from domain names and controlled by the actual individuals or entities listed under such contacts.

[DE-D01-R36] – Contacts must be managed using Validators who manage contact databases, implement validation regimes, and maintain information on the level of validity for the contact and its data elements (accessible through the [gTLD registration directory service]).

[DE-D01-R37] – Domain registrations may be associated with Contact IDs designated by their Registrants and approved by such designated contacts for various purposes associated with a domain name.

[DE-D01-R38] – Such contacts must contain valid mandatory data elements. Policies and oversight will be needed to manage these processes to ensure that Contact IDs are not used without contact's authorization and meet minimum standards.

[DE-D01-R39] – Change management and authorization of use of contact information is controlled by the Contact Holder and affects all domains associated to a contact. Processes and policies to ensure accurate, authentic, and timely implementation of desired changes without burdening contacts or Registrants must be developed to support this new paradigm.

[DE-D01-R40] – Each individual block of contact data must have a Contact ID which uniquely identifies both the Validator and the Contact Holder to enable retrieval and update of associated contact data. This Contact ID must be published in any public display of [registration] data.

[DE-D02-R01] – "Internationalization MUST be supported by default, not called out separately. The focus should be on Recommendation 2 from the IRD-WG final report."

[DE-D06-R01] – From 3.2.1: As part of its registration of Registered Names in a gTLD, Registrar shall submit to, or shall place in the Registry Database operated by, the Registry Operator for the gTLD the following data elements:

- The name of the Registered Name being registered;
- The IP addresses of the primary name server and secondary name server(s) for the Registered Name;
- The corresponding names of those name servers;
- Unless automatically generated by the registry system, the identity of the Registrar;
- Unless automatically generated by the registry system, the expiration date of the registration; and
- Any other data the Registry Operator requires be submitted to it.

[DE-D06-R02] – The agreement between the Registry Operator of a gTLD and Registrar may, if approved by ICANN in writing, state alternative required data elements applicable to that gTLD, in which event, the alternative required data elements shall replace and supersede RAA Subsections 3.2.1.1 through 3.2.1.6 stated above for all purposes under this Agreement but only with respect to that particular gTLD.

[DE-D06-R03] – From 3.3.1: At its expense, Registrar shall provide an interactive web page and, with respect to any gTLD operating a "thin" registry, a port 43 Whois [or gTLD registration directory] service (each accessible via both IPv4 and IPv6) providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar in any gTLD. Until otherwise specified by a Consensus Policy, such data shall consist of the following elements as contained in Registrar's database:

- The name of the Registered Name;
- The names of the primary name server and secondary name server(s) for the Registered Name;
- The identity of Registrar (which may be provided through Registrar's website);
- The original creation date of the registration;
- The expiration date of the registration;
- The name and postal address of the Registered Name Holder;
- The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and
- The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.

[DE-D06-R04] – The agreement between the Registry Operator of a gTLD and Registrar may, if approved by ICANN in writing, state alternative required data elements applicable to that gTLD, in which event, the alternative required data elements shall replace and supersede RAA Subsections 3.3.1.1 through 3.3.1.8 stated above for all purposes under this Agreement but only with respect to that particular gTLD.

[DE-D06-R05] – From 3.4.1: For each Registered Name sponsored by Registrar within a gTLD, Registrar shall collect and securely maintain, in its own electronic database, as updated from time to time:

- The data specified in the Data Retention Specification attached hereto for the period specified therein;

- The data elements listed in RAA Subsections 3.3.1.1 through 3.3.1.8;
- The name and (where available) postal address, e-mail address, voice telephone number, and fax number of the billing contact;
- Any other Registry Data that Registrar has submitted to the Registry Operator or placed in the Registry Database under Subsection RAA 3.2; and
- The name, postal address, e-mail address, and voice telephone number provided by the customer of any privacy service or licensee of any proxy registration service, in each case, offered or made available by Registrar or its Affiliates in connection with each registration. Effective on the date that ICANN fully implements a Proxy Accreditation Program established in accordance with RAA Section 3.14, the obligations under this Section 3.4.1.5 will cease to apply as to any specific category of data (such as postal address) that is expressly required to be retained by another party in accordance with such Proxy Accreditation Program.

[DE-D06-R06] – From 3.4.2: During the Term of this [Registrar Accreditation] Agreement and for two (2) years thereafter, Registrar (itself or by its agent(s)) shall maintain the following records relating to its dealings with the Registry Operator(s) and Registered Name Holders:

- In electronic form, the submission date and time, and the content, of all registration data (including updates) submitted in electronic form to the Registry Operator(s);
- In electronic, paper, or microfilm form, all written communications constituting registration applications, confirmations, modifications, or terminations and related correspondence with Registered Name Holders, including registration contracts; and
- In electronic form, records of the accounts of all Registered Name Holders with Registrar.

[DE-D06-R07] – From 3.4.3: During the Term of this [Registrar Accreditation] Agreement and for two (2) years thereafter, Registrar shall make the data, information and records specified in this Section 3.4 available for inspection and copying by ICANN upon reasonable notice. In addition, upon reasonable notice and request from ICANN, Registrar shall deliver copies of such data, information and records to ICANN in respect to limited transactions or circumstances that may be the subject of a compliance-related inquiry; provided, however, that such obligation shall not apply to requests for copies of the Registrar's entire database or transaction history. Such copies are to be provided at Registrar's expense. In responding to ICANN's request for delivery of electronic data, information and records, Registrar may submit such information in a format reasonably convenient to Registrar and acceptable to ICANN so as to minimize disruption to the Registrar's business. In the event Registrar believes that the provision of any such data, information or records to ICANN would violate applicable law or any legal proceedings, ICANN and Registrar agree to discuss in good faith whether appropriate limitations, protections, or alternative solutions can be identified to allow the production of such data, information or records in complete or redacted form, as appropriate. ICANN shall not disclose the content of such data, information or records except as expressly required by applicable law, any legal proceeding or Specification or Policy.

[DE-D06-R08] – From RAA WHOIS Spec 1.4: For a Domain Name Data Query "whois – h whois.example-registrar.tld EXAMPLE.TLD" the format of responses shall contain all the elements and follow a semi-free text format outline below. Additional data elements can be added at the end of the text format outlined below. The data element may, at the option of Registrar, be followed by a blank line and a legal disclaimer specifying the rights of Registrar, and of the user querying the database (provided that any such legal disclaimer must be preceded by such blank line).

Domain Name: EXAMPLE.TLD
Registry Domain ID: D1234567-TLD
Registrar WHOIS Server: whois.example-registrar.tld
Registrar URL: http://www.example-registrar.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Registrar Registration Expiration Date: 2010-10-08T00:44:59Z
Registrar: EXAMPLE REGISTRAR LLC
Registrar IANA ID: 5555555
Registrar Abuse Contact Email: email at registrar.tld
Registrar Abuse Contact Phone: +1.1235551234
Reseller: EXAMPLE RESELLER1
Domain Status: clientDeleteProhibited2
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Registry Registrant ID: 5372808-ERL3
Registrant Name: EXAMPLE REGISTRANT4
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP5
Registrant Postal Code: A1A1A16
Registrant Country: AA
Registrant Phone: +1.5555551212
Registrant Phone Ext: 12347
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL at EXAMPLE.TLD
Registry Admin ID: 5372809-ERL8
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: AA
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext: 1234
Admin Email: EMAIL at EXAMPLE.TLD
Registry Tech ID: 5372811-ERL9
Tech Name: EXAMPLE REGISTRANT TECHNICAL
Tech Organization: EXAMPLE REGISTRANT LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: AA

Tech Phone: +1.1235551234
Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL at EXAMPLE.TLD
Name Server: NS01.EXAMPLE-REGISTRAR.TLD10
Name Server: NS02.EXAMPLE-REGISTRAR.TLD
DNSSEC: signedDelegation
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2009-05-29T20:15:00Z <<<

[DE-D06-R09] – From RAA WHOIS Spec 1.5: The format of the following data fields: domain status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers, email addresses, date and times must conform to the mappings specified in EPP RFCs 5730-5734 (or its successors), and IPv6 addresses format should conform to RFC 5952 (or its successor), so that the display of this information (or values returned in… responses) can be uniformly processed and understood.

[DE-D06-R10] – From RAA Data Retention Spec: Registrar shall collect the following information from registrants at the time of registration of a domain name (a "Registration") and shall maintain that information for the duration of Registrar's sponsorship of the Registration and for a period of two additional years thereafter:

- First and last name or full legal name of registrant;
- First and last name or, in the event registrant is a legal person, the title of the registrant's administrative contact, technical contact, and billing contact;
- Postal address of registrant, administrative contact, technical contact, and billing contact;
- Email address of registrant, administrative contact, technical contact, and billing contact;
- Telephone contact for registrant, administrative contact, technical contact, and billing contact;
- WHOIS [or gTLD registration directory service] information, as set forth in the [above] Specification;
- Types of domain name services purchased for use in connection with the Registration; and
- To the extent collected by Registrar, "card on file," current period third party transaction number, or other recurring payment data.

[DE-D06-R11] – Registrar shall collect the following information and maintain that information for no less than one hundred and eighty (180) days following the relevant interaction:

- Information regarding the means and source of payment reasonably necessary for the Registrar to process the Registration transaction, or a transaction number provided by a third party payment processor;

- Log files, billing records and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other records containing communications source and destination information, including, depending on the method of transmission and without limitation: (1) Source IP address, HTTP headers, (2) the telephone, text, or fax number; and (3) email address, Skype handle, or instant messaging identifier,

associated with communications between Registrar and the registrant about the Registration; and

- Log files and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration.

[DE-D07-R01] – From Spec 4, Section 1.4: Requires that registries provide registrar information and contact details as part of a registrar query on the [gTLD registration directory service], as well as registrar information as part of the name server [gTLD registration directory service] query. "The fields specified below set forth the minimum output requirements. Registry Operators may output data fields in addition to those specified below, subject to approval by ICANN, which approval shall not be unreasonably withheld."

[DE-D07-R02] – From Spec 4, Section 1.6: "Registrar Data [must include]

- Registrar Name
- Registrar Postal Address
- Registrar Phone Number
- Registrar Email Address
- WHOIS Server
- Referral URL
- Admin Contact Information (phone number and email)
- Technical Contact Information (phone number, email)"

[DE-D07-R03] – From Spec 4, Section 1.7: "Name Server Data [must include]

- Server Name
- IP Address (1 or more, IPv4 and/or IPv6)
- Registrar Name
- Registrar WHOIS Server
- Referral URL"

[DE-D07-R04] – From Specification 4, Section 1.8: "The format of the following data fields: domain status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers (the extension will be provided as a separate field as shown above), email addresses, date and times should conform to the mappings specified in EPP RFCs 5730-5734 so that the display of this information (or values return in WHOIS responses) can be uniformly processed and understood."

[DE-D07-R05] – From Specification 4, Section 1.9: "In order to be compatible with ICANN's common interface for WHOIS (interNIC), [gTLD registration directory service] output shall be in the format outlined above"

[DE-D08-R01]—The "designated role" for each purpose-based contact must be clearly defined and communicated to registrants and to persons/entities designated as contacts, as well as to requestors. (Related to **[DE-D01-R30]**)

[DE-D09-R01] – In Recommendations 12-16, the WHOIS RT recommends that gTLD registration directory services support Internationalization of [registration] data, and the consistent handling of non-ASCII text in both the records and the display of the domain name itself.

[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-D12-R02] – The [gTLD registration directory service] should collect and display uniform sets of data regardless of the registry involved. (sec. 5.2)

[DE-D13-R01] – Based on the review of ICANN's procedure for handling WHOIS conflicts with privacy law, the following Data Element-related requirements from past accreditation agreements are unchanged: Registrars must notify registrants of: 3) which data are obligatory, and that 5) Data collection may only be conducted with the consent of the registrant.

[DE-D14-R01] – According to the 2013 RAA Data Retention Waiver and Discussion Document, registrars should have access to standard data elements, including first and last name of the registrant, Technical contact and billing contact, Postal address, Email address, Telephone number, Types of domain name services purchased, information on the means and source of payment, for billing and billing disputes.

[DE-D15-R01] – ICANN's UDRP requires registrant information (Name and Company Name) taken from [gTLD registration directory services] for the disputed domain name. Specifically, "To demonstrate "legitimate interests in a Domain Name in Responding UDRP to a Complaint... (ii) Respondent (as an individual, business, or other organization) have been [commonly known] by the domain name, even if acquired no trademark or service mark rights;" (UDRP policy, Paragraph 4(c)). For proving legitimate rights in a Domain Name, mostly under Exparte matters, the Complainant and Panelist in a UDRP matter analyze WHOIS information mainly to determine whether the Respondent (Owner of Disputed Domain) is commonly known by the disputed domain name. The Complainant will require access to WHOIS even before filing of the Complaint, to determine whether to go for UDRP/legal action or not.

[DE-D15-R02] – According to ICANN's UDRP, the UDRP Service provider, "when forwarding a complaint, including any annexes, electronically to the Respondent, it has to employ reasonably available means calculated to achieve actual notice to the Respondent. Achieving actual notice, or employing the following measures to do so, shall discharge this responsibility: (i) sending [Written Notice] of the complaint to all postal mail and facsimile addresses shown in the domain name's registration data in [Registrar's Whois database] for the registered domain name holder, the technical contact, and the administrative contact and supplied by Registrar to the Provider for the registration's billing contact; and (ii) sending the complaint, including any annexes, in electronic form by email to the [email addresses] for those technical, administrative, and billing contacts;" (Rules for Uniform Domain Name Dispute Resolution Policy, Paragraph 2) UDRP Service Providers therefore require these WHOIS details for service of notice.

[DE-D15-R03] – According to ICANN's UDRP, in a UDRP Complaint, "the Complainant [needs] to provide the name of the Respondent (domain name holder) and all information (including any postal and

email addresses and telephone and telefax numbers) known to Complainant regarding how to contact Respondent or any representative of Respondent and Identify the Registrar with whom the Domain is registered at the time of the Complaint." (Rules for Uniform Domain Name Dispute Resolution Policy, Paragraph 3) The Complainant is required to provide contact information (i.e., Name, Address, Email, Telephone, Telefax and Domain Registrar) as a part of the UDRP Complaint and the most important source to know such information is WHOIS of a Domain Name, as the Respondent (i.e., owner of a disputed domain name) may be from any part of the world.

