QQ-D#-R#	Possible Requirement - USERS/PURPOSES (UP) Phase 1 with CODE = A, highlighting Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[UP-D01-R01]	"In support of ICANN's mission to coordinate the global Internet's system of unique identifiers, and to ensure the stable and secure operation of the Internet's unique identifier system, information about gTLD domain names is necessary to promote trust and confidence in the Internet for all stakeholders." (p. 16, Section IIb, Purpose)	None	1	A,AA,AD,I,IA,J	a
[UP-D01-R02]	"gTLD registration data [must be] collected, validated and disclosed for permissible purposes only." (p. 21, p. 31 Principle 6)	None	1	A,AA,AB,AC,B,BA,BC,C,CB,CC,DB,EB,EC,H,I,J,L,IA,IC,	a
[UP-D01-R03]	gTLD registration directory services must "accommodate in some manner all identified permissible purposes", including the following users and permissible purposes. (pp. 21-25, 27-29)	Precedes [UP-D01-R04 to R14], Depends on Permissible Purposes, Permissible Users	1	A,AA,AB,AD,B,BA,C,CA,CB,CC,DA,EA,H,I,IA,IC,J,L	a
[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."	None, Supports [UP-D01-R03]	1	A,AA,AC,AD,B,BA,BC,C,CA,CB,CC,DA,DB,EA,IB,IC,J	e
[UP-D01-R05]	* Personal Data Protection – "Identifying the accredited Privacy/Proxy Provider or Secure Protected Credential Approver associated with a DN and reporting abuse, requesting reveal, or otherwise contacting that Provider."	None, Supports [UP-D01-R03]	1	A,AA,AC,AD,B,BC,C,CA,CB,CC,D,DA,DB,EA,I,IA,IC,ID,J,L	g
[UP-D01-R06]	* Technical Issue Resolution – "Working to resolve technical issues associated with domain name use, including email delivery issues, DNS resolution failures, and website functional issues, by contacting technical staff responsible for handling these issues."	None, Supports [UP-D01-R03]	1	A,AC,AD,B,BC,C,CA,CB,CC,D,DA,F,I,IA,J,L	b
[UP-D01-R07]	* Domain Name Certification – "Certification Authority (CA) issuing an X.509 certificate to a subject identified by a domain name needing to confirm that the DN is registered to the certificate subject."	None, Supports [UP-D01-R03]	1	A,AA,AC,AD,B,BB,BA,BC,C,CA,D,G	a,c
[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."	None, Supports [UP-D01-R03]	1	A,AA,AC,AD,B,C,CC,DA,EA,EB,L	e,f
[UP-D01-R09]	* Business Domain Name Purchase or Sale – "Making purchase queries about a DN, acquiring a DN from another Registrant, and enabling due diligence research."	None, Supports [UP-D01-R03]	1	A,AA,AC,AD,B,C,CA,CC,DA	j
[UP-D01-R10]	* Academic/Public-Interest DNS Research – "Academic public-interest research studies about domain names published in [gTLD registration directory services], including public information about the Registrant and designated contacts, the domain name's history and status, and DNs registered by a given Registrant."	None, Supports [UP-D01-R03]	1	A,AA,AC,AD,B,BC,C,CA,CC	i
[UP-D01-R11]	* Legal Actions – "Investigating possible fraudulent use of a Registrant's name or address by other domain names, investigating possible trademark infringement, contacting a Registrant/Licensee's legal representative prior to taking legal action and then taking a legal action if the concern is not satisfactorily addressed. "	None, Supports [UP-D01-R03]	1	A,AA,AC,AD,B,C,CA,CC,DA,EB,I,IA,IC,J,L	j
[UP-D01-R12]	* Regulatory and Contractual Enforcement – "Tax authority investigation of businesses with online presence, UDRP investigation, contractual compliance investigation, and registration data escrow audits."	None, Supports [UP-D01-R03]	1	A,AA,AC,AD,B,C,CA,CC,DA,EB,I,IA,IC,J,L	i
[UP-D01-R13]	* Criminal Investigation & DNS Abuse Mitigation – "Reporting abuse to someone who can investigate and address that abuse, or contacting entities associated with a domain name during an offline criminal investigation."	None, Supports [UP-D01-R03]	1	A,AAA,AC,AD,B,C,CA,CB,CC,DA,CC,G,J,	b,q
[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."	None, Supports [UP-D01-R03]	1	A,AA,AC,AD,B,BA,C,CA,CB,CC,DA,EB,G	c