[DE-D16-R01] – ICANN's URS policy requires registrant information taken from [gTLD registration directory services] for the disputed domain name. Specifically, "the contents of Complaint under URS, [should] contain:

(i) Name of Registrant (i.e. relevant information available from WHOIS) and WHOIS listed available contact information for the relevant domain name(s). (URS Procedure Para 1.2.3)

(ii) The specific domain name(s) that are the subject of the Complaint. For each domain name, the Complainant [shall include] a copy of the currently available WHOIS information." (URS Procedure Para 1.2.4)

[DE-D16-R02] – ICANN's URS policy paragraph 4 provides for service of Notice by the URS Provider to the Domain Registrant, through email, fax and postal mail obtained from WHOIS. Specifically, "after the Notice of Lock from the Registry Operator, within 24 hours, the URS Provider [shall] notify the Registrant of the Complaint, sending a hard copy of the Notice of Complaint to the addresses listed in the WHOIS contact information." (URS Policy Para 4.2) "The said Notice of Complaint to the Registrant [shall] be sent through email, fax (where available) and postal mail. The Complaint and accompanying exhibits, if any, shall be served electronically." (URS Procedure Para 4.3)

[DE-D16-R03] – According to ICANN's URS policy, when the Domain Registrant does not respond within 14 days period, it is considered as Default and the URS Provider will notify the Registry Operator accordingly. Specifically, "in case of Default, the URS Provider [shall] provide Notice of Default via email to the Complainant and Registrant, and via mail and fax to Registrant. During the Default period, the Registrant will be prohibited from changing content found on the site to argue that it is now a legitimate use and will also be prohibited from changing the WHOIS information." (URS Procedure Para 6.2)

[DE-D16-R04] – According to ICANN's URS policy, "after URS Determination, the Registry Operator shall suspend the domain name... The WHOIS for the domain name shall continue to display all of the information of the original Registrant except for the redirection of the name servers. In addition, the Registry Operator [shall cause] the WHOIS to reflect that the domain name will not be able to be transferred, deleted or modified for the life of the registration." (URS Procedure Para 10.2) This restricts Domain Status and [the display of data through gTLD registration directory services] to reflect the above data elements. Data for this purpose could be made available through a gated [gTLD registration directory service] to the Registry Operator.

[DE-D16-R05] – According to ICANN's URS rules, "Mutual Jurisdiction has been defined to mean a court jurisdiction at the location of [either] (a) the principal office of the Registrar or (b) the domain name holder's address as shown for the registration of the domain name in Registrar's WHOIS database at the time the complaint is submitted to the Provider." (URS Rules, Para 1 Definitions) The location of the Domain Holder [obtained from gTLD registration directory services] is required to determine one of the Mutual Jurisdictions.

[DE-D16-R06] – According to ICANN's URS rules, "The Notice of Complaint to be sent to all email, postal mail and facsimile addresses shown in the domain name's registration data in the WHOIS database for the registered domain name holder, the technical contact, and the administrative contact, as well as to any email addresses for the Respondent provided by the Complainant." (URS Rules, Para 2 (i)) Service of notice upon the Domain Holder requires Email, Postal mail and Facsimile Addresses as shown in [gTLD registration directory services] Registrant, Technical and Administrative contacts.

[DE-D16-R07] – According to ICANN's URS rules, "The Complaint, including any annexes.... [shall] provide the name of the Respondent and all other relevant contact information [from] the WHOIS record as well as all information known to Complainant regarding URS Rules, Para 3 (b)(iii)." This requires the Complaint to include registrant information taken from WHOIS for the disputed domain name.

[DE-D16-R08] – According to ICANN's URS rules, "The Notice of Complaint to the Respondent [shall] be transmitted in English and shall be translated by the Provider into the predominant language used in the registrant's country or territory, as determined by the country(ies) listed in the WHOIS record when the Complaint is filed." (URS Rules, Para 4(b)). Service of Notice by the URS Provider to the Domain Registrant therefore requires WHOIS to determine the country of the Registrant.

[DE-D16-R09] – According to ICANN's URS rules, when the Domain Registrant does not respond within 14 days period, it is considered as Default under the URS Policy and the URS Provider will notify the Registry Operator accordingly. Specifically, "In case of Default by Registrant, the Provider shall notify the Registry Operator that the Registrant is prohibited from changing content found on the site and that the Registrant is prohibited from changing the WHOIS information." (URS Rules, Para 12)

[DE-D18-R01] – Based on the WHOIS Inter-Registrar Transfer Policy, Section I.A.2.1.2: "In the event that the Gaining Registrar relies on a physical process to obtain this authorization, a paper copy of the FOA will suffice insofar as it has been signed by the Transfer Contact and further that it is accompanied by a physical copy of the Registrar of Record's WHOIS output for the domain name in question"

[DE-D18-R02] – Based on the WHOIS Inter-Registrar Transfer Policy, Section I.A.2.1.3.1: "In the event that the Gaining Registrar relies on an electronic process to obtain this authorization the acceptable forms of identity would include:

(a) Electronic signature in conformance with national legislation, in the location of the Gaining Registrar (if such legislation exists).

(b) Consent from an individual or entity that has an email address matching the Transfer Contact email address."

[DE-D18-R03] – Based on the WHOIS Inter-Registrar Transfer Policy, Section I.A.3.6: "In the event that a Transfer Contact listed in the WHOIS has not confirmed their request to transfer with the Registrar of Record and the Registrar of Record has not explicitly denied the transfer request, the default action will be that the Registrar of Record must allow the transfer to proceed."

[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)

[DE-D20-R01] – Based on the Article 29 WP's statement on the data protection impact of the revision of the ICANN RAA (2013-2014) and correspondence (including the back and forth with ICANN), there should be a specified period of time for [gTLD registration] data retention passed the contract period that is consistent with applicable law.

[DE-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* requirement: There should be a differentiation for data collection/use between legal and natural persons when registering domain names.

[DE-D22-R01] – In sum, from the Article 29 WP's Opinion 2/2003, we could draw out the following *possible* requirement: Data collected should be relevant (and not excessive) for defined purpose. Specifically, the WP states:

- "... data should be relevant and not excessive for the specific purpose."
- "... the processing of personal data in reverse directories or multi-criteria searching services without unambiguous and informed consent by the individual is unfair and unlawful."

[DE-D26-R01] – According to the Directive (12), whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

[DE-D26-R02] – According to the Directive (13), whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters

[DE-D26-R03] – According to the Directive (14), whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

[DE-D26-R04] – According to the Directive (15), whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be

contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

[DE-D26-R05] – 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;

[DE-D26-R06] – According to the Directive (e33), 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;

[DE-D26-R07] – According to the Directive (47), whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

[DE-D26-R08] – According to the Directive (57), whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited; (58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

[DE-D26-R09] – As used in the Directive, (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

[DE-D26-R10] – 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 [above] may not be lifted by the data subject's giving his consent;

[DE-D26-R11] – According to the Directive, 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
- the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

[DE-D26-R12] – According to the Directive Article 10, Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected 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 for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- 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 collected, to guarantee fair processing in respect of the data subject.

[DE-D29-R01] – Each data controller must respect the following rules as set out in the Directive:

[DE-D29-R02] – Personal Data must be processed legally and fairly;

[DE-D29-R03] – It must be collected for explicit and legitimate purposes and used accordingly;

[DE-D29-R04] – It must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed.

[DE-D30-R01] – 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

[DE-D30-R02] – **Proportionality:** The Privacy Shield (Annex II, II.5.a) states that the information must be limited to what is relevant for the processing. The WP29 would prefer if this wording is amended in the final adequacy decision, since the mere fact that the data shall be relevant to the processing is

not sufficient to make the processing proportionate. In order to meet the proportionality principle, the processing should be limited to the data that are necessary for the processing at stake.

[DE-D30-R03] – 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

[DE-D30-R04] – 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 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

[DE-D30-R05] – Privacy Shield documents make use of terminology that is not consistent with the vocabulary generally used in the EU when dealing with data protection. This is not necessarily a problem, as long as it is clear what the corresponding terminology under EU law (and under U.S. law) would be. The WP29 regrets to note however this is not the case, including in the draft adequacy decision. For example, the word 'access' is used in chapter 3 of the draft adequacy decision in a sense that implies the collection of personal data, instead of allowing someone to see data that is already collected. Access by companies to the data and the individuals' right of access are two separate notions that should not be confused. pg. 13

[DE-D30-R06] – The WP29 would like to recall that any processing (including collection and transfer) of sensitive data subject to EU law has to be made on legitimate grounds according to article 8 of the Directive. The Privacy Shield cannot be interpreted as offering alternative grounds for such processing pg. 14

[DE-D30-R07] – important new notions like the right to data portability and additional obligations on data controllers, including the need to carry out data protection impact assessments and to comply with the principles of privacy by design and privacy by default, have not been included in the Privacy Shield. The WP29 would therefore like to suggest that the Privacy Shield, as with any existing adequacy decisions, is reviewed shortly after the GDPR enters into application pg. 15

[DE-D30-R08] – The individual must receive both confirmation that data are being processed regarding him and communication of the data processed. pg15

[DE-D30-R09] – 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. pg17

[DE-D30-R10] – 2.2.9 Publicly available information states: The exception to the right of access in the case of publicly available information and public record information (Annex II, III.15.d and e) raises

concerns to the extent that an individual, when exercising his/her right of access, is interested to know whether a particular controller processes data about himself/herself, and also to know what data is being processed, in order to be able to control the processing of his/her data. The WP29 has repeatedly stated that according to EU law data subjects always have the right to access their data, and, where necessary, to require rectification or erasure of the data if the data have not been processed lawfully or if they are incomplete or inaccurate, regardless of whether or not the personal data have been published.37 If the individual's request for access is rejected on the grounds that the data were obtained from publicly available sources or public records, the individual would lose the ability to control the accuracy of the data and to control whether the data were lawfully made public in the first place.pg.38

[DE-D30-R11] – 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

[DE-D32-R01] – The specifications below are recommended requirements for dispute resolution and other procedures related to trademarks. These include:

[DE-D32-R02] – Minimum Application Requirements: Sufficient owner and contact information (e.g., names, mail address for service of process, e-mail address, telephone and fax numbers, etc.) to enable an interested party to contact either the owner/applicant or its designated representative;

[DE-D32-R03] – Minimum Application Requirements: Certification statement by the applicant that:

- It is entitled to register the domain name for which it is applying and knows of no entity with superior rights in the domain name; and
- It intends to use the domain name.

[DE-D32-R04] – Searchable Database Requirements. Utilizing a simple, easy-to-use, standardized search interface that features multiple field or string searching and the retrieval of similar names, the following information must be included in all registry databases, and available to anyone with access to the Internet:

- Up-to-date ownership and contact information;
- Up-to-date and historical chain of title information for the domain name;
- A mail address for service of process;
- The date of the domain name registration; and
- The date an objection to registration of the domain name was filed.

[DE-D40-R01] – RFC 7480, Section 4.3, specifies "In accordance with [RFC5226], the IANA policy for assigning new values, shall be Specification Required: values and their meanings must be documented in an RFC or in some other permanent and readily available reference, in sufficient detail that interoperability between independent implementations is possible. This might apply to a registration directory service that implements RDAP.

[DE-D43-R01] – The EPP RFCs (5730, 5731, 5732, 5733) make no assumptions about the existence of a registration directory service. They do, however, describe the syntax of data elements that are included when objects are registered. As such, *possible* requirements may be derived from EPP RFCs for data elements that might be collected for registration directory service publication. In cases where data elements are repeated in the RFCs, the following *possible* requirements only identify the first use in each document.

[DE-D43-R02] – RFC 5730: Extensible Provisioning Protocol (EPP) a framework specification that describes a method for the publication of data collection and disclosure policies. Section 2.4 provides this *possible* requirement: Registration directory service and EPP data collection and disclosure policies must be consistent.

[DE-D43-R03] – RFC 5731: Extensible Provisioning Protocol (EPP) Domain Name Mapping, Section 2.1, describes the [required] syntax of domain names. Section 2.2 describes the [required] syntax of contact and client identifiers. Section 2.3 describes [required] domain status values. Section 2.4 describes the [required] syntax of date-time values. Section 3.2.1 describes the EPP <create> Command, including a mandatory domain name element and optional registration period, name server, registrant identifier, and contact identifier data elements. Section 3.2.3, EPP <renew> Command, describes an expiration date element.

These sections provide this *possible* requirement: A registration directory service must conform to the data element syntax specifications for domain names, EPP contact and client identifiers, EPP domain status values, and date-time values as specified in RFC 5731.

[DE-D43-R04] – RFC 5732: Extensible Provisioning Protocol (EPP) Host Mapping, Section 2.1, describes the [required] syntax of host (name servers in this context) names. Section 2.2 describes the [required] syntax of client identifiers. Section 2.3 describes [required] host status values. Section 2.4 describes the [required] syntax of date-time values. Section 2.5 describes the [required] syntax of IPv4 and IPv6 addresses.

These sections provide this *possible* requirement: A registration directory service must conform to the data element syntax specifications for host (name server) names, EPP client identifiers, EPP host status values, date-time values, and IPv4 and IPv6 addresses as specified in RFC 5732.

[DE-D43-R05] – RFC 5733: Extensible Provisioning Protocol (EPP) Contact Mapping, Section 2.1, describes the [required] syntax of contact and client identifiers. Section 2.2 describes [required] contact status values. Section 2.3 describes the [required] syntax of individual and organizational names. Section 2.4 describes the [required] syntax of postal addresses. Section 2.5 describes the [required] syntax of telephone numbers. Section 2.6 describes the [required] syntax of email addresses. Section 2.7 describes the [required] syntax of date-time values. Section 2.9 requires for server disclosure of data collection policies (see above). Section 3.2.1, EPP <create> Command, describes contact name elements. It also describes the ability to specify localized forms of address information that can be represented using non-ASCII characters. These sections provide these *possible* requirements:

[DE-D43-R06] – A registration directory service must conform to the data element syntax specifications for EPP contact and client identifiers, EPP contact status values, EPP individual and organizational names, EPP postal addresses, telephone numbers, email addresses, and date-time values as specified in RFC 5733.

[DE-D43-R07] – A registration directory service must have the ability to collect, store, and represent internationalized and localized forms of address information that can be represented using both ASCII and non-ASCII characters.

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.

Privacy (PR)

The following *possible* requirements address the charter question on Privacy (PR):
What steps are needed to protect data and privacy?

[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

Privacy Reqs	Privacy Design	Privacy Guidance on
- Privacy/Proxy Needs	- Overarching DP Policy	- RDS Privacy Policy Needs
- At-Risk Reg Needs	- DP Law Compliance	- Detailed Legal Analysis
- Data Protection Laws	- Privacy/Proxy Policies	- P/P Accreditation Needs
	- Secure Protected Creds	- SPC Provider Criteria

[PR-D01-R01] – ". . . in some jurisdictions, privacy rights extend to legal persons and to entities with respect to free speech and freedom of association." (Next to last paragraph on p.81)

[PR-D01-R02] – As described under Option (2) of the Summary of Data Protection Mechanisms Considered table on p.85 with further description on p.86, a basic ICANN privacy policy for gTLD registration directory services must] be drafted, based on standard best practices for privacy protection, and standard contractual clauses [must] be developed which give effect to this policy throughout the [registration directory services] ecosystem. Standard clauses could be included in all contracts between ICANN and all ecosystem actors engaged in data transfers, ensuring a sufficiently high level of data protection to permit unfettered transfer within this ecosystem.

[PR-D01-R03] – The gTLD registration directory service must comply with a defined "policy using standard contractual clauses that are harmonized with data protection laws to implement the requirements of the policy, and ensure through various audit mechanisms that these privacy protections are enforced through contracts between all ecosystem actors involved in handling personal information." (pp.86-87)

[**PR-D01-R04]** – As described under Options (1) & (2) in the Summary of Data Protection Implementations Considered table on pages 87-88, gTLD registration directory services must protect data elements:

[PR-D01-R05] – Provide for legal compartmentalization by tagging data elements according to the applicable law for the data subject and treating that that data accordingly by applying those law(s) to each specific transfer.