QQ-D#-R#	Possible Requirement - USERS/PURPOSES (UP) Phase 1 with CODE = A, highlighting Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[UP-D01-R15]	* gTLD registration directory services must support active deterrence of known malicious activities to the extent other requirements are satisfied. (See paragraph c on page 25.)	None	1	A,AA,AC,AD,B,C,CA,CB,CC,DA,EB,I,IA,IC,L	b
[UP-D01-R17]	Since it is likely that further [permissible purposes] will be identified over time, any [gTLD registration directory service] must be designed with extensibility in mind.	None	1	A,F,I,IA	a,h
[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.	None, Precedes [UP-D01-R26 to R31]	1	A,B,C,F,I,IA	h
[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.	Precedes [UP-D01-R35 to R41], Depends on Permissible Purposes	1	A,AA,AC,AD,B,CA,CB,CC,DA,DB,EB,IC,L	a
[UP-D01-R35]	* Purpose-based contact data must be provided for every registered domain name which makes public the union of data elements that are mandatory. [See DE possible requirements.]	Supports [UP-D01-R34], Depends on Data Element PR(s) for Contacts	1	A,AA,AC,AD,B,CA,CB,CC,DA,DB,EB,IC,L	a
[UP-D01-R36]	* All mandatory purpose-based contact data must be syntactically accurate and operationally reachable to meet the needs of every codified permissible purpose.	Supports [UP-D01-R34], Depends on Data Accuracy PR(s) for Contacts	1	A,AD,DA,DB	f
[UP-D01-R37]	* During domain name registration, the Registrant must be informed of all permissible purposes and given an opportunity to publish contact data for each purpose, including replacing the Registrant's contact data for any or all purposes.	Supports [UP-D01-R34], Depends on Data Element PR(s) for Contacts	1	A,AA,B,E,EA,EB,I,IA	e
[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].	Supports [UP-D01-R34], Depends on Data Element PR(s) for Contacts	1	A,AC,DB,DA	f
[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.	Supports [UP-D01-R34], Depends on Data Element PR(s) for Contacts	1	A,B,C,F,I,IA	a,h
[UP-D02-R02]	"Law enforcement has a legitimate need to access the real identity of the responsible party(ies) for a domain name."	None	1	A,AA,AD,B,C,CA,CB,CC,DA,E,EB,EC,L	b
[UP-D02-R03]	"Security practitioners have a legitimate need to access the real identity of those responsible for a domain name."	None	1	A,AA,AD,B,C,CA,CB,CC,DA,E,EB,EC,L	b
[UP-D05-R01]	"The WHOIS protocol has no provisions for strong security. WHOIS lacks mechanisms for access control, integrity, and confidentiality. Accordingly, WHOIS-based services should only be used for information which is non-sensitive and intended to be accessible to everyone." (From Section 5: Security Considerations) This text implies that there should be a requirement to provide services for access control, integrity, and confidentiality. It also suggests that [gTLD registration directory services] should not be used to access sensitive information.	Same as [GA-D05-R01] [PR-D05-R01], Depends on Access PR(s) for Public Access	1,3	A,AB,B,BA,C,CB,CC,DA,E,EA,EB,I,IA,L	d,l,u
[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.	Depends on Lawful Permissible Purposes	1	A,AA,AC,B,C,CA,CB,CC,D,DA,E,EA,EB,I,IA,L	d

QQ-D#-R#	Possible Requirement - USERS/PURPOSES (UP) Phase 1 with CODE = A, highlighting Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[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.	Depends on Permissible Purposes, Data Element PR(s) for collection of Personal Data, Privacy PR(s) stating limitations	1	A,BC,C,D,E,EA,EC,I,IA,J	a
[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.	None, Variant of [UP-D01-R11]	1	A,AC,B,BA,C,CA,CB,CC,DA,DB,EB,EC,I,IA,IC,L	a,d
[UP-D08-R02]	[gTLD directory services must support] Providing a public record of domain name ownership, accessible by the public for any lawful use.	None, Variant of [UP-D01-R14]	1	A,AC,B,C,CA,CB,CC,DA,EB,IC,L	a
[UP-D13-R01]	Based on the review of ICANN's procedure for handling WHOIS conflicts with privacy law, the following User/Purpose-related requirements from past accreditation agreements are unchanged: Registrars must notify registrants of: 1) the purposes for the collection of any personal data, and 2) the intended recipients of the data.	Depends on Permissible Purposes, Permissible Users, Data Element PR(s)	1	A,AA,AD,BC,C,CA,CB,CC,D,DA,DB,E,EA,EC,I,IA	b
[UP-D14-R01]	The 2013 RAA Data Retention Waiver and Discussion Document lists and describes all data elements that can be collected by the registrars in accordance with the 2013 RAA and it provides reasons / legitimate purposes for that collection and retention. The following possible User/Purpose requirement stems from this document: Registrars should have access to standard data elements.	Related to [DE-D14-R01], Depends on standard data elements such as those defined by [DE-D06-R08] and Permissible Purposes	1	A,AC,AD,D,DB,E,EA,EC,I,IA	a
[UP-D14-R02]	According to the 2013 RAA Data Retention Waiver and Discussion Document, the public community should have access to WHOIS Information (described in the WHOIS Specification) in order to mitigate abuse, address hijacking, theft and slamming.	Depends on WHOIS Specification	1	A,AC,B,C,CA,CB,CC,E,EA,EB,I,IA,IC,L	j
[UP-D14-R03]	According to the 2013 RAA Data Retention Waiver and Discussion Document, registrars should have access to and be able to collect records of communications with the registrant regarding the registration (log files including communication sources, IP, ISP, behaviour on the website, method of transmission, source IP address, HTTP header, email, Skype handle associated with communication) in order to mitigate fraud prevention, for billing disputes, for commercial purposes.	None	1	A,AC,B,C,CA,CB,CC,E,EA,EB,I,IA,IC,L	a,m
[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.	Related to [UP-D01-R12], Depends on Access PR(s) for Public Access, Data Element PR(s) for Contacts	1	A,AC,B,C,D,DA,DB,EB,EC,I,IA,IB,IC,L	k
[UP-D19-R01]	Based on the ICANN Governmental Advisory Committee (GAC) proposed principles and recommendations related to gTLD WHOIS services on the basis of general public policy issues, gTLD WHOIS [that is, registration directory] services should reflect and respect the following functions: detailed in [UP-D19-R02 to R09]	Precedes [UP-D19-R02 to R09]	1	A,I,IA	d
[UP-D19-R02]	* [Must reflect] Providing "a lookup service to internet users" (para 3.1 and para 2.1)	Supports [UP-D19-R01], Depends on Permissible Purposes involving this functionality	1	A,AC,B,BA,C,CA,CB,CC,DA	a,f
[UP-D19-R03]	* [Must reflect] "Providing contact points for network operators and administrators, including ISPs, and certified computer incident response teams" "to support the security and stability of the internet" (para 3.1 and para 2.1.1)	Supports [UP-D19-R01], Depends on Permissible Purposes involving this functionality, Data Element PR(s) for Contacts	1	A,AA,AC,B,C,CA,CB,CC,DA,EB,L	a,b
[UP-D19-R04]	* [Must reflect] "Allowing users to determine the availability of domain names" (para 3.1 and para 2.1.2)	Supports [UP-D19-R01], Depends on Permissible Purposes involving this functionality, Data Element PR(s) for Ops	1	A,AC,AD,B,BA,C,CA,CB,CC,DA	a,c