[PR-D01-R06] – Select location(s) for gTLD registration data storage where the applicable national data protection law provides for a high level of protection.

[PR-D01-R07] – Mechanisms must be adopted to facilitate routine legally compliant data collection and transfer between actors within the [gTLD registration directory services] ecosystem.

[PR-D01-R08] – Standard contract clauses that are harmonized with privacy and data protection laws should be codified in a policy and enforced through contracts between all ecosystem actors involved in handling personal information.

[PR-D01-R09] – An information system to apply data protection laws and localization of data storage must be considered as two means of implementing the high level of data protection required. This must be ensured through standard contractual clauses, which flow from a logical privacy policy for the ecosystem.

[PR-D01-R10] – Summary of Law Enforcement Access Options Considered Option (1) on page 89; "In addition, for option (1), it has to be ensured that the legal framework for national law enforcement in jurisdiction(s) where registration data is stored does not override the framework established for the gTLD registration directory service. The geography of data localisation is therefore critically important."

[PR-D01-R11] – Law Enforcement Access Principle 108: "[gTLD registration data] must [be] stored in jurisdiction(s) where law enforcement is globally trusted, regardless of implementation model." (p.90)

[PR-D01-R12] – The following overarching legal principles normally found in data protection law must be considered when drafting policies and implementation processes for gTLD registration directory services:

- Personal data must be:

  [PR-D01-R13] – processed lawfully, fairly and in a transparent manner in relation to the data subject,

  [PR-D01-R14] – collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,

  [PR-D01-R15] – adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed, and

  [PR-D01-R16] – accurate and kept up-to-date as required for the specified purposes.

- Lawful processing, including transfer and disclosure can be – subject to the relevant jurisdiction – based on:

  [PR-D01-R17] – consent of the data subject,

  [PR-D01-R18] – the necessity for the performance of a contract to which the data subject is party, and

  [PR-D01-R19] – the necessity for compliance with a legal obligation to which the controller is subject.

  [PR-D01-R20] – A right of access to information and a right to rectify inaccuracy for the data subject have to be ensured.

[PR-D01-R21] – In addition to the privacy afforded by compliance with data protection laws, the [gTLD registration directory services] ecosystem must accommodate needs for privacy by including:

- An accredited Privacy/Proxy Service for general personal data protection and adherence to local privacy law; and
- An accredited Secure Protected Credentials Service for persons at risk, and in instances where free-speech rights may be denied or speakers persecuted.

[PR-D01-R22] – There must be accreditation for Privacy/Proxy service providers and rules regarding the provision and use of accredited Privacy/Proxy services. *[Note: See PPSAI PDP Final Report for GNSO consensus policy on accreditation of Privacy/Proxy service providers developed after the EWG Report was published.]*

[PR-D01-R23] – Outside of domain names registered via accredited Privacy/Proxy services, all Registrants must assume responsibility for the domain names they register.

[PR-D01-R24] – ICANN must investigate the development of a single, harmonized privacy policy which governs [gTLD registration directory services] activities in a comprehensive manner, as discussed on pp 96-97.

[PR-D01-R25] – ICANN must accredit Privacy and Proxy service Providers. At minimum, the accreditation program must continue the Privacy/Proxy commitments under the 2013 RAA Specification.

[PR-D01-R26] – Entities and natural persons may register domain names using accredited Privacy services that do not disclose the Registrant's contact details except in defined circumstances (e.g., terms of service violation, subpoena).

[PR-D01-R27] – ICANN must require specific terms to be included in the terms of service. The terms of service must include requiring the service provider to endeavor to provide notice in cases of expedited take-downs.

[PR-D01-R28] – Accredited Privacy services must provide the Registrar with accurate and reliable contact details for all mandatory Purpose-Based Contacts, in order to reach the Privacy service provider and entities authorized to resolve technical, administrative, and other issues on behalf of the Registrant.

[PR-D01-R29] – Accredited Privacy services must be obligated to relay emails received by the Registrant's forwarding email address to the Registrant.

[PR-D01-R30] – Entities and natural persons may register domain names using accredited proxy services that register domain names on behalf of the Proxy service customer.

[PR-D01-R31] – Accredited Proxy service providers must provide the Registrar with their own Registrant name and contact details, including a unique forwarding email address to contact the entity authorized to register the domain name on behalf of the Proxy service customer.

[PR-D01-R32] – As the registered name holder, accredited proxy service providers must assume all the usual Registrant responsibilities for that domain name, including provision of accurate and reliable mandatory Purpose-Based Contacts and other registration data.

[PR-D01-R33] – Accredited Proxy services must provide the Registrar with accurate and reliable contact details for all mandatory Purpose-Based Contacts, in order to reach the Proxy service provider and entities authorized to resolve technical, administrative, and other issues on behalf of the Proxy service customer.

[PR-D01-R34] – Accredited Proxy services must be obligated to relay emails received by the Registrant's forwarding email address.

[PR-D01-R35] – Accredited Proxy services must be obligated to respond to reveal requests in a timely manner as outlined in the escalation procedures.

[PR-D01-R36] – The six key functions listed on pages 104-105 must be developed to provide enhanced security to at-risk entities. These functions include:

- A process to establish criteria for at-risk entity eligibility.
- Application forms, attestations, and financial systems to protect identities of at-risk entities.
- An independent review board to evaluate and approve applications.
- Trusted parties willing to relay secure protected credentials.
- Accredited proxy service providers willing to accept secure protected credentials.
- Policies surrounding expedited takedown procedures and other DNS abuse mitigations.

[PR-D01-R37] – "Secure Protected Credentials (must) be developed for limited use and after ensuring entities availing themselves of the service do indeed have legitimate need for anonymity." (1st paragraph on p.106)

[PR-D01-R38] – "Information generated from the actual use of a domain name must be the responsibility of the entities applying for and using secure credential-registered domain names, and it may be important to provide information underscoring this risk." (2nd paragraph on p.106)

[PR-D01-R39] – Individuals and groups who can demonstrate that they would be at risk if identified must be able to anonymously apply for and receive domain names registered using secure credentials, aided by attestors and trusted third parties to provide a shield between at-risk entities and Registrars/Validators.

[PR-D01-R40] – ICANN must facilitate the establishment of an independent trusted review board that will validate claims of at-risk organizations or individuals to approve (and when necessary, revoke)

credentials. Such an organization – referred to herein as a Secure Credential Approver (SCA) -- might develop other services, such as educating users about risks and safe Internet practices.

[PR-D01-R41] – ICANN must facilitate the development or licensing of a Secure Credential Issuer that recognizes SCA approvals and generates corresponding Secure Credentials.

[PR-D01-R42] – The Secure Credential Approver must use issued Secure Credentials to license domain names from accredited Proxy Service Providers in the usual manner. Information of the proxy service provider will appear in the gTLD registration directory service. No data about the at-risk entity using the secure credential-registered domain name would be known to the registration directory service, and some system of anonymous or proxy payment would have to be used.

[PR-D01-R43] – Domain names registered using secure protected credentials must follow regular accredited Privacy/Proxy service provider reveal and take-down procedures. Failure of the Privacy/Proxy customer (i.e., the Secure Credential Approver) to respond in a timely manner, or evidence of DNS abuse, could result in expedited take-down of secure credential-registered domain names.

[PR-D01-R44] – Recognizing that domain names registered using secure protected credentials might be at risk themselves for cyberattack, or that investigation of offences would be difficult, heightened security monitoring of these domain names must be considered to mitigate risk.

[PR-D01-R45] – Policies and processes must be established for secure protected credential application approval and revocation.

[PR-D04-R01] – Any collection of personal data must be both conscious and consenting. Where individuals are aware that they are making data available for public view, it must be made clear the extent of the risk to them and their reputation were this data to be used or misused.

[PR-D04-R02] – The [gTLD registration directory service] must not be used to allow the good name and/or reputation of a citizen to be attacked and/or destroyed. There must be concrete safeguards protecting privacy, and real remedies for violations to privacy, dignity and reputation online which are or were enabled by the [gTLD registration directory service].

[PR-D04-R03] – In the event that the decision is made for the [gTLD registration directory service] to contain personal data, the [gTLD registration directory service] must actively and regularly raise awareness amongst those individuals whose personal data is stored to help them understand what privacy is, what their privacy rights are, and how their privacy may be infringed upon. Information must also be actively provided on how privacy risks can be mitigated or minimised, and on what remedies are available if necessary. It is not sufficient for this information to be communicated solely via electronic means.

[PR-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.

[PR-D06-R01] – From 3.7.7.8: Registrar shall agree that it will take reasonable precautions to protect Personal Data from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

[PR-D09-R01] – In Recommendation 10, the WHOIS RT states that the current use of privacy and proxy services raises questions about whether ICANN is meeting its AoC commitments relating to 'timely, unrestricted and public access' to WHOIS data. To provide enhanced usability for consumers, including the display of full registrant data for all gTLD domain names from one source, the WHOIS RT recommends that registrars disclose their relationship with any proxy/privacy service provider and maintain dedicated abuse points of contact for each provider.

[PR-D09-R02] – The WHOIS RT reported its well-researched finding that there are legitimate reasons for companies, organizations and individuals to seek privacy of WHOIS data. Specifically, "Privacy and proxy services are used to address noncommercial and commercial interests, which many view as legitimate. For example:

- **Individuals** – who prefer not to have their personal data published on the Internet as part of a WHOIS record.
- **Organizations** – as religious, political or ethnic minority, or sharing controversial moral or sexual information; and
- **Companies** – for upcoming mergers, new product or service names, new movie names, or other product launches." pp.13-14

[PR-D12-R01] – The [gTLD registration directory service] should provide additional security measures for data in motion, i.e., when data is transferred, downloaded or replicated, especially in large volumes. (sec. 5.5)

[PR-D13-R01] – The review of ICANN's procedure for handling WHOIS conflicts with privacy law found that requirements that remain unchanged from past accreditation agreements were broadly consistent with data privacy and protection expectations and legal requirements in most jurisdictions, and they have underpinned the successful operation of the Internet's shared registration system for at least the past 15 years.

[PR-D13-R02] – During the negotiation of the 2013 RAA, some registrars expressed concerns that local or national data protection and other privacy laws might make it difficult for them to comply with the new requirements, while law enforcement and intellectual property owners advocated for retention of information in the Data Retention Specification. Accordingly, the 2013 RAA's Data Retention Specification includes a provision concerning waivers to deal with cases where compliance with the data collection and/or retention requirements might be prohibited by applicable law. Indeed, ICANN contracted parties are obligated to abide by any applicable laws.

[PR-D13-R03] – To initiate the Data Retention Waiver process, registrars must present ICANN with an opinion from a law firm or a ruling or guidance from a governmental body of competent jurisdiction that states that collecting or retaining one or more data elements in the manner required by the specification violates applicable law. A general assertion that the data collection and Data Retention Specification requirements are unlawful is not sufficient. Rather, the waiver request must specify the applicable law, the specific allegedly offending data collection and/or retention requirement(s), and the manner in which the collection and/or retention violates the

law. This specificity helps ICANN to determine the appropriate limitations on the scope and duration of data collection and retention requirements when granting the waiver. This will also help ICANN balance the interests of the registrar, governments, and the broader Internet community when considering granting such waivers.

[PR-D13-R04] – The 2013 RAA calls for ICANN and the registrar to discuss data retention waiver requests in good faith in an effort to reach a mutually acceptable resolution. The Data Retention Specification contemplates potential future modifications to the Whois Procedure in section 2: "Until such time as ICANN's Procedure for Handling Whois Conflicts with Privacy Law is modified to include conflicts relating to the requirements of this Specification and if ICANN agrees with Registrar's determination, ICANN's office of general counsel may temporarily or permanently suspend compliance and enforcement of the affected provisions of the Data Retention Specification and grant the waiver request. Prior to granting any exemption, ICANN will post its determination on its website for a period of thirty (30) calendar days." ICANN contemplates that waivers should be tailored to limit the scope and/or duration of data collection and retention as necessary to comply with local law, but will not completely eliminate all requirements for data collection and retention.

[PR-D13-R05] – Because each country may interpret its data privacy requirements differently, ICANN is working through each of the submitted requests to change Whois data retention requirements, country-by-country. The complexity and diversity of national privacy laws has resulted in considerable investments of time and resources by ICANN and registrars alike. In countries with data privacy laws applicable to registrars, ICANN has found that restrictions generally permit the retention of registration data, but only for legitimate purposes, and for a period no longer than is necessary for the purposes for which the data were collected or for which they are further processed. What constitutes a legitimate purpose and how long data can be retained are complicated questions, and the answers may vary from one country to the next, even within the EU. All EU member states are subject to the same data privacy directive, but individual member state's legislation implementing the data privacy directive may differ in significant respects.

[PR-D13-R06] – In all, 15 requests to waive the Data Retention Specification in the 2013 RAA have been submitted by registrars, all from within the European Union. The EU's Article 29 Working Party has also written to ICANN to express its concerns about the legality of the requirements of the 2013 RAA within the EU. ICANN has also received correspondence from the European Data Protection Supervisor urging ICANN to waive the retention period under the 2013 RAA Data Retention Specification to all registrars operating in EU member states.

[PR-D19-R01] – Based on the ICANN Governmental Advisory Committee (GAC) proposed principles, "The GAC recognizes that there are also legitimate concerns about the misuse of WHOIS [registration] data and conflicts with national laws and regulations, in particular applicable privacy and data protection laws" (para 2.2).

[PR-D19-R02] – "gTLD [registration directory] services must comply with applicable national laws and regulations" (para 3.2)

[PR-D19-R03] – "gTLD [registration directory] services should provide (…) data (…) subject to national safeguards for individual's privacy" (para 3.3),

[PR-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* requirement: When considering privacy (e.g., publication of data), there should be a consideration as to whether the registrant is a private domain holders that use domains solely in a non-commercial context, and if so, the data should only be published with explicit, freely given consent. Specifically:

[PR-D21-R02] – "The Article 29 WP's primary concern relates to private domain holders that use domains solely in a non-commercial context."

[PR-D21-R03] – "The Article 29 WP therefore recommends to modify the proposal in such a way that at least for private domain holders that use domains solely in a non-commercial context the name of the domain holder should only be published in the WHOIS service with the explicit, freely given consent of the data subject."

[PR-D21-R04] – "The Article 29 WP sees, in the current situation, actual conflicts between current WHOIS practice and EU data protection and privacy laws, not just potential conflicts as the title of the proposed procedure on ICANN's website states."

[PR-D21-R05] – "As a matter of fact, registrars operating in EU member states under the current ICANN registrar accreditation agreement face a generally present and unresolved conflict between EU data protection legislation and several international rules on the one hand, and current WHOIS practice on the other hand."