QQ-D#-R#	Possible Requirement - USERS/PURPOSES (UP) Phase 1 with CODE = A, highlighting Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[UP-D19-R05]	* [Must reflect] "Assisting law enforcement authorities (which may include non-governmental entities) in investigations, in enforcing national and international law" (para 3.1 and para 2.1.3)	Supports [UP-D19-R01], Depends on Permissible Purposes involving this functionality	1	A,AA,AD,BA,BC,C,CA,CB,CC,DA,EB,L	a,j
[UP-D19-R06]	* [Must reflect] "Assisting in combating against abusive use of ICTs, such as illegal and other acts motivated by racisms (…) including child pornography (…)" (para 3.1 and para 2.1.4)	Supports [UP-D19-R01], Depends on Permissible Purposes involving this functionality	1	A,AA,AD,BA,BC,C,CA,CB,CC,DA,EB,L	a,j
[UP-D19-R07]	* [Must reflect] "Facilitating clearance of trademarks and countering intellectual property infringements in accordance with applicable national laws and international treaties" (para 3.1 and para 2.1.5)	Supports [UP-D19-R01], Depends on Permissible Purposes involving this functionality	1	A,AA,AD,BA,BC,C,CA,CB,CC,DA,EB,L	a,j
[UP-D19-R08]	* [Must reflect] "Helping users to identify persons or entities responsible for content or services online" in contribution to user confidence in the Internet (para 3.1 and para 2.1.6)	Supports [UP-D19-R01], Depends on Permissible Purposes involving this functionality, Data Element PR(s) for RegID	1	A,B,BA,C,CA,CB,CC,DA,EB,IC,L	a,b,c
[UP-D19-R09]	* [Must reflect] "Assisting businesses, other organizations and users in combating fraud and general compliance with relevant laws" (para 3.1 and para 2.1.7)	Supports [UP-D19-R01], Depends on Permissible Purposes involving this functionality, Data Accuracy PR(s) antifraud	1	A,B,BA,C,DA,CB,CC,EB,IC,L	a,j
[UP-D21-R01]	In sum, from the Article 29 WP's comments on ICANN's procedures for handling WHOIS conflicts with privacy law (and related correspondence), we could draw out the following possible Purpose requirements: [detailed in [UP-D21-R02 to R04]	Precedes [UP-D21-R02 to R04]	1	A,E,EA,I,IA	a
[UP-D21-R02]	* Need a well-defined purpose for processing/use of data;	Supports [UP-D21-R01], Depends on Privacy PR(s) for Processing/Use	1	A,E,EA,I,IA	a,j
[UP-D21-R04]	* Bulk access to WHOIS data for direct marketing should be limited.	Supports [UP-D21-R01], Depends on Access PR(s) for Bulk Access, Same as [UP-D22-R04]	1	A,CA,E,EA,A,IA	i,j
[UP-D21-R05]	According to Article 29 WP's comments on ICANN's procedures for handling WHOIS conflicts with privacy law (and related correspondence), "Purpose definition is a central element in determining whether a specific processing or use of personal data is in accordance with EU data protection legislation."	Depends on Definition of personal data such as [DE-D26-R09]	1	A,E,EA,I,IA	a
[UP-D21-R06]	"Article 29 WP acknowledges the legitimacy of the purpose of the making available of some personal data through the WHOIS services ...[t]his publicity is necessary in order to put the person running a Website in a position to face the legal and technical responsibilities which are inherent to the running of such a site."	None	1	A,AC,AD,B,C,DA,DB,E,EA,EB,IC,L	b,e
[UP-D22-R01]	In sum, from the Article 29 WP's Opinion 2/2003, we could draw out the following possible Purpose requirements: [detailed in [UP-D22-R02 to R05]	Precedes [UP-D22-R02 to R05]	1	A,E,EA,EC	a
[UP-D22-R02]	* Need a well-defined purpose;	Supports [UP-D22-R01], Depends on Privacy PR(s) for Processing/Use	1	A,AC,AD,B,BA,C,CA,CB,CC,D,DA,DB,E,EA,EC,I,IA,IC,L	a,j
[UP-D22-R03]	* Data collected should be relevant (and not excessive) for defined purpose;	Supports [UP-D22-R01], Depends on Data Element PR(s)	1	A,AC,AD,B,BA,C,CA,CB,CC,D,DA,DB,E,EA,EC,I,IA,IC,L	a
[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."	Depends on Original Purpose	1	A,C,D,E,EA,I,IA,J	a