[PR-D23-R01] – Article 8 of the European Convention on Human Rights, adopted in 1950, incorporates the right to privacy - i.e. respect for everyone's private and family life, home and correspondence. It prohibits any interference with the right to privacy except if 'in accordance with the law' and 'necessary in a democratic society' in order to satisfy certain types of specifically listed, compelling public interests. p. 7

[PR-D25-R01] – Council of Europe's Treaty 108 on Data Protections is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the trans-frontier flow of personal data. [highlight added]

[PR-D25-R02] – Council of Europe's Treaty 108 on Data Protections, Article 1, Object and purpose, states: "The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")."

[PR-D25-R03] – Council of Europe's Treaty 108 on Data Protections, Article 5, Quality of data, restricts the collection of data under its privacy laws to only that data that is:

a. obtained and processed fairly and lawfully;
b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored." See also **[UP-D25-R03]**

[PR-D25-R04] – Council of Europe's Treaty 108 on Data Protections, Article 6, Special categories of data, restricts the collection of data under its privacy laws to only that data that is: "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."

[PR-D26-R01] – According to the Directive, 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;

[PR-D26-R02] – According to the Directive (10), whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

[PR-D26-R03] – According to the Directive (12), whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

[PR-D26-R04] – According to the Directive (26), whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

[PR-D26-R05] – According to the Directive (30), whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether

carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

[PR-D26-R06] – 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;

[PR-D26-R07] – 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;

[PR-D26-R08] – According to the Directive (68), whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

[PR-D26-R09] – According to the Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

[PR-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."

[PR-D28-R02] – 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." See also **[UP-D28-R03]**

[PR-D28-R03] – Data controllers determine 'the purposes and the means of the processing of personal data'. This applies to both public and private sectors. See also **[UP-D28-R04]**

[PR-D28-R04] – "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.

(note: highlights are in the original) See also **[UP-D28-R05]**

[PR-D30-R01] – The WP29 considers a review must be undertaken shortly after the entry into application of the General Data Protection Regulation, in order to ensure the higher level of data protection offered by the Regulation is followed in the adequacy decision and its annexes. pg. 3

[PR-D30-R02] – The WP29's key objective is to make sure that an essentially equivalent level of protection afforded to individuals is maintained when personal data is processed. pg. 3

[PR-D30-R03] – Although the WP29 does not expect the Privacy Shield to be a mere and exhaustive copy of the EU legal framework it considers that it should contain the substance of the fundamental principles and as a result, ensure an 'essentially equivalent' level of protection. pg.3

[PR-D30-R04] – Because the Privacy Shield will also be used to transfer data outside the US, the WP29 insists that onward transfers from a Privacy Shield entity to third country recipients should provide the same level of protection on all aspects of the Shield (including national security) and should not lead to lower or circumvent EU data protection principles pg. 3

[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

[PR-D30-R06] – 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

[PR-D30-R07] – 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

[PR-D30-R08] – 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 listed in **[UP-D30-R05]**

[PR-D30-R09] – The WP29 would like to recall that any processing (including collection and transfer) of sensitive data subject to EU law has to be made on legitimate grounds according to article 8 of the Directive. The Privacy Shield cannot be interpreted as offering alternative grounds for such processing pg. 14

[PR-D30-R10] – Important new notions like the right to data portability and additional obligations on data controllers, including the need to carry out data protection impact assessments and to comply with the principles of privacy by design and privacy by default, have not been included in the

Privacy Shield. The WP29 would therefore like to suggest that the Privacy Shield, as with any existing adequacy decisions, is reviewed shortly after the GDPR enters into application. pg. 15

[PR-D30-R11] – 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

[PR-D30-R12] – 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

[PR-D30-R13] – It should be clarified that in any case, the Choice principle cannot be used to circumvent the 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

[PR-D30-R14] – The WP29 would like to emphasise that aggregated data can still be re-identified and therefore should be regarded as personal data. pg. 36

[PR-D30-R15] – 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

[PR-D31-R01] – The following sections of the Africa Union convention on cybersecurity and personal data protection could possibly confer requirements on a gTLD directory service.

[PR-D31-R02] – Article 2 (2) requires provision of certain information. It states: "Without prejudice to other information obligations defined by extant legislative and regulatory texts in African Union Member States, State Parties shall ensure that any person exercising e-commerce activities shall provide to those for whom the goods and services are meant, easy, direct and uninterrupted access using non-proprietary standards with regard to the following information:

- Where a physical person is involved, the provider shall indicate his/her name and where it is a legal person, its corporate name; its capital, its registration number in the register of companies or associations;

- Full address of the place of establishment, electronic mail address and telephone number;
- Where the person is subject to business registration formalities or registration in the national directory of businesses and associations, the registration number, the share capital and corporate headquarters;
- Where the person is subject to taxes, the tax identification number;
- Where his/her activity is subject to a licensing regime, the name and address of the issuing authority, and the reference of the authorization;
- Where the person is member of a regulated profession, the applicable professional rules, his/her professional title, the African Union State Party in which he/she was granted such authorization, as well as the name of the order or professional body with which he/she is registered."

[PR-D31-R03] – On personal data, the Africa Union convention makes personal data processing subject to a declaration before the protection authority and each authority may establish standards for such processing. Article 8: Objective of this Convention states with respect to personal data:

- "Each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data.
- The mechanism so established shall ensure that any form of data processing respects the fundamental freedoms and rights of natural persons while recognizing the prerogatives of the State, the rights of local communities and the purposes for which the businesses were established."

[PR-D31-R04] – Article 9: Scope of application of the Convention states that the following actions shall be subject to this [Africa Union] Convention:

- "Any collection, processing, transmission, storage or use of personal data by a natural person, the State, local communities, and public or private corporate bodies;
- Any automated or non-automated processing of data contained in or meant to be part of a file, with the exception of the processing defined in Article 9.2 of this [Africa Union] Convention;
- Any processing of data undertaken in the territory of a State Party of the African Union;
- Any processing of data relating to public security, defence, research, criminal prosecution or State security, subject to the exceptions defined by specific provisions of other extant laws."

[PR-D31-R05] – Article 10: Preliminary personal data processing formalities, states: "With regard to the most common categories of personal data processing which are not likely to constitute a breach of privacy or individual freedoms, the protection authority may establish and publish standards with a view to simplifying or introducing exemptions from the obligation to make a declaration."

[PR-D31-R06] – Article 10: Preliminary personal data processing formalities, states: "The following actions shall be undertaken after authorization by the national protection authority:

- Processing of personal data involving genetic information and health research;

- Processing of personal data involving information on offenses, convictions or security measures;
- Processing of personal data for the purpose of interconnection of files as defined in Article 15 of this [Africa Union] Convention, data processing involving national identification number or any other identifier of the same type;
- Processing of personal data involving biometric data;
- Processing of personal data of public interest, particularly for historical, statistical or scientific purposes"

[PR-D31-R07] – Article 13: Basic principles governing the processing of personal data, defines:

- Principle 1: Principle of consent and legitimacy of personal data processing
- Principle 2: Principle of lawfulness and fairness of personal data processing
- Principle 3: Principle of purpose, relevance and storage of processed personal data
- Principle 4: Principle of accuracy of personal data
- Principle 5: Principle of transparency of personal data processing
- Principle 6: Principle of confidentiality and security of personal data processing

[PR-D31-R08] – Article 14: Specific principles for the processing of sensitive data, states: "State Parties shall undertake to prohibit any data collection and processing revealing racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject." However, the prohibitions set forth in Article 14.1 shall not apply to the following categories where:

a) Processing relates to data which are manifestly made public by the data subject;
b) The data subject has given his/her written consent, by any means, to the processing and in conformity with extant texts;
c) Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/her consent;
d) Processing, particularly of genetic data, is required for the establishment, exercise or defence of legal claims;
e) A judicial procedure or criminal investigation has been instituted;
f) Processing is necessary in the public interest, especially for historical, statistical or scientific purposes;
g) 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;
h) Processing is necessary for compliance with a legal or regulatory obligation to which the controller is subject;
i) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority or assigned by a public authority vested in the controller or in a third party to whom data are disclosed;
j) Processing is carried out in the course of the legitimate activities of a foundation, association or any other non-profit making body with a political, philosophical, religious, cooperative 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.

[PR-D31-R09] – Article 14: Specific principles for the processing of sensitive data, states: "Personal data processing for journalistic purposes or for the purpose of research or artistic or literary expression shall be acceptable where the processing is solely for literary and artistic expression or for professional exercise of journalistic or research activity, in accordance with the code of conduct of these professions."

[PR-D31-R10] – Article 14: Specific principles for the processing of sensitive data, states: "The provisions of this [Africa Union] Convention shall not preclude the application of national legislations with regard to the print media or the audio-visual sector, as well as the provisions of the criminal code which provide for the conditions for exercise of the right of reply, and which prevent, limit, compensate for and, where necessary, repress breaches of privacy and damage to personal reputation."

[PR-D31-R11] – Article 14: Specific principles for the processing of sensitive data, states: "A person shall not be subject to a decision which produces legal effects concerning him/her or significantly affects him/her to a substantial degree, and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her."

[PR-D31-R12] – Article 14: Specific principles for the processing of sensitive data, states:

"a) The data controller shall not transfer personal data to a non-Member State of the African Union unless such a State ensures an adequate level of protection of the privacy, freedoms and fundamental rights of persons whose data are being or are likely to be processed.

b) The previous prohibition is not applicable where, before any personal data is transferred to the third country, the data controller shall request authorization for such transfer from the national protection authority."

[PR-D31-R13] – Article 34: Settlement of Disputes, states:

- "Any dispute arising from this [Africa Union] Convention shall be settled amicably through direct negotiations between the State Parties concerned.
- Where the dispute cannot be resolved through direct negotiation, the State Parties shall endeavour to resolve the dispute through other peaceful means, including good offices, mediation and conciliation, or any other peaceful means agreed upon by the State Parties. In this regard, the State Parties shall be encouraged to make use of the procedures and mechanisms for resolution of disputes established within the framework of the [Africa] Union."

[PR-D35-R01] – The Constitution of the State of California (USA): Article 1, Section 1, states that "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

[PR-D36-R01] – The Massachusetts Right of Privacy, Section 1B, states that, "A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages."

[PR-D37-R01] – The U.S. Supreme Court Case – McIntyre v. Ohio Elections Commission, states that, "An author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the [U.S. Constitution] First Amendment."

[PR-D37-R02] – The U.S. Supreme Court Case – McIntyre v. Ohio Elections Commission, states that, "The freedom to publish anonymously extends beyond the literary realm. In Talley, the Court held that the [U.S. Constitution] First Amendment protects the distribution of unsigned handbills urging readers to boycott certain Los Angeles merchants who were allegedly engaging in discriminatory employment practices. 362 U.S. 60."

[PR-D37-R03] – The U.S. Supreme Court Case – McIntyre v. Ohio Elections Commission, states that, "Despite readers' curiosity and the public's interest in identifying the creator of a work of art, an author generally is free to decide whether or not to disclose her true identity. The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry."

[PR-D38-R01] – The following sections of the Ghana Protection Act could possibly confer requirements on a gTLD directory service.

[PR-D38-R02] – Section 17, Privacy of the individual, states: "A person who processes data shall take into account the privacy of the individual by applying the following principles: (a) accountability, (b) lawfulness of processing, (c) specification of purpose, (d) compatibility of further processing with purpose of collection, (e) quality of information, (f) openness, (g) data security safeguards, and (h) data subject participation."

[PR-D38-R03] – Section 19 further elaborates these principles by providing for:

a) minimality,
b) Consent, justification and objection,
c) how personal data may be collected (directly except where it is in public record, there is consent, no prejudice is likely to be suffered, for purposes of crime prevention, enforcement of the law, conduct of judicial proceedings, protection of national security or protection of a third party's interests), compliance would prejudice a lawful purpose or compliance is not reasonably practicable
d) Collection of data for specific purpose
e) Data subject to be made aware of purpose of collection
f) Retention of records where the guidelines are that:
    (i) the retention of the record is required or authorised by law,

(ii) the retention of the record is reasonably necessary for a lawful purpose related to a function or activity,
(iii) retention of the record is required by virtue of a contract between the parties to the contract, or
(iv) the data subject consents to the retention of the record.

g) Further processing to be compatible with purpose of collection
h) Quality of information

[PR-D38-R04] – Registration of data controller is necessary and section 27 states that

- A data controller who intends to process personal data shall register with the Commission.
- A data controller who intends to collect personal data shall ensure that the data subject is aware of:
  a) the nature of the data being collected;
  b) the name and address of the person responsible for the collection;
  c) the purpose for which the data is required for collection;
  d) whether or not the supply of the data by the data subject is discretionary or mandatory;
  e) the consequences of failure to provide the data;
  f) the authorised requirement for the collection of the information or the requirement by law for its collection;
  g) the recipients of the data;
  h) the nature or category of the data; and
  i) the existence of the right of access to and the right to request rectification of the data collected before the collection.

[PR-D38-R05] – Other Ghana Protection Act *possible* requirements for a data processor are there must be security of the data (Section 28) and that data must be processed by an authorised person (section 29). Data subjects have a right to access the data and the law specifies how the data controller is to provide the access. Specifically, the data controller must notify the data subject that their (personal) data is being sought.

[PR-D38-R06] – The Ghana Protection Act also specifies how the right of access to personal data may be exercised in section 35.

[PR-D39-R01] – The following sections of South Africa's Protection of Personal Information Act could possibly confer requirements on a gTLD directory service.

[PR-D39-R02] – Section 4, Lawful processing of personal information, states: "The conditions for the lawful processing of personal information by or for a responsible party are the following: accountability, processing limitation (including minimality), purpose specification (including limitations on retention), further processing limitation, information quality, openness, security safeguards and data subject participation."

[PR-D39-R03] – Section 5, Rights of data subjects, states: "A data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3, including the right—

(a) to be notified that—

(i) personal information about him, her or it is being collected as provided for in terms of section 18; or

(ii) his, her or its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22;

(b) to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information as provided for in terms of section 23;

(c) to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24;

(d) to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11(3)*(a)*;

(e) to object to the processing of his, her or its personal information—

(i) at any time for purposes of direct marketing in terms of section 11(3)*(b)*; or

(ii) in terms of section 69(3)*(c)*;

(f) not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69(1);

(g) not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71;

(h) to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 74; and

(i) to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99."

[PR-D39-R04] – Section 6, Exclusions, states: "This Act does not apply to the processing of personal information—

(a) in the course of a purely personal or household activity;

(b) that has been de-identified to the extent that it cannot be re-identified again;

(c) by or on behalf of a public body—

(i) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders;

(ii) or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information;

(d) by the Cabinet and its committees or the Executive Council of a province; or

(e) relating to the judicial functions of a court referred to in section 166 of the Constitution."

[PR-D39-R05] – Section 26, Prohibition on processing of special personal information, states: "A responsible party may, subject to section 27, not process personal information concerning—

(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

(b) the criminal behaviour of a data subject to the extent that such information relates to—

(i) the alleged commission by a data subject of any offence; or

(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings."

[PR-D39-R06] – Section 27 states: "The prohibition on processing personal information, as referred to in section 26, does not apply if the—

(a) processing is carried out with the consent of a data subject referred to in section 26;

(b) processing is necessary for the establishment, exercise or defence of a right or obligation in law;

(c) processing is necessary to comply with an obligation of international public law;

(d) processing is for historical, statistical or research purposes to the extent that—

(i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or

(ii) it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;

(e) information has deliberately been made public by the data subject; or

(f) provisions of sections 28 to 33 are, as the case may be, complied with."

[PR-D39-R07] – Section 27 further states: "(2) The Regulator may, subject to subsection (3), upon application by a responsible party and by notice in the *Gazette*, authorise a responsible party to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject" and "(3) The Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (2)."

[PR-D39-R08] – Sections 28 to 32 specify how authorisation on data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or criminal behaviour or biometric information.

[PR-D41-R01] – RFC 7481, Section 4, Privacy Threats Associated with Registration Data, specifies that "RDAP data structures allow servers to indicate via status values when data returned to clients has been made private, redacted, obscured, or registered by a proxy." This provides a *possible* requirement: A registration directory service must be able to identify data elements that have been made private, redacted, obscured, or registered by a proxy.

[PR-D44-R01] – [gTLD directory services policies must take into consideration this statement by Professor Greenleaf:] In 2015, the number of countries with comprehensive data protection laws

surpassed those without data protection laws – for a total of 109 countries. Those adopting comprehensive data protection laws recently include: the Dominican Republic, Kazakhstan, South Africa, Mali, Cote d'Ivoire, Lesotho and Madagascar. Further, the pace continues as about 20 countries currently evaluate adoption.

[PR-D44-R02] – [gTLD directory services policies must take into consideration this statement by Professor Greenleaf:] "Countries without data privacy laws now in a minority." "Future growth: Heading toward ubiquity." "Global growth is likely to continue beyond 2020.

[PR-D44-R03] – [gTLD directory services policies must take into consideration] Greenleaf's years of research [which] are summarized in his finding that by the end of this decade the number of countries with data privacy laws, all of which have a strong 'family resemblance,' will be between 66% and 80% of all independent jurisdictions globally.

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.

[THE FOLLOWING SECTIONS HAVE NOT YET BEEN COMPLETED. IT IS EXPECTED THAT THE WG WILL FOCUS INITIALLY ON POSSIBLE REQUIREMENTS TO ADDRESS FUNDAMENTAL QUESTIONS. HOWEVER, CROSS-CUTTING QUESTIONS HAVE ALSO BEEN INCLUDED BELOW AS PLACE-HOLDERS TO BE EXPANDED LATER AND TO ALLOW FOR POSSIBLE REQUIREMENTS TO BE MOVED OR ADDED.]

Coexistence (CX)

The following *possible* requirements address the charter question on Coexistence (CX):
What steps should be taken to enable next-generation RDS coexistence with & replacement of the legacy WHOIS system?

[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

Coexistence Reqs	Coexistence Design	Coexistence Guidance on
- Coexistence Needs (incl. Time Period, Phased Transition Plan)	- Policies to address Coexistence Needs Per Stakeholder	- Incremental Test/Adoption - Transition Plan for each Area (e.g., Access, Accuracy, Privacy)

[CX-D01-R##] – Draw from EWG Section 5a, Alignment with 2013 RAA and New Data Elements, and Annex F, System Models – Ease of Transition. [TO DO – COPY/PASTE *possible* requirements HERE]

[CX-D09-R01] – The WHOIS RT recommends ongoing development of [gTLD registration directory services] policy within ICANN's existing machinery, and the impact of other policy development on [registration directory services].

[CX-D12-R01] – Adoption of a new [gTLD registration directory service] should take into account impacts (e.g., on cost of data access and parsing) on existing providers of applications and services related to registration data. (Sec. 5.10)

[CX-D25-R01] – Council of Europe's Treaty 108 on Data Protections imposes some restrictions on transborder flows of personal data to States where legal regulation does not provide equivalent protection. These legal restrictions may impact [this PDP] if large amounts of data from the

[existing gTLD registration directory service known as] WHOIS are "repurposed" by a next-generation gTLD registration directory service or moved from registries and registrars to new database(s). See also **[SM-D25-R01]**.

[CX-D26-R01] – According to the Directive (5), whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

[CX-D26-R02] – According to the Directive (45), whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

[CX-D30-R01] – Because the Privacy Shield will also be used to transfer data outside the US, the WP29 insists that onward transfers from a Privacy Shield entity to third country recipients should provide the same level of protection on all aspects of the Shield (including national security) and should not lead to lower or circumvent EU data protection principles pg3

[CX-D30-R02] – 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

[CX-D30-R03] – Privacy Shield documents make use of terminology that is not consistent with the vocabulary generally used in the EU when dealing with data protection. This is not necessarily a problem, as long as it is clear what the corresponding terminology under EU law (and under U.S. law) would be. The WP29 regrets to note however this is not the case, including in the draft adequacy decision. For example, the word 'access' is used in chapter 3 of the draft adequacy decision in a sense that implies the collection of personal data, instead of allowing someone to see data that is already collected. Access by companies to the data and the individuals' right of access are two separate notions that should not be confused. pg. 13

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.

Compliance (CM)

The following ***possible*** requirements address the charter question on Compliance (CM):
What steps are needed to enforce these policies?

[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

Compliance Reqs	Compliance Design	Compliance Guidance on
- Guiding Principles for Anti-Abuse Deterrents, Auditing, Enforcement - Establish Goals/Metrics	- Compliance Policy Per Ecosystem Player (e.g., RDS Operator, Requestors, Validators)	- Contract Ammend. Needs (RAA and Registry) - New Contract Needs - Compliance Benchmarks

[CM-D01-R##]– Draw from Contractual Relationship Principles 109-113 on page 91
[TO DO – COPY/PASTE EWG Principles 109-113 HERE]

[CM-D01-R##] – Draw from Accountability & Audit Principles 114-133 on pages 91-94. See also summary of types of accountability and audit requirements in Table 6 on page 95.
[TO DO – COPY/PASTE EWG Principles 114-133 HERE]

[CM-D02-R01] – "Develop clear targets for compliance with respect to registration data accuracy; performance provisions such as SLA must be considered as part of the compliance function....

[CM-D02-R02] – "ICANN should take appropriate measures to reduce the number of WHOIS registrations that fall into the accuracy groups Substantial Failure and Full Failure"

[CM-D02-R03] – "ICANN should ensure that there is a clear, unambiguous and enforceable chain of contractual agreements with registries, registrars, and registrants to require the provision and maintenance of accurate WHOIS data. As part of these agreements, ICANN should ensure that clear, enforceable and graduated sanctions apply to registries, registrars and registrants that do not comply with its WHOIS policies. These sanctions should include de-registration and/or deaccreditation as appropriate in cases of serious or serial non-compliance."

[CM-D06-R01] – Registrar shall abide by any Consensus Policy that requires registrars to cooperatively implement a distributed capability that provides query-based [gTLD registration directory service] search functionality across all registrars. If the [gTLD registration directory service] implemented by registrars does not in a reasonable time provide reasonably robust, reliable, and convenient access to accurate and up-to-date data, the Registrar shall abide by any Consensus Policy requiring Registrar, if reasonably determined by ICANN to be necessary (considering such possibilities as remedial action by specific registrars), to supply data from Registrar's database to facilitate the development of a centralized [gTLD registration] database for the purpose of providing comprehensive Registrar [gTLD registration directory service] search capability.

[**CM-D09-R01]** – In Recommendations 7 and 9, the WHOIS RT recommends that:

[CM-D09-R02] – ICANN shall produce and publish an accuracy report focused on measured reduction in gTLD registration data that fall into the accuracy groups Substantial Failure and Full Failure, on an annual basis.

[CM-D09-R03] – ICANN should develop metrics to track the impact of the annual WHOIS Data Reminder policy notices to registrants, or alternatively, an effective policy that achieves the objective of improving data quality in a measurable way.

[CM-D09-R04] – In Recommendation 12, the WHOIS RT urged ICANN to focus its measurements and compliance work on those data elements that allow a Registrant to be "contactable," (minimal

data elements), rather than requiring that all WHOIS data be accurate. Specifically, the WHOIS RT stated "ICANN shall produce and publish an accuracy report focused on measured reduction in WHOIS registrations that fall into the accuracy groups Substantial Failure and Full Failure, on an annual basis."

[CM-D18-R01] – Based on the WHOIS Inter-Registrar Transfer Policy, **Section I.A.2.2.1**: "Transmission of a "transfer" command constitutes a representation on the part of the Gaining Registrar that the requisite authorization has been obtained from the Transfer Contact listed in the authoritative WHOIS database."

[CM-D18-R02] – Based on the WHOIS Inter-Registrar Transfer Policy, **Section I.A.4.4**: "If either a Registrar of Record or a Gaining Registrar does not believe that a transfer request was handled in accordance with the provisions of this policy, then the Registrar may initiate a dispute resolution procedure as set forth in Section C."

[CM-D23-R01] – "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. (See also **[UP-D23-R13]**)

[CM-D23-R02] – "This does not mean that the presented purpose should always be trusted as the actual and effective one, as there may be a discrepancy between what is claimed and what is pursued in practice by the data controller. Ultimately, compliance with other data protection requirements, such as the necessity and relevance of data, will always need to be measured against the actual purpose." (p.14)

[CM-D26-R01] – According to the Directive (3), whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

[CM-D26-R02] – According to the Directive (8), whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

[CM-D26-R03] – According to the Directive (18), whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

[CM-D26-R04] – According to the Directive (19), whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities

[CM-D26-R05] – According to the Directive (20), whereas the fact that the processing of data is carried out by a 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;

[CM-D26-R06] – According to the Directive (45), whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

[CM-D26-R07] – According to the Directive (46), whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

[CM-D26-R08] – According to the Directive (53), whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

[CM-D26-R09] – According to the Directive (54), whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out;

[CM-D26-R10] – According to the Directive (62), whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

[CM-D26-R10] – According to the Directive Article 4, whereas Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: the processing is carried out in the context of the activities of an establishment of the controller

on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

[CM-D26-R11] – According to the Directive Article 18, Obligation to notify the supervisory authority, Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

[CM-D30-R01] – The WP29 considers a review must be undertaken shortly after the entry into application of the General Data Protection Regulation, in order to ensure the higher level of data protection offered by the Regulation is followed in the adequacy decision and its annexes. pg. 3

[CM-D30-R02] – Because the Privacy Shield will also be used to transfer data outside the US, the WP29 insists that onward transfers from a Privacy Shield entity to third country recipients should provide the same level of protection on all aspects of the Shield (including national security) and should not lead to lower or circumvent EU data protection principles. pg. 3

[CM-D30-R03] – 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

[CM-D30-R04] – 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

[CM-D30-R05] – Given the amount of data transfers that take place between the EU and the U.S. on a daily basis, which the WP29 recognises is a vital part of the economy on both sides of the Atlantic, legal clarity is needed sooner rather than later. pg. 12

[CM-D30-R06] – 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 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

[CM-D30-R07] – Privacy Shield documents make use of terminology that is not consistent with the vocabulary generally used in the EU when dealing with data protection. This is not necessarily a problem, as long as it is clear what the corresponding terminology under EU law (and under U.S. law) would be. The WP29 regrets to note however this is not the case, including in the draft adequacy decision. For example, the word 'access' is used in chapter 3 of the draft adequacy decision in a sense that implies the collection of personal data, instead of allowing someone to see data that is already collected. Access by companies to the data and the individuals' right of access are two separate notions that should not be confused. pg. 13

[CM-D30-R08] – The WP29 would like to recall that any processing (including collection and transfer) of sensitive data subject to EU law has to be made on legitimate grounds according to article 8 of the Directive. The Privacy Shield cannot be interpreted as offering alternative grounds for such processing pg. 14

[CM-D30-R09] – 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

[CM-D30-R10] – In any case of an onward transfer to a third country, every Privacy Shield organisation should be obliged to assess the mandatory requirements of the third country's national legislation applicable to the data importer prior to the transfer. If a risk of substantial adverse effect on the guarantees, obligations and level of protection provided by the Privacy Shield is identified, the U.S. Privacy Shield organisation acting as a Processor (Agent) shall promptly notify the EU data controller before carrying out any onward transfer. In these cases the data exporter is entitled to suspend the transfer of data and/or terminate the contract. Where there is such a risk of substantial adverse effect, a Shield organisation acting as a controller should not be allowed to onward transfer the data, as this would compromise its duty to provide the same level of protection as under the Principles in case of onward transfers (see Annex II,II.3.a).pg. 21

[CM-D30-R11] – A violation of the Privacy Shield principles might go unnoticed for a long period of time and might only be detected after serious harm has been caused to the data subject's fundamental rights, possibly beyond repair. Hence, this approach might contravene the European precautionary principle. pg. 30

[CM-D32-R01] – The specifications below are recommended requirements for registries. These requirements include independently-reviewed Management Policies, Procedures, and Personnel:

[CM-D32-R02] – Alternate (i.e., non-litigation) dispute resolution providing a timely and inexpensive forum for trademark-related complaints. (These procedures should be consistent with applicable national laws and compatible with any available judicial or administrative remedies.)

[CM-D32-R03] – A plan to ensure that the registry's obligations to its customers will be fulfilled in the event that the registry goes out of business. This plan must indicate how the registry

would ensure that domain name holders will continue to have use of their domain name and that operation of the Internet will not be adversely affected.

[CM-D32-R04] – Procedures for assuring and maintaining the expertise and experience of technical staff.

[CM-D32-R05] – Commonly-accepted procedures for information systems security to prevent malicious hackers and others from disrupting operations of the registry. (may also apply to Privacy charter question)

[CM-D32-R06] – The specifications below are recommended requirements for registrars. These requirements include Management Policies, Procedures, and Personnel:

[CM-D32-R07] – A plan to ensure that the registrar's obligations to its customers and to the registries will be fulfilled in the event that the registrar goes out of business. This plan must indicate how the registrar would ensure that domain name holders will continue to have use of their domain name and that operation of the Internet will not be adversely affected.

[CM-D32-R08] – Commonly-accepted procedures for information systems security to prevent malicious hackers and others from disrupting operations. (may also apply to Privacy charter question)

[CM-D32-R09] – Alternative Dispute Resolution of Domain Name Conflicts. There must be a readily available and convenient dispute resolution process that requires no involvement by registrars. Registries/Registrars will abide by the decisions resulting from an agreed upon dispute resolution process or by the decision of a court of competent jurisdiction. If an objection to registration is raised within 30 days after registration of the domain name, a brief period of suspension during the pendency of the dispute will be provided by the registries.

[CM-D40-R01] – RFC 7480, HTTP Usage in the Registration Data Access Protocol (RDAP), Section 4.3, specifies that RDAP "servers must ignore unknown query parameters. Use of unknown query parameters for cache busting is described in Appendix B." This might apply to a registration directory service that implements RDAP.

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.

System Model (SM)

The following ***possible*** requirements address the charter question on System Model (SM):
What system requirements must be satisfied by any next-generation RDS implementation?