QQ-D#-R#	Possible Requirement - USERS/PURPOSES (UP) Phase 1 with CODE = A, highlighting Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[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	Depends on Permissible Purposes, Data Accuracy PR(s), Data Element PR(s)	1	A,C,D,E,EA,I,IA,J	a
[UP-D23-R02]	"When we share personal data with others, we usually have an expectation about the purposes for which the data will be used. There is a value in honouring these expectations and preserving trust and legal certainty, which is why purpose limitation is such an important safeguard, a cornerstone of data protection. Indeed, the principle of purpose limitation inhibits 'mission creep', which could otherwise give rise to the usage of the available personal data beyond the purposes for which they were initially collected." p.4	Same as [BE-D23-R01], Depends on Permissible Purposes, Privacy PR(s) on personal data	1	A,C,D,E,EA,I,IA,J	a
[UP-D23-R03]	"On the other hand, data that have already been gathered may also be genuinely useful for other purposes, not initially specified. Therefore, there is also a value in allowing, within carefully balanced limits, some degree of additional use. The prohibition of 'incompatibility' in Article 6(1)(b) does not altogether rule out new, different uses of the data – provided that this takes place within the parameters of compatibility." p.4	Depends on Permissible Purposes, Privacy PR(s) on personal data	1	A,C,D,E,EA,I,IA,J	a
[UP-D23-R04]	"The principle of purpose limitation - which includes the notion of compatible use - requires that in each situation where further use is considered, a distinction be made between additional uses that are 'compatible', and other uses, which should remain 'incompatible'. The principle of purpose limitation is designed to offer a balanced approach: an approach that aims to reconcile the need for predictability and legal certainty regarding the purposes of the processing on one hand, and the pragmatic need for some flexibility on the other." p.5	Depends on Permissible Purposes, Privacy PR(s) on personal data	1	A,C,D,E,EA,I,IA,J	a
[UP-D23-R05]	Council of Europe "CoE Resolution (73) 22 requires the information to be 'appropriate and relevant with regard to the purpose for which it has been stored' and - in the absence of 'appropriate authorisation' - prohibits its use 'for purposes other than those for which it has been stored' as well as its 'communication to third parties'." p.8.	Depends on Permissible Purposes, Access PR(s) for authorization, Privacy PR(s) on personal data	1	A,C,D,E,EA,I,IA,J	a
[UP-D23-R06]	"When applying data protection law, it must first be ensured that the purpose is specific, explicit and legitimate. This is a prerequisite for other data quality requirements, including adequacy, 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	Depends on Permissible Purposes, Data Accuracy PR(s), Access PR(s) for authorization, Privacy PR(s) on personal data	1	A,C,D,E,EA,I,IA,J	a
[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	Depends on Permissible Purposes, Data Accuracy PR(s), Data Element PR(s)	1	A,EA,C,D,E,I,IA,J	a
[UP-D23-R09]	* "First building block: purpose specification. Collection for 'specified, explicit and legitimate' purpose"	Supports [UP-D23-R08], Depends on Permissible Purposes	1	A,C,D,E,EA,I,IA,J	a
[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	Depends on Permissible Purposes, Original Purpose, Privacy PR(s)	1	A,EA,C,D,E,I,IA,J	a,d
[UP-D23-R13]	"User control: User control is only possible when the purpose of data processing is sufficiently clear and predictable. If data subjects fully understand the purposes of the processing, they can exercise their rights in the most effective way. For instance, they can object to the processing or request the correction or deletion of their data." p. 14	Depends on Permissible Purposes, Privacy PR(s)	1	A,C,D,E,EA,I,IA,J	a,e

QQ-D#-R#	Possible Requirement - USERS/PURPOSES (UP) Phase 1 with CODE = A, highlighting Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[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	Depends on Permissible Purposes, Data Element PR(s) on Collection, Privacy PR(s) on personal data	1	A,C,D,E,EA,I,IA,J	a,d
[UP-D23-R16]	"Processing of personal data in a way incompatible with the purposes specified at collection is against the law and therefore prohibited. The data controller cannot legitimise incompatible processing by simply relying on a new legal ground in Article 7. The purpose limitation principle can only be restricted subject to the conditions set forth in Article 13 of the Directive."	Depends on Permissible Purposes, Privacy PR(s) for Processing/Use	1	A,C,D,E,EA,I,IA,J	a
[UP-D25-R03]	Council of Europe's Treaty 108 on Data Protections specifies in Article 5, Quality of data that personal data undergoing automatic processing shall be: a. obtained and processed fairly and lawfully; b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c. adequate, relevant and not excessive in relation to the purposes for which they are stored; d. accurate and, where necessary, kept up to date; e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."	Same as [PR-D25-R03], Depends on Permissible Purposes, Data Accuracy PR(s), Definition of personal data such as [DE-D26-R09]	1	A,C,D,DB,E,EA,I,IA,J	a,m
[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;	Same as [PR-D26-R04], Depends on Permissible Purposes, Definition of personal data such as [DE-D26-R09]	1	A,C,D,E,EA,I,IA,J	a,d
[UP-D26-R04]	According to the Directive (28), whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;	Same as [DE-D26-R05], Depends on Permissible Purposes, Original Purpose, Definition of personal data such as [DE-D26-R09]	1	A,C,D,E,EA,I,IA,J	a,d
[UP-D26-R05]	According to the Directive (29), whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;	Depends on Definition of personal data such as [DE-D26-R09], Definition of Suitable Safeguards	1	A,C,CA,CC,D,E,EA,I,IA,J	a,d
[UP-D26-R06]	According to the Directive (30), whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding….subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;	Same as [PR-D26-R05], Depends on Definition of personal data such as [DE-D26-R09], Privacy PR(s) on Legal and Natural Persons	1	A,B,BA,C,CA,CB,CC,D,E,EA,EC,I,IA,J	a,d
[UP-D26-R07]	According to the Directive (31), whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;	Depends on Definition of personal data such as [DE-D26-R09]	1	A,B,BA,C,CA,CB,CC,D,DA,E,EA,EC,I,IA,J	a,b,d
[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;	Depends on National Law, Legitimate Interest, Permissible Purpose	1	A,AC,AD,B,BA,C,CA,CB,CC,D,DA,E,EA,EB,EC,IC,L	c

QQ-D#-R#	Possible Requirement - USERS/PURPOSES (UP) Phase 1 with CODE = A, highlighting Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[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;	Depends on Definition of personal data such as [DE-D26-R09], National or Community Law	1	A,B,E,EA,EC,I,IA,J	m
[UP-D26-R15]	As used in the Directive, [data] 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;	Depends on Definition of Controller such as [UP-D26-R14], Definition of personal data such as [DE-D26-R09]	1	A,B,E,EA,EC,I,IA,J	m
[UP-D26-R16]	As used in the Directive, 'third party' means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;	Depends on Definition of Controller such as [UP-D26-R14], Definition of Processor such as [UP-D26-R15]	1	A,B,E,EA,EC,I,IA,J	m
[UP-D26-R17]	As used in the Directive, [data] 'recipient' means a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;	None	1	A,B,BA,E,EC,I,IA,J	c
[UP-D26-R18]	As used in the Directive, 'the data subject's consent' means any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.	Depends on Definition of personal data such as [DE-D26-R09]	1	A,B,E,EA,EC,I,IA,J	l
[UP-D26-R19]	According to the Directive, Member States shall provide that personal data must be [handled as detailed in [UP-D26-R20 to R24]	Precedes [UP-D26-R20 to R24], Depends on Definition of personal data such as [DE-D26-R09]	1	A,B,E,EA,EC,I,IA,J	d
[UP-D26-R20]	* [personal data must be] processed fairly and lawfully;	Supports [UP-D26-R19], Related to [PR-D25-R03], Depends on Applicable Law	1	A,B,E,EA,EC,I,IA,J	d
[UP-D26-R21]	* [personal data must be] collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;	Supports [UP-D26-R19], Similar to [UP-D23-R01], Depends on Permissible Purposes	1	A,B,C,CA,CB,CC,D,E,EA,EC,I,IA,J	a
[UP-D26-R22]	* [personal data must be] adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;	Supports [UP-D26-R19], Similar to [UP-D23-R01], Depends on Permissible Purposes	1	A,AA,ABAC,B,BA,BC,C,CB,CC,DB,EA,EB,EC,H,I,IA,IC,J,L	r
[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.	Depends on National Law, Official Authority	1	A,AB,AD,BA,C,CA,CB,CC,D,E,EA,H,I,IA	a,d
[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.”	Depends on Permissible Purposes, Data Element PR(s) - RAA, Definition of personal data such as [DE-D26-R09]	1	A,B,BA,C,CA,CB,CC,D,DA,DB,E,EA,EB,EC,H,I,IA,IC,J,L	a,d