[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

Cost Model Reqs	Cost Model Design	Cost Model Guidance on
- List of Expenses - List of Income Sources - Cost Drivers & Principles on Goals/Metrics/Mitigation	- Management & Allocation of Costs - Recovery Model (e.g., fees) - Cost Tracking Policies	- Ballpark Cost #s for entire Ecosystem, based on Model Design, covering full lifecycle (dev, test, migration, operation)

[SM-D01-R01] – The gTLD registration directory service "must be designed with extensibility in mind" (p.27)

[SM-D01-R02] – gTLD registration directory service must "log all access to gTLD registration data, including unauthenticated access to public data elements, and access restrictions to deter bulk harvesting." (p.40)

[SM-D01-R03] – gTLD registration directory service must "audit both public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use." (p.40)

[SM-D01-R04] – Draw from Model Design Principles 157, 159 & 160 on page 109
[TO DO – COPY/PASTE EWG Principles 157, 159 & 160 HERE]

[**SM-D01-R07]**– Draw from Data Storage, Escrow & Logging Principles 161-174 on pages 115-116
[TO DO – COPY/PASTE EWG Principles 161-174 HERE]

[SM-D01-R21] – Draw from Protocol Extensions &/or Additions on page 157
[TO DO – TURN THIS INPUT INTO A POSSIBLE REQUIREMENT]

[SM-D05-R01] – "The WHOIS protocol has not been internationalised. The WHOIS protocol has no mechanism for indicating the character set in use. Originally, the predominant text encoding in use was US-ASCII. In practice, some WHOIS servers, particularly those outside the USA, might be using some other character set either for requests, replies, or both. This inability to predict or express text encoding has adversely impacted the interoperability (and, therefore, usefulness) of the WHOIS protocol." (From Section 4: Internationalisation) This text implies that there is a [gTLD registration directory service] requirement for internationalization support.

[SM-D07-R01] – From Specification 6, Section 1: "Standards Compliance: For DNS, EPP, DNSSEC, IDN, IPv6." May also apply to other charter questions (data elements, compliance, standardization?)

[SM-D07-R02] – From Specification 10, Section 4.1: RDDS availability. Refers to the ability of all the RDDS services for the TLD, to respond to queries from an Internet user with appropriate data from the relevant Registry System. If 51% or more of the RDDS testing probes see any of the RDDS services as unavailable during a given time, the RDDS will be considered unavailable. (Note: Possible requirements taken from Section 4 many also belong under Compliance?)

[SM-D07-R03] – From Specification 10, Section 4.2: WHOIS [or replacement] Query RTT. Refers to the RTT of the sequence of packets from the start of the TCP connection to its end, including the reception of the WHOIS response. If the RTT is 5-times or more the corresponding SLR, the RTT will be considered undefined.

[SM-D07-R04] – From Specification 10, Section 4.3: Web-based-WHOIS [or replacement] query RTT. Refers to the RTT of the sequence of packets from the start of the TCP connection to its end, including the reception of the HTTP response for only one HTTP request. If Registry Operator implements a multiple-step process to get to the information, only the last step shall be measured. If the RTT is 5-times or more the corresponding SLR, the RTT will be considered undefined.

[SM-D07-R05] – From Specification 10, Section 4.4: RDDS query RTT. Refers to the collective of "WHOIS [or replacement] query RTT" and "Web-based- WHOIS [or replacement] query RTT".

[SM-D07-R06] – From Specification 10, Section 4.5: RDDS update time. Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, host or contact, up until the servers of the RDDS services reflect the changes made.

[SM-D07-R07] – From Specification 10, Section 4.6: RDDS test. Means one query sent to a particular "IP address" of one of the servers of one of the RDDS services. Queries shall be about existing objects in the Registry System and the responses must contain the corresponding information otherwise the query will be considered unanswered. Queries with an RTT 5 times higher than the corresponding SLR will be considered as unanswered. The possible results to an RDDS test are: a number in milliseconds corresponding to the RTT or undefined/unanswered.

[SM-D07-R08] – From Specification 10, Section 4.7: Measuring RDDS parameters. Every 5 minutes, RDDS probes will select one IP address from all the public-DNS registered "IP addresses" of the servers for each RDDS service of the TLD being monitored and make an "RDDS test" to each one. If an "RDDS test" result is undefined/unanswered, the corresponding RDDS service will be considered as unavailable from that probe until it is time to make a new test.

[SM-D07-R09] – From Specification 10, Section 4.8: Collating the results from RDDS probes. The minimum number of active testing probes to consider a measurement valid is 10 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

[SM-D07-R10] – From Specification 10, Section 4.9: Placement of RDDS probes. Probes for measuring RDDS parameters shall be placed inside the networks with the most users across the different geographic regions; care shall be taken not to deploy probes behind high propagation-delay links, such as satellite links."

[SM-D12-R01] – Information associated with the domain name, and information associated with the domain name registrant, must both be accessible at the registry level. (Rec. #1)

[SM-D12-R02] – The [gTLD registration directory service] should provide multiple fallback locations where data is stored, such that, in case of a failure, there are at least two geographically dispersed sources of data that are available for recovery. (sec. 5.3, 5.11)

[SM-D12-R03] – Under the [gTLD registration directory service], all information associated with the domain name as well as the registrant must be accessible via both the registrar and registry services. (sec. 5.4)

[SM-D12-R04] – The [gTLD registration directory service] should create a competitive level playing field among entities holding data, s and avoid making diversity in [gTLD registration directory service] data models a matter of competitive advantage. (sec. 5.9)

[SM-D13-R01] – Based on the review of ICANN's procedure for handling WHOIS conflicts with privacy law, the following System Modeling requirements from past accreditation agreements are unchanged: Registrars must notify registrants of: 4) How to access and rectify any data.

[SM-D25-R01] – Council of Europe's Treaty 108 on Data Protections imposes some restrictions on transborder flows of personal data to States where legal regulation does not provide equivalent

protection. These legal restrictions may impact [this PDP] if large amounts of data from the [existing gTLD registration directory service known as] WHOIS are "repurposed" by a next-generation gTLD registration directory service or moved from registries and registrars to new database(s). See also **[CX-D25-R01]**.

[SM-D26-R01] – According to the Directive (3), whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

[SM-D26-R02] – According to the Directive (8), whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

[SM-D26-R03] – According to the Directive (27), whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention;

[SM-D26-R04] – 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;

[SM-D26-R05] – According to the Directive (46), whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

[SM-D26-R06] – According to the Directive (55), whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force

majeure; whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

[SM-D26-R07] – As used in the Directive, (c) 'personal data filing system' ('filing system') means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

[SM-D26-R08] – According to the Directive Article 17, Security of processing, Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

[SM-D26-R09] – According to the Directive Article 17, Security of processing, Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

[SM-D28-R01] – [Any system model adopted for gTLD registration directory services] would be required to ensure that ICANN, Registries and Registrars:

- "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.
  See also **[UP-D28-R05]**

[SM-D29-R01] – Each data controller must respect the following rules as set out in the Directive:

[SM-D29-R02] – Personal Data must be processed legally and fairly;

[SM-D29-R03] – It must be collected for explicit and legitimate purposes and used accordingly;

[SM-D29-R04] – It must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed;

[SM-D29-R05] – It must be accurate, and updated where necessary;

[SM-D29-R06] – Data controllers must ensure that data subjects can rectify, remove or block incorrect data about themselves;

[SM-D29-R07] – Data that identifies individuals (personal data) must not be kept any longer than strictly necessary;

[SM-D29-R08] – Data controllers must protect personal data against accidental or unlawful destruction, loss, alteration and disclosure, particularly when processing involves data transmission over networks. They shall implement the appropriate security measures;

[SM-D29-R09] – These protection measures must ensure a level of protection appropriate to the data.

[SM-D29-R10] – Responsibilities towards data subjects. If a data subject is of the view that his/her data has been compromised, he/she can send a complaint to the data controller.

[SM-D29-R11] – If the data controller's handling of a complaint is not satisfactory, the data subject can file a complaint to the national supervisory data protection authority.

[SM-D29-R12] – In principle, all data controllers must notify their supervisory authorities when they process personal data.

[SM-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

[SM-D30-R02] – 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

[SM-D30-R03] – 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 listed in **[UP-D30-R05]**

[SM-D30-R04] – 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 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

[SM-D30-R05] – Privacy Shield documents make use of terminology that is not consistent with the vocabulary generally used in the EU when dealing with data protection. This is not necessarily a problem, as long as it is clear what the corresponding terminology under EU law (and under U.S. law) would be. The WP29 regrets to note however this is not the case, including in the draft adequacy decision. For example, the word 'access' is used in chapter 3 of the draft adequacy decision in a sense that implies the collection of personal data, instead of allowing someone to see data that is already collected. Access by companies to the data and the individuals' right of access are two separate notions that should not be confused. pg. 13

[**SM-D30-R06]** 4.2.4 Effective remedies need to be available to the individual As mentioned before, "The protection under the Fourth Amendment does not extend to non-U.S. persons that are not resident in the United States" This means that a non-U.S. person would not be able to challenge warrants or subpoenas in Court invoking the Fourth Amendment. The draft adequacy decision specifies that non-U.S. persons benefit indirectly through the protection afforded to the U.S. companies holding the personal data and who are the recipients of law enforcement requests. The WP29 however notes that, even if this protection were effective, it does not mean that effective remedies are available to individuals, since the subject of the right to an effective remedy in this scenario seems to be the company receiving the request of access, and not the individual whose data is at issue. pg. 55

[SM-D32-R01] – The specifications below are recommended requirements for **registries**. These requirements include an independently-tested, functioning Database and Communications System that:

[SM-D32-R02] – Is both robust (24 hours per day, 365 days per year) and scalable (i.e., capable of handling high volumes of entries and inquiries)

[SM-D32-R03] – Has multiple high-throughput (i.e., at least T1) connections to the Internet via at least two separate Internet Service Providers.

[SM-D32-R04] – Includes a daily data backup and archiving system.

[SM-D32-R05] – Incorporates a record management system that maintains copies of all transactions, correspondence, and communications with registrars for at least the length of a registration contract.

[SM-D32-R06] – Features a searchable, on-line database meeting the requirements of [NTIA Green Paper] Appendix 2.

[SM-D32-R07] – [Provides for] an adequate number (perhaps two or three) of globally- positioned zone-file servers connected to the Internet for each TLD.

[SM-D32-R08] – The specifications below are recommended requirements for registrars. These requirements include a functioning Database and Communications System that supports:

[SM-D32-R09] – Robust and scalable operations capable of handling moderate volumes
[SM-D32-R10] – Multiple connections to the Internet via at least two Internet Service Providers
[SM-D32-R11] – A daily data backup and archival system
[SM-D32-R12] – A record management system that maintains copies of all transactions, correspondence, and communications with all registries for at least the length of a registration contract.

[SM-D32-R13] – The specifications below are recommended requirements for registries**.** These requirements include an independently-inspected Physical Sites that feature:

[SM-D32-R14] – A backup power system including a multi-day power source.

[SM-D32-R15] – A high level of security due to twenty-four-hour guards and appropriate physical safeguards against intruders. (may also apply to Privacy)

[SM-D32-R16] – A remotely-located, fully redundant and staffed twin facility with ``hot switchover'' capability in the event of a main facility failure caused by either a natural disaster (e.g., earthquake or tornado) or an accidental (fire, burst pipe) or deliberate (arson, bomb) man-made event. (This might be provided at, or jointly supported with, another registry, which would encourage compatibility of hardware and commonality of interfaces.)

[SM-D32-R17] – The specifications below are recommended requirements for registrars. These requirements include an independently-inspected Physical Sites that feature:

[SM-D32-R18] – A backup power system.

[SM-D32-R19] – A high level of security due to twenty-four-hour guards and appropriate physical safeguards against intruders. (may also apply to Privacy charter question)

[SM-D32-R20] – Remotely-stored backup files to permit recreation of customer records.

[SM-D33-R01] – The NTIA's White and Green Papers set out four principles to guide the evolution of the domain name system: stability, competition, private bottom-up coordination, and representation. These principles presumably also apply to the design of any gTLD registration directory service.

[SM-D42-R04] – RFC 7482, Section 3, Path Segment Specification, specifies "The base URLs used to construct RDAP queries are maintained in an IANA registry described in [RFC7484]." This provides a *possible* requirement: A registration directory service must be able to form queries using provider-specific information maintained in an IANA registry.

[SM-D42-R05] – RFC 7482, Section 3.1.6, Help Path Segment Specification, specifies "The help path segment can be used to request helpful information (command syntax, terms of service, privacy policy, rate-limiting policy, supported authentication methods, supported extensions, technical support contact, etc.) from an RDAP server." This provides a *possible* requirement: A registration directory service must provide an online help facility that describes how to use the service.

[SM-D42-R06] – RFC 7482, Section 3.2, Search Path Segment Specification, specifies "The resource type path segments for search are..." This provides a *possible* requirement: A registration directory service must provide a search facility for domain names, name servers, and entities in addition to a basic lookup facility.

[SM-D42-R07] – RFC 7482, Section 5, Extensibility, specifies "This document describes path segment specifications for a limited number of objects commonly registered in both RIRs and DNRs. It does not attempt to describe path segments for all of the objects registered in all registries." This provides a *possible* requirement: It must be possible to add new features to a registration directory service.

[SM-D42-R08] – RFC 7482, Section 6, Internationalization Considerations, specifies "There is value in supporting the ability to submit either a U-label (Unicode form of an IDN label) or an A-label (US-

ASCII form of an IDN label) as a query argument to an RDAP service." This provides a *possible* requirement:

- A registration directory service must support queries using both the A-label and U-label forms of an Internationalized Domain Name (IDN) label; and
- A registration directory service must be able to return domain name and name server variants in response to IDN queries.

[SM-D46-R01] – A synchronized gTLD registration directory services system model is recommended by EWG to provide a single point of uniformly-controlled and logged access to domain or contact/registrant data from registries, registrars and validators.

[SM-D46-R02] – A synchronized gTLD registration directory services system model should receive registration data via EPP from a thick registry or validator in real time.

[SM-D46-R03] – A synchronized gTLD registration directory services system model does NOT require a centralized database containing all gTLD registration data. It may be deployed diverse data centers for robustness and high performance.

[SM-D46-R04] – Compared to a federated gTLD registration directory services system model, a synchronized model is recommended to provide "one stop shopping" which is uniform and reduces confusion for users

[SM-D46-R05] – Compared to a federated gTLD registration directory services system model, a synchronized model is recommended to reduce costs especially for Reverse Queries or WhoWas data.

[SM-D46-R06] – Compared to a federated gTLD registration directory services system model, a synchronized model provides no greater security risk of attack, abuse or exposure of sensitive data. “The argument that the [registration directory service] would create a giant database of extremely sensitive data that would be heavily attacked simply doesn't hold much water when examined with these real-world, risk-based factors in mind.”

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.

Cost (CS)

The following ***possible*** requirements address the charter question on Cost (CS):
What costs will be incurred & how must they be covered?