QQ-D#-R#	Possible Requirement - USERS/PURPOSES (UP) Phase 1 with CODE = A, highlighting Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[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."	Depends on Definition of personal data such as [DE-D26-R09], Data Element PR(s) on Retention	1	A,B,BA,C,CA,CB,CC,D,DA,DB,E,EA,EB,EC,H,I,IA,IC,J,L	o
[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."	Variant of [GA-D28-R01], Depends on Definition of personal data such as [DE-D26-R09], Data Protection Directive	1	A,IA,B,C,D,E,EC,F,G,H,I,J	a,d
[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	None, Same as [GA-D30-R01] [PR-D30-R05] [CM-D30-R03]	1	A,E,EA,EC,I,IA,J	a,d
[UP-D30-R06]	* Processing should be in accordance with the law and based on clear, precise and accessible rules: this means that anyone who is reasonably informed should be able to foresee what might happen with her/his data where they are transferred;	Supports [UP-D30-R05], Similar to [UP-D30-R21], Depends on Laws and Rules	1	A,AA,AB,B,BA,BC,C,CA,CB,CC,D,DA,E,EA,EC,I,IA,J,L	a,l
[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	Same as [DE-D30-R09], Depends on Permissible Purposes, Definition of personal data such as [DE-D26-R09]	1	A,AC,B,BA,C,CA,CB,CC,D,DA,E,EA,EC,I,IA,J,L	d
[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	Depends on PPD-28 Bulk Collection Purposes	1	A,CC,B,BC,CA,CB,D,E,EA,EC,I,IA,J,L	a,q
[UP-D53-R01]	In the Singapore GAC Communiqué of March 27, 2014, GAC requests that registration data be made available for the following stated purpose: "Safeguard 3: Should Registry Operators undertake periodic security checks to analyze whether domains in its gTLD are being used for threats to security, such as pharming, phishing, malware and botnets?" (Page 10	Depends on 2013 RAA	1	A,AC,B,BA,BC,C,CA,CB,CC,D,E,EA,EC,F,H,I,IA,IC,J,K,L	o
[UP-D62-R03]	When I buy something on the web, I would like to be able to access the registration data for the web page I am using to know it is the real company	None	1	A,AB,AC,AD,B,BA,C,CA,CC,D,DA,DB,E,I,IA,J,L	u
[UP-D62-R04]	There are a lot of third parties (not just LEAs) who have legitimate reasons for access to avoid their rights being infringed upon	None	1	A,AB,AD,B,BA,BC,C,CA,CB,CC,D,DA,DB,E,EA,EC,I,IA,IC,J,L	u
[UP-D62-R05]	Related to TM Clearinghouse notices, when notices are received, analysis that is performed includes going to see who is the registrant - this often eliminates the need for further action (~60-70%)	None	1	A,AB,AD,B,C,CA,CB,CC,D,DA,DB,EB,EC,I,I,IC,L	u

QQ-D#-R#	Possible Requirement - DATA ELEMENTS (DE) with CODE = A ONLY, filter set to Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[DE-D01-R01]	The [gTLD registration directory service] must accommodate purpose-driven disclosure of data elements.	None, Related to [UP-D01-R02]	1	A,AB	a,s
[DE-D01-R02]	Not all [gTLD registration] data collected is to be public; disclosure must depend upon Requestor and Purpose.	Depends on Permissible Users, Permissible Purposes	1	A,AB	a,s
[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.	Depends on Minimum Data Set such as [DE-D01-R26], Access PR(s) for Public Access	1	A,AA,DA	b,t
[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.	Depends on Data Set for each Permissible Purpose [DE-D01-R07], Access PR(s) for Gated Access	1	A,AB	a,s
[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).	Related to [DE-D01-R04], Depends on Data Set for each Permissible Purpose [DE-D01-R07], Access PR(s) for Gated Access	1	A,AB,D	a
[DE-D01-R06]	The only [gTLD registration] data elements that must be collected are those with at least one permissible purpose.	Related to [UP-D23-R14], Depends on Data Set for each Permissible Purpose [DE-D01-R07]	1	A,D	a
[DE-D01-R07]	Each [gTLD registration] data element must be associated with a set of permissible purposes.	Precedes [DE-D01-R08 to R11], Related to [DE-D01-R04 to R06], Similar to [DE-D01-R09], Depends on Permissible Purposes	1	A,D	a
[DE-D01-R08]	* An initial set of acceptable uses, permissible purposes, and data element needs are identified [by possible requirements fo Users/Purposes.]	Supports [DE-D01-R07], Depends on Permissible Purposes, Permissible Users, Privacy PR(s) for Processing/Use	1	A	a
[DE-D01-R09]	* Each permissible purpose must be associated with clearly-defined data element access and use policies.	Supports [DE-D01-R07], Similar to [DE-D01-R07], Depends on Privacy PR(s) for Processing/Use	1	A,AB	a
[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.	Related to [DE-D01-R26], Depends on Permissible Purposes, Privacy PR(s) for Collection and Processing/Use, Risk PR(s)	1	A,D,M	a
[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.	Depends on Data Set for each Permissible Purpose [DE-D01-R07], Privacy PR(s) on Choice and Limitation of Purpose	1	A,EA	a,l
[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.	Depends on PR(s) for Purpose-Based Contacts such as [UP-D01-R35], Privacy PR(s) for Collection	1	A,DA	f