[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

Cost Model Reqs	Cost Model Design	Cost Model Guidance on
- List of Expenses - List of Income Sources - Cost Drivers & Principles on Goals/Metrics/Mitigation	- Management & Allocation of Costs - Recovery Model (e.g., fees) - Cost Tracking Policies	- Ballpark Cost #s for entire Ecosystem, based on Model Design, covering full lifecycle (dev, test, migration, operation)

[CS-D01-R##]– Draw from Cost Principles 175-180 on page 117
[TO DO – COPY/PASTE EWG Principles 175-180 HERE]

[CS-D10-R01] – The actual cost of validation is dependent on many factors that need to be considered at the same time. Some of these factors are the cost of developing and deploying automation where applicable, the cost of a single validation, the cost of repeating the validation, and the cost of maintaining the information and infrastructure necessary to support the process of validation. (Page 9)

[CS-D10-R02] – Verifying whether or not an E.164 conformant phone number can be called requires attempting to connect to it using either the PSTN or the Signaling System No. 7 (SS7) network. Both methods may incur charges. (Page 12)

[CS-D10-R03] – When a cellular number is verified with the use of the Short Message Service (SMS), having a registrant call from a particular number may pose problems for those that use corporate direct inward dialing (DID) lines where outbound calls are automatically mapped to the main corporate number, frequently without the knowledge of the person making the call. Both may incur charges for either the sender or receiver or both. (Page 12)

[CS-D10-R04] – Within the G20 major economies, about eight have highly accurate address information. While the information is available it is expensive and each country has a different procedure for normalizing an address, which must be done before it can be checked against a postal address database. (Page 13)

[CS-D10-R05] – There is a large upfront cost in the beginning as nothing is validated. As registrants are validated the number of unverified registrants drops significantly, and thus costs for subsequent years might be more directly related to the validity periods, i.e., the frequency at which data must be revalidated. (Page 14)

[CS-D10-R06] – There are economies of scale for validation: costs of per contact data element validation drops as more contacts are validated. (Page 14)

[CS-D10-R07] – In EPP registries, registrars are free to create and manage multiple contact objects that refer to the same individual. Thus, the cost of validating the contact data associated with a domain name may be the cost of validating each contact object. However, from an operational cost and registrant experience perspective, validation of a registrant associated with multiple domains might not require each domain's contact data elements to be re-validated if the registrant's contact data elements are the same for each domain name. (Page 14)

[CS-D12-R01] – Design of the [gTLD registration directory service] should take into account the costs incurred by registrars, registries and data consumers. (sec. 5.6)

[CS-D26-R01] – According to the Directive (46), whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to

prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

[CS-D26-R02] – According to the Directive (53), whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

[CS-D26-R03] – According to the Directive (54), whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out;

[CS-D26-R04] – 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 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;

[CS-D26-R05] – According to the Directive (64), whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

[CS-D30-R01] – Given the amount of data transfers that take place between the EU and the U.S. on a daily basis, which the WP29 recognises is a vital part of the economy on both sides of the Atlantic, legal clarity is needed sooner rather than later. pg. 12

[CS-D34-R01] – [gTLD registration directory services policies must consider this question:] What are the costs to Registrars, Registries, Registrants and ICANN, of creating a centralized system?

[CS-D34-R02] – [gTLD registration directory services policies must consider this question:] What are the costs to Registrars, Registries, Registrants and ICANN, of creating gated access to a centralized (or more centralized) system that may provide access to law enforcement or lawyers who are acting beyond or outside their jurisdiction in seeking the information or the person, company or organization for whom that domain name registration data is posted?

[CS-D34-R03] – [gTLD registration directory services policies must consider this question:] What are the costs to Registrars, Registries, Registrants and ICANN, of creating gated access to a centralized or more centralized system that may provide access to law enforcement who is specifically seeking to investigate or enforce criminal laws regarding conduct online that is not illegal in the country of the Registrar or the Registrant?

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.

Benefits (BE)

The following ***possible*** requirements address the charter question on Benefits (BE):
What benefits will be achieved & how will they be measured?

[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

Benefit Analysis Reqs	Benefit Analysis Design	Benefit Analysis Guidance on
- Guiding Principles on Benefit Goals/Metrics	- Benefit Tracking Policies	- Benefit Modeling, Metrics & Benchmarks

[BE-D01-R01] – The gTLD registration directory service must provide these benefits:
[INSERT EWG Key benefits listed in Section d on pages 67-68]

[BE-D01-R02] – ". . the provision of purpose-based contacts by Registrants must lead to significant improvements in reachability of appropriate contacts for various purposes and creates an incentive for Registrants to provide accurate information for those roles.

[BE-D01-R03] – Gated access to more sensitive data elements must reduce Registrant incentive to supply inaccurate data and increase Registrant accountability for data accuracy." (Bottom of p.68)

[BE-D01-R04] – "Pre-validation of Registrant or other contact information [must result in measurable benefits, including]:

[BE-D01-R05] – Increase accuracy of contact information by utilizing pre-validation to check data prior to use for a new domain name and to promote consistent data across all registrations (reduces error and fraud);

[BE-D01-R06] – Avoid the need to validate Registrant or other designated contact data each time a Registrant registers a new domain name by performing validation once and then reusing that block of contact data for several domain registrations (simplifies the process and reduces work requirements); and

[BE-D01-R07] – Avoid delay in the processing of a domain registration, since validation has to take place at the time of registration." (Section a on p.69)

[BE-D01-R08] – "To allow for much greater accuracy across such a diverse space and ease-of-use for such contacts, mechanisms [must be provided] to allow easy use of such contacts by multiple Registrants; for example, a web hosting company providing their NOC's unique ID for "technical" and "abuse" contacts for domains controlled by their customers." (Bottom of p.69)
[Also included as a requirement for DA Question]

[BE-D01-R09] – ". . when an entity needs to update their contact information to reflect a new address/phone number or a merger/acquisition, it must be easy to update that information in one place and have that reflected to all domains associated with that contact data set" (Top of p.70)
[Also included as a requirement for DA Question]

[BE-D01-R10] – The gTLD registration directory service must provide these benefits:
[TO DO: INSERT EWG Summary of Data Quality Key Benefits from Section h on pp. 79-80]

[BE-D01-R11] – The gTLD registration directory service must provide these benefits:
[TO DO: INSERT EWG Advantages from all of page 108]

[BE-D01-R12] – The gTLD registration directory service must provide benefits compared to Current Whois under the 2013 RAA, including… [TO DO: INSERT EWG Section b, pp.118-119]

[**BE-D10-R01]** – From a technical perspective, certain verification measures can be taken to reduce unintentional errors by registrants; for example, a formal data structure and strong typing of data (e.g., this field must be Arabic numbers only, this field must be alphabetical characters only) can reduce certain typographical errors. Enforcing mandatory submission of data for key data fields may reduce cases where users omit information. (Page 14)

[BE-D10-R02] – The use of automated techniques may necessitate an initial investment but the long-term improvement in the quality and accuracy of registration data will be substantial. (Page 15)

[BE-D19-R01] – Based on the ICANN Governmental Advisory Committee (GAC) proposed principles, "gTLD [registration directory] services should provide (…) data (…) in a manner that supports the stability, reliability, security, and global interoperability of the Internet, from both a technical and public trust perspective (…)" (para 3.3),

[BE-D23-R01] – 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.

[BE-D23-R02] – [The following potential benefit must be assessed:] "Article 8 of the European Convention on Human Rights focuses on the protection of private life, and requires justification for any interference with privacy. This approach is based on a general prohibition of interference with the right of privacy and allows exceptions only under strictly defined conditions. In cases where there is 'interference with privacy' a legal basis is required, as well as the specification of a legitimate purpose as a precondition to assess the necessity of the interference." p. 7.

[BE-D26-R01] – According to the Directive, 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

[BE-D29-R01] – "The EU Data Protection Directive requires data controllers to observe a number of principles when they process personal data. These principles not only protect the rights of those about whom the data is collected ("data subjects") but also reflect good business practices that contribute to reliable and efficient data processing."

[BE-D30-R01] – Given the amount of data transfers that take place between the EU and the U.S. on a daily basis, which the WP29 recognises is a vital part of the economy on both sides of the Atlantic, legal clarity is needed sooner rather than later. pg. 12

[BE-D37-R01] – If [gTLD registration directory services policies] include provisions that [provide registration data to] those seeking to access [gTLD domain name registrant's] names and/or physical locations for the purpose of harming the speaker of unpopular or minority ideas (be they individual or organizational) (see U.S. Supreme Court Case – McIntyre v. Ohio Elections Commission cited in **[PR-D37-R03]**), [any such policies must assess] the risk to Registrant stakeholders. (See also **[RI-D37-R01])**

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.

Risks (RI)

The following ***possible*** requirements address the charter question on Risks (RI):
What risks do stakeholders face & how will they be reconciled?

[CHECK FOR ALIGNMENT WITH PROCESS FRAMEWORK PHASE 1 FOR THIS QUESTION]

Risk Assess Reqs	Risk Assess Design	Risk Assess Guidance on
- Guiding Principles to reconcile Risks, Impacts, and Benefits	- Identify Risks - Assess Impacts	- Possible measures to accept, mitigate, and transfer risks

[RI-D01-R01] – "A widely scoped risk/impact analysis [must be done] to confirm that these principle-based [data element] classifications do in fact result in appropriate collection and disclosure of data for defined purposes." (p.56 & in Section c on pp.119-120)

[RI-D01-R02] – [TO DO – ADD FURTHER REQUIREMENTS FROM EWG Risk Analysis Section?]

[RI-D02-R01] – "The ICANN Board should ensure that a formal security risk assessment of the registration data policy be conducted as an input into the Policy Development Process. A separate security risk assessment should also be conducted regarding the implementation of the policy."

[RI-D10-R01] – Registration data often contain "stale" contact information and that this problem can cause difficulties when registrants seek to renew a domain name or modify DNS information. Stale information may prevent registrars from notifying a registrant that a domain registration is about to expire or that changes, possibly unauthorized, have been made to his domain registration. Failure to update information may result in domain hijacking or a dispute over the "ownership" of a domain. (Page 6)

[RI-D10-R02] – Since current access to registration data is public and anonymous, some individuals and businesses submit incorrect information because they do not wish their contact information to be collected and used by miscreants as targets for spam and other attacks. (Page 6)

[RI-D10-R03] – Some people intentionally submit false information because they do not wish to disclose personal contact information that can be accessed publicly and anonymously. (Page 6)

[RI-D10-R04] – Miscreants intentionally provide false information to obfuscate identification by law enforcement or parties that investigate malicious use of domains. (Page 7)

[RI-D10-R05] – Current registration requirements take a minimalist approach to validation. Unless credit verification measures are stringently applied for all levels of payment, little or no additional proof of identity and verification of contact information is required when a user registers a domain name. (Page 8)

[RI-D10-R06] – Users may mistype when registering domain names. The current validation processes can overlook errors. (Page 8)

[RI-D10-R07] – Users may not understand the consequences of the registration data accuracy program and annual obligation to maintain accurate and complete registration data. They also may refuse to take time to check that their contact information is current, or reject the notion that they will forfeit a domain registration simply because some registration data are inaccurate. (Page 8)

[RI-D10-R08] – If an email address is verified requiring explicit user action upon receiving a verification email (such as clicking on a web link or replying to the message in a specific way), the timing of the verification email message will need to be carefully considered as to how it affects the overall registration process. Sending the verification email as an integral part of the registration process would alter the business process and may affect registration costs. Sending the verification email after registration would risk being ignored by the registrant or could introduce an attack vector. A miscreant, knowing that these verification emails will be sent, could initiate various types of man-in-the-middle attacks. Past security research has shown that such spear-phishing attacks are highly effective. (Page 11)

[RI-D10-R09] – Existence of a postal address in a database does not guarantee that the physical address exists (e.g. apartment numbers in the United State Postal Service address database are indicated as a range. As a result, an address may validate as accurate and complete when in fact it is undeliverable). (Page 13)

[RI-D19-R01] – Based on the ICANN Governmental Advisory Committee (GAC) proposed principles, "The GAC recognizes that there are also legitimate concerns about the misuse of WHOIS [registration] data and conflicts with national laws and regulations, in particular applicable privacy and data protection laws" (para 2.2) (see **[PR-D19-R01]** and **[PR-D19-R02]**)

[RI-D23-R01] – [The following potential risk must be assessed:] “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 [European Data Protection] Directive.”

[RI-D25-R01] – Given the Council of Europe's Treaty 108 on Data Protections, Articles 5 and 6 (cited in **[PR-D25-R03]** and **[PR-D25-R04]**), a question that must be asked is: What Risks will Registrars, Registries and ICANN face if they are (a) collecting data, (b) processing data, and (c) shipping to other countries data that is not in compliance with Treaty 108?

[RI-D26-R01] – According to the Directive (9), whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free

movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

[RI-D30-R01] – Because the Privacy Shield will also be used to transfer data outside the US, the WP29 insists that onward transfers from a Privacy Shield entity to third country recipients should provide the same level of protection on all aspects of the Shield (including national security) and should not lead to lower or circumvent EU data protection principles pg 3

[RI-D30-R02] – 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

[RI-D30-R03] – 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

[RI-D30-R04] – Privacy Shield documents make use of terminology that is not consistent with the vocabulary generally used in the EU when dealing with data protection. This is not necessarily a problem, as long as it is clear what the corresponding terminology under EU law (and under U.S. law) would be. The WP29 regrets to note however this is not the case, including in the draft adequacy decision. For example, the word 'access' is used in chapter 3 of the draft adequacy decision in a sense that implies the collection of personal data, instead of allowing someone to see data that is already collected. Access by companies to the data and the individuals' right of access are two separate notions that should not be confused. pg 13

[RI-D30-R05] – A violation of the Privacy Shield principles might go unnoticed for a long period of time and might only be detected after serious harm has been caused to the data subject's fundamental rights, possibly beyond repair. Hence, this approach might contravene the European precautionary principle. pg. 30

[RI-D34-R01] – [gTLD registration directory services policies must assess] the risks to ICANN, Registrars and Registries of creating gated access to a centralized (or more centralized) system of hundreds of millions of gTLD registrations if the data is accessed illegally or accessed legally and then misused? To what extent might fundamental data protection and privacy rights be deemed violated by national laws, treaties, constitutions or other legal provisions, and who would be accountable?

[RI-D35-R01] – The Constitution of the State of California (USA)'s Right to Privacy states that "In contrast to the right to privacy recognized in the U.S. Constitution which requires state action, the right to

privacy under California law is generally understood to encompass actions by private individuals and entities which violate a privacy right." [citing Dorsey & Whitney LLP, A primer on California privacy law] If [gTLD registration directory services policies] include provisions that violate the privacy rights of California's citizens, [any such policies must assess] the risk to Registrars, Registries and ICANN.

[RI-D36-R01] – If [gTLD registration directory services policies] include provisions that violate the privacy rights of Massachusetts's citizens (see Massachusetts Right of Privacy cited in **[PR-D36-R01]**), [any such policies must assess] the risk to Registrars, Registries and ICANN.

[RI-D37-R01] – If [gTLD registration directory services policies] include provisions that [provide registration data to] those seeking to access [gTLD domain name registrant's] names and/or physical locations for the purpose of harming the speaker of unpopular or minority ideas (be they individual or organizational) (see U.S. Supreme Court Case – McIntyre v. Ohio Elections Commission cited in **[PR-D37-R03]**), [any such policies must assess] the risk to Registrant stakeholders.