QQ-D#-R#	Possible Requirement - DATA ELEMENTS (DE) with CODE = A ONLY, filter set to Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[DE-D01-R16]	Registrants may optionally designate Privacy/Proxy-supplied contacts or authorized third party contacts for specified permissible purposes.	Depends on Privacy PR(s) for P/P Providers	1	A,DA,ID	g
[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.	Depends on Data Accuracy PR(s) for Validation, Minimum Data Set such as [DE-D01-R26]	1	A,AD,DA,DB	a,e,f
[DE-D01-R18]	If a Registrant does not designate a contact for each mandatory permissible purpose, the Registrant's own contact data mus be used by default. (Note that the Registrant can avoid this by using an accredited Privacy/Proxy service, or by designating other contacts.	Related to [DE-D01-R17], Depends on PR(s) for Purpose-Based Contacts such as [UP-D01-R35], Privacy PR(s) for Collection	1	A,AA,DA,DB	f
[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.	Related to [DE-D01-R14 to R18] [PR-D01-R06], Depends on Privacy PR(s) for Collection and Storage	1	A,AD,DA,DB	f
[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	Similar to [DE-D06-R01] [DE-D07-R02], PR to be defined in P1, each referenced Data Element to be fully defined in P2, Depends on Permissible Purposes involving this data, Privacy PR(s)	1, 2	A,AD,D,J	an
[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].	None	1	A,AA,AB,DA	ae
[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.	Depends on Access PR(s), Definition of Registrant-Supplied Data such as [DE-D01-R26], Privacy PR(s) for Consent	1	A,AA,AB,M	s
[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.	Depends on Access PR(s) for Public Access, Definition of Registry/Registrar-Supplied Data such as [DE-D01-R20], Risk PR(s)	1	A,AA,AB,M	t
[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.	Depends on PR(s) for Purpose-Based Contacts such as [UP-D01-R35], Privacy PR(s)	1	A,AA,AB,DA	b
[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)	Similar to [DE-D06-R01] [DE-D07-R02], PR to be defined in P1, each referenced Data Element to be fully defined in P2, Depends on Permissible Purposes involving this data, Privacy PR(s), Risk PR(s)	1, 2	A,AA,D,DA	b
[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.	Related to [DE-D07-R01], Depends on Permissible Purposes	1	A,AB	d

QQ-D#-R#	Possible Requirement - DATA ELEMENTS (DE) with CODE = A ONLY, filter set to Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[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."	Depends on PR(s) for Purpose-Based Contacts such as [UP-D01-R35]	1	A,AB,AD,DA	f
[DE-D01-R32]	* Policies and processes must prevent unauthorized use of [a purpose-based contact's] contact data.	Supports [DE-D01-R30]	1	A	af
[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.	Related to Data Accuracy PR(s) for reusable Contact Directory such as [DA-D01-R02], Depends on Privacy PR(s)	1	A,AA,DA,DB	af
[DE-D01-R38]	Such contacts must contain valid mandatory data elements. Policies and oversight will be needed to manage these processe to ensure that Contact IDs are not used without contact's authorization and meet minimum standards.	Related to [DE-D01-R39], Depends on Contact's Authorization [DE-D01-R30], Data Accuracy PR(s) for Validation	1	A,AB	d
[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.	Variant of [DE-D01-R30], Depends on PR(s) for Purpose-Based Contacts such as [UP-D01-R35]	1	A,IA	d
[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)	Depends on Rules for Labeling and Display such as RAA Spec 3	1	A,AA,AD,DA,DB,F	al,am
[DE-D12-R02]	The [gTLD registration directory service] should collect and display uniform sets of data regardless of the registry involved. (sec. 5.2)	None, Variant of [DE-D12-R01]	1	A,AA,AD,DA,DB,F	al,am
[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.	Related to [UP-D14-R01] , Depends on standard data elements such as those defined by [DE-D06-R08]	1	A,D	ar
[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)	None, Same as [DA-D19-R01]	1	A,DA,DB	f,n
[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;	Same as [UP-D26-R04], Depends on Permissible Purposes, Original Purpose, Definition of personal data such as [DE-D26-R09]	1	A	a,d
[DE-D29-R03]	* [Personal Data] must be collected for explicit and legitimate purposes and used accordingly;	Supports [DE-D29-R01], Similar to [UP-D23-R01]	1	A	a,d
[DE-D29-R04]	* [Personal Data] must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed.	Supports [DE-D29-R01], Similar to [UP-D23-R01]	1	A,AB	r
[DE-D32-R01]	The specifications below are recommended requirements for dispute resolution and other procedures related to trademarks. These include:	Related to [UP-D01-R11], Precedes [DE-D32-R02 to R04]	1	-	-