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.

Other Questions (OQ)

The following *possible* requirements would apply to a totally new next-generation registration directory service or a modification of the existing WHOIS system, but may not belong under any of the 11 charter questions. During deliberation, the WG may determine these *possible* requirements are in fact already covered under other questions, or the WG may decide that questions(s) should be added to the charter to fill gaps.

[OQ-D01-R01] – "Provides appropriate access to accurate, reliable, and uniform registration data" (p.7)

[OQ-D01-R02] – gTLD registration directory services must provide for "accountability for all parties involved in the disclosure and use of gTLD domain name registration data." (p.10). [This can be done by:]

[OQ-D01-R03] – "Logging all access to gTLD registration data, including unauthenticated access to public data elements, to enable detection and mitigation of abuses; =

[OQ-D01-R04] – "Gating access to more sensitive data elements that would only be available to requestors who applied for and were accredited to receive gTLD registration data access, at the level appropriate for each user and stated purpose; and

[OQ-D01-R05] – "Auditing both public and gated data access to minimize abuse and impose penalties and other remedies for inappropriate use, in accordance with terms and conditions explicitly agreed upon by each requestor."

[OQ-D01-R06] – A "centralized interface must enable appropriate requestors to access registration information across all gTLDs, including unauthenticated public data access and authenticated

gated data access." (p.14)

[OQ-D04-R01] – The [gTLD registration directory service] must foster cyberpeace. Cyberspace will be destroyed by cyberwar and cyber surveillance if privacy is not respected online. Cyberspace will not be a peaceful sphere if the [gTLD registration directory service] enables, in any form, threats posed by terrorists, the activities of some States, organised crime, and/or corporations acting illegitimately.

[OQ-D17-R01] – Based on the WHOIS Expired Domain Deletion Policy, Section 3.7.5.2, which states: "Where Registrar chooses, under extenuating circumstances, to renew a domain name without the explicit consent of the registrant, the registrar must maintain a record of the extenuating circumstances associated with renewing that specific domain name for inspection by ICANN consistent with clauses 3.4.2 and 3.4.3 of this registrar accreditation agreement," the following additional *possible* requirement is suggested:

[OQ-D17-R02] – The Registrar must get consent from the domain owner to renew the domain. In case the registrar chooses to renew the domain without consent of the domain owner then the domain owner may not be held liable for the costs unless there is a mutual agreement between the Domain owner and the Registrant on specific terms. (Despite the fact that the registrant has reason for extenuating circumstances.)

[OQ-D17-R03] – The WHOIS Expired Domain Deletion Policy, Sections 3.7.5.4 through 3.7.5.6, require the Registrar to provide notice to each new registrant describing the details of their deletion and auto-renewal policy, to operate a website for domain name registration or renewal clearly displaying the details of the Registrar's deletion and auto-renewal policies, and to state, both at the time of registration and in a clear place on its website, any fee charged for the recovery of a domain name during the Redemption Grace Period. Based on these sections, the following additional *possible* requirement is suggested:

[OQ-D17-R04] – Domain owners (including those who would like to have temporal domains) should be granted an option to alert the Registrar of intentions not to renew a domain so as to let it expire and be left in the loop.

[OQ-D17-R05] – The WHOIS Expired Domain Deletion Policy, Sections 3.7.5.7, requires that "In the event that a domain which is the subject of a UDRP dispute is deleted or expires during the course of the dispute, the complainant in the UDRP dispute will have the option to renew or restore the name under the same commercial terms as the registrant. If the complainant renews or restores the name, the name will be placed in Registrar HOLD and Registrar LOCK status, the WHOIS contact information for the registrant will be removed, and the WHOIS entry will indicate that the name is subject to dispute. If the complaint is terminated, or the UDRP dispute finds against the complainant, the name will be deleted within 45 days. The registrant retains the right under the existing redemption grace period provisions to recover the name at any time during the Redemption Grace Period, and retains the right to renew the name before it is deleted." Based on this section, the following additional *possible* requirement is suggested:

[OQ-D17-R06] – WHOIS content [associated with] a domain which has been considered Expired or Deleted (after the agreed expiry time even after the grace period) should be hidden by the registrar to protect the identity of former owners who do not need to associate with a domain that has expired or deleted. This should be done with consent of the Domain owner.

[OQ-D24-R01] – Based on the Article 29 WP's Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, the following *possible* requirements apply to Data Controllers.

[OQ-D24-R02] – Article 7 [of Directive 95/46/EC] requires that personal data shall only be processed if at least one of six legal grounds listed in that Article apply. In particular, personal data shall only be processed (a) based on the data subject's unambiguous consent; or if - briefly put - processing is necessary for:

(b) Performance of a contract with the data subject;
(c) Compliance with a legal obligation imposed on the controller;
(d) Protection of the vital interests of the data subject;
(e) Performance of a task carried out in the public interest; or
(f) Legitimate interests pursued by the controller, subject to an additional balancing test against the data subject's rights and interests.

[OQ-D24-R03] – The Work Programme itself clearly stated two objectives: 'ensuring the correct implementation of the current legal framework' and also 'preparing for the future'.

[OQ-D24-R04] – Article 8 of the European Convention on Human Rights, adopted in 1950, incorporates the right to privacy - i.e. respect for everyone's private and family life, home and correspondence. It prohibits any interference with the right to privacy except if 'in accordance with the law' and 'necessary in a democratic society' in order to satisfy certain types of specifically listed, compelling public interests.

[OQ-D24-R05] – Article 8 of the European Convention on Human Rights focuses on the protection of private life, and requires justification for any interference with privacy. This approach is based on a general prohibition of interference with the right of privacy and allows exceptions only under strictly defined conditions. In cases where there is 'interference with privacy' a legal basis is required, as well as the specification of a legitimate purpose as a precondition to assess the necessity of the interference.

[OQ-D24-R06] – The Charter [of?] enshrines the protection of personal data as a fundamental right under Article 8 of the European Convention on Human Rights, which is distinct from the respect for private and family life under Article 7 7 [of Directive 95/46/EC]. Article 8 of the European Convention on Human Rights lays down the requirement for a legitimate basis for the processing. In particular, it provides that personal data must be processed 'on the basis of the consent of the person concerned or some other legitimate basis laid down by law'. These provisions reinforce both the importance of the principle of lawfulness and the need for an adequate legal basis for the processing of personal data.

[OQ-D24-R07] – This Section III [of Opinion 4/2014] provides a brief overview of each of the legal grounds in Article 7(a) through (e) [of Directive 95/46/EC], before the Opinion focuses, in Section III, on Article 7(f) [of Directive 95/46/EC]. This analysis will also highlight some of the most common interfaces between these legal grounds, for instance involving 'contract', 'legal

obligation' and 'legitimate interest', depending upon the particular context and the facts of the case.

[OQ-D24-R08] – It has an important role, but this does not exclude the possibility, depending on the context, that other legal grounds may be more appropriate either from the controller's or from the data subject's perspective. If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject's control becomes illusory and consent constitutes an inappropriate basis for processing.

[OQ-D24-R09] – "Clarification should aim at emphasizing that unambiguous consent requires the use of mechanisms that leave no doubt of the data subject's intention to consent. At the same time it should be made clear that the use of default options which the data subject is required to modify in order to reject the processing (consent based on silence) does not in itself constitute unambiguous consent. This is especially true in the on-line environment." It also required data controllers to put in place mechanisms to demonstrate consent (within a general accountability obligation) and requested the legislator to add an explicit requirement regarding the quality and accessibility of the information forming the basis for consent.

[OQ-D24-R10] – There is a clear connection here between the assessment of necessity and compliance with the purpose limitation principle. It is important to determine the exact *rationale* of the contract, i.e. its substance and fundamental objective, as it is against this that it will be tested whether the data processing is necessary for its performance. In some borderline situations it may be arguable, or may require more specific fact-finding to determine whether processing is necessary for the performance of the contract.

[OQ-D24-R11] – Fraud prevention - which may include, among others, monitoring and profiling customers - is another typical area, which is likely to be considered as going beyond what is necessary for the performance of a contract. Such processing could then still be legitimate under another ground of Article 7 [of Directive 95/46/EC], for instance, consent where appropriate, a legal obligation or the legitimate interest of the controller (Article 7(a), (c) or (f)). In the latter case, the processing should be subject to additional safeguards and measures to adequately protect the interests or rights and freedoms of data subjects. Article 7(b) only applies to what is necessary for the *performance* of a contract. It does not apply to all further actions triggered by non-compliance or to all other incidents in the execution of a contract. As long as processing covers the normal execution of a contract, it could fall within Article 7(b).

[OQ-D24-R12] – Article 7(d) [of Directive 95/46/EC] provides for a legal ground in situations where 'processing is necessary in order to protect the vital interests of the data subject'. This wording is different to the language used in Article 8(2)(c) [of the European Convention on Human Rights] which is more specific and refers to situations where 'processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent'.

[OQ-D24-R13] – Recital 27 of this Regulation 45/2001 provides that 'processing of personal data for the performance of tasks carried out *in the public interest* by the Community institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies.' This provision thus allows data processing on a broadly interpreted

'public task' ground in a large variety of cases, which could have otherwise been covered by a provision similar to Article 7(f) [of Directive 95/46/EC]. This includes:

[OQ-D24-R14] – Assessing which legal ground may potentially apply under Article 7(a)-(f). Data processing can be implemented only if one or more of the six grounds - (a) through (f) - of Article 7 [of Directive 95/46/EC] applies (different grounds can be relied on at different stages of the same processing activity).

[OQ-D24-R15] – Qualifying an interest as 'legitimate' or 'illegitimate' **-** To be considered as legitimate, an interest must cumulatively fulfil the following conditions:

- be lawful (i.e. in accordance with EU and national law);
- be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently concrete);
- represent a real and present interest (i.e. not be speculative).

[OQ-D24-R16] – Determining whether the processing is necessary to achieve the interest pursued - To meet this requirement, consider whether there are other less invasive means to reach the identified purpose of the processing and serve the legitimate interest of the data controller.

[OQ-D24-R17] – Establishing a provisional balance by assessing whether the data controller's interest is overridden by the fundamental rights or interests of the data subjects -

- Consider the nature of the interests of the controller (fundamental right, other type of interest, public interest);
- Evaluate the possible prejudice suffered by the controller, by third parties or the broader community if the data processing does not take place;
- Take into account the nature of the data (sensitive in a strict or broader sense?);
- Consider the status of the data subject (minor, employee, etc.) and of the controller (e.g. whether a business organisation is in a dominant market position);
- Take into account the way data are processed (large scale, data mining, profiling, disclosure to a large number of people or publication);
- Identify the fundamental rights and/or interests of the data subject that could be impacted;
- Consider data subjects' reasonable expectations;
- Evaluate impacts on the data subject and compare with the benefit expected from the processing by the data controller.

[OQ-D24-R18] – Establishing a final balance by taking into account additional safeguards Identify and implement appropriate additional safeguards resulting from the duty of care and diligence such as:

- data minimisation (e.g. strict limitations on the collection of data, or immediate deletion of data after use)
- technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation')
- wide use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments;

- increased transparency, general and unconditional right to object (opt-out), data portability & related measures to empower data subjects.

[OQ-D24-R19] – Demonstrat[ing] compliance and ensur[ing] transparency [by] draw[ing] a blueprint of steps 1 to 5 to justify the processing before its launch -

- Inform data subjects of the reasons for believing the balance tips in the controller's favour.
- Keep documentation available to data protection authorities.

[OQ-D24-R20] – What if the data subject exercises his/her right to object?

- Where only a qualified right to opt-out is available as a safeguard (this is explicitly required under Article 14(a) [of Directive 95/46/EC] as a minimum safeguard):- in case the data subject objects to the processing, it should be ensured that an appropriate and user-friendly mechanism is in place to re-assess the balance as for the individual concerned and stop processing his/her data if the re-assessment shows that his/her interests prevail.
- Where an unconditional right to opt-out is provided as an additional safeguard (either because this is explicitly required under Article 14(b) [of Directive 95/46/EC] or because this is otherwise deemed a necessary or helpful additional safeguard):- in case the data subject objects to the processing, it should be ensured that this choice is respected, without the need to take any further step or assessment.

[OQ-D25-R01] – How can policy requirements for [gTLD registration directory services] be created to be in compliance with the detailed requirements of the Council of Europe's Treaty 108 on Data Protections – and particularly its Articles 1, 5, 6, 12 and 14. [Note: Refer to **[FQ-D25]** for a list of *possible* requirements which cite those Articles and their legal requirements.]

[OQ-D28-R01] – *Is ICANN a Data Controller under the rules of the Data Protection Directive and other materials before this Working Group?* "Data controllers determine 'the purposes and the means of the processing of personal data'. This applies to both public and private sectors." If so, what are ICANN's requirements regarding a [gTLD registration] directory in which data is collected, processed and shared according to its contracts and agreements?

[OQ-D28-R02] – How can this PDP WG help ICANN review the key question of whether it is a Data Controller under EU and other Data Protection Laws and if so, how its obligations, responsibilities and liabilities are part of a [gTLD registration] directory and obligations it may impose on Registries and Registrars via contract and agreement?

Foundational Questions (FQ)

This section contains *possible* answers provided by key inputs to the charter's foundational questions:

- Is a new policy framework and next-generation RDS needed to address these requirements?
- If no, does the current WHOIS policy framework sufficiently address these requirements?
- If not, what revisions are recommended to the current WHOIS policy framework to do so?

[**FQ-D01]** – Abandon today's Whois model: "The EWG unanimously recommends abandoning today's WHOIS model of giving every user the same entirely anonymous public access to (often inaccurate) gTLD registration data." (p.5)

[FQ-D25] – ICANN's [gTLD registration directory service] policy [must] be shaped to be in compliance with the detailed requirements of the Council of Europe's Treaty 108 on Data Protections – and particularly its Articles 1, 5, 6, 12 and 14, and their specific requirements. [Note: Requirements given by Articles 1, 5, and 6 can be found in **[UP-D25-R02]**, **[UP/PR-D25-R03]**, **[PR-D25-R04]**. Article 12 states provisions that "shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed." Article 14, Assistance to data subjects resident abroad, states that "Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention." (This requirement may belong in "Other Questions" – see also **[OQ-D25-R01]**)

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.

Note: This draft contains *possible* requirements for registration data and directory services submitted by RDS PDP WG members as of 10 June. WG members continue to work on possible requirements from several other key documents already identified. Assignments still underway as of 10 June include:

- WHOIS Misuse Study and Final Study Report (2014)
- 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)
- Marrakech, Singapore, and Los Angeles GAC Communiqués (2014-2016)
- Article 29 WP 33 Opinion 5/2000, 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)
- U.S. Federal Communications Commission Proposed Rule FCC 16-39: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services
- Privacy Considerations for Internet Protocols (RFC 6973) (2013)
- Book: Global Tables of Data Privacy Laws and Bills (Greenleaf, 4rd Edition, January 2015)