QQ-D#-R#	Possible Requirement - PRIVACY (PR) with CODE = A ONLY, filter set to Dependencies = None	Prerequisites/Dependencies	Ph	C	K
[PR-D25-R03]	Council of Europe's Treaty 108 on Data Protections, Article 5, Quality of data, restricts the collection of data under its privacy laws to only that data that is: a. obtained and processed fairly and lawfully; b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c. adequate, relevant and not excessive in relation to the purposes for which they are stored; d. accurate and, where necessary, kept up to date; e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."	Same as [UP-D25-R03], Depends on Permissible Purposes, Data Accuracy PR(s), Definition of personal data such as [DE-D26-R09]	1	A,EA	a,m
[PR-D26-R04]	According to the Directive (26), whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;	Same as [UP-D26-R03], Depends on Permissible Purposes, Definition of personal data such as [DE-D26-R09]	1	A,IA	a,d
[PR-D26-R05]	According to the Directive (30), whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;	Same as [UP-D26-R06], Depends on Definition of personal data such as [DE-D26-R09], Privacy PR(s) on Legal and Natural Persons	1	A,IA	a,d
[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	None, Same as [UP-D30-R02] [CM-D30-R03]	1	A,IA	a,d

Note: Codes not yet reviewed

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)
[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
[47] Article 29 WP 33 Opinion 5/2000, Article 29 WP 41 Opinion 4/2001, and Article 29 WP 56 Working Document 5/2002
[48] U.S. Federal Communications Commission Proposed Rule FCC 16-39: Protecting the Privacy of Customers of broadband and Other Telecommunications Services
[49] Los Angeles GAC Communiqué (16 October 2014)
[50] Singapore GAC Communiqué (11 February 2015)
[51] Marrakech GAC Communiqué (March 2016)
[52] London GAC Communiqué (25 June 2014)
[53] Singapore GAC Communiqué (27 March 2014)
[54] SAC051, Report on Domain Name WHOIS Terminology (2011)
[55] Dissenting Report from Stephanie Perrin [PDF, 108 Kb] by Stephanie Perrin, EWG Member
[56] Law Enforcement Due Diligence Recommendations for ICANN (2010)
[57] GAC Comments to New gTLD Program Safeguards Against DNS Abuse Report (19 May 2016)
[58] GAC Public Comments to 2013 RAA WHOIS Accuracy Specification Review
[59] GAC Comments to Initial Report on the PPSAI PDP (Sep 2015)
[60] Where Do Old Protocols Go To Die?, by Scott Hollenbeck, EWG Member
[61] building a better WHOIS for the Individual Registrant, by Carlton Samuels, EWG Member
[62] Possible Requirements identified during the ICANN56 Cross-Community Session on RDS
[63] RDS PDP WG 2nd Outreach Responses from the RySG (26 June 2016)
[64] WHOIS Study Group Report to the GNSO Council (2008)
[65] IWG Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet (Crete, 4./5.05.2000)

[66] GNSO PDP on Privacy & Proxy Services Accreditation Issues (PPSAI) Final Report (2015)

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
Questions posed by the Charter

Note: All of the above hyperlinked documents and WG members submissions can be found at the following link:
https://community.icann.org/x/shOOAw

Assignments still underway as of 11 September include:
- 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)
- Final Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016)
- Privacy Considerations for Internet Protocols (RFC 6973) (2013)

QQ-D#-R# COLUMN - The unique number for each possible requirement which identifies…

QQ = Fundamental Questions from Charter**

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?

This Excel workbook contains all possible requirements from Draft 5 for the 5 fundamental questions only.

To view or print the entire list of possible requirements, please use Draft 5 in PDF format: https://community.icann.org/x/shOOAw

R# = A unique sequence number for that possible requirement, assigned within each question and document

This sequence number is to allow cross-referencing and link back to the source of each possible requirement

D# = The source document (D01, etc) from which the possible requirement was extracted

See hyperlinked list of source documents on the Tab Annex A

PHASE (Ph) COLUMN - Maps each possible requirement into one or more PDP Phases based on Charter guidance

1 = Policy Requirements

2 = Specific policies the WG will design, based on Phase 1 requirements

3 = Implementation and Coexistence Guidance associated with Phase 2 policies

For guidance on each question, refer to figure on Page 70 of the Final Issue Report

PREREQUISITES/DEPENDENCIES COLUMN - Starting point to identify the following

1) Inter-dependencies between possible requirements

2) Assumptions or pre-requisites or external dependencies included in possible requirements

3) Possible requirements that are verbatim duplicates or near-duplicates

This column is dynamic, to be fleshed out during deliberation to track identified dependencies

CODING (C) COLUMN - Hierarchical codes that can be FILTERED to select subsets of possible requirements

The table below provides a proposed coding of possible requirements to organize them into hierarchical groups to aid in deliberation.

The PDP WG may refine or add to the initial coding values below to examine new subsets.

	Code (C) Name	**Code (C) Definition**
A	Goals of System	PRs describing goals of RDS
AA	Transparency	PRs relating to transparency
AB	Differentiated (Gated) Access	PRs relating to differentiated or tiered access (see the "Gated Access" Charter Question)
AC	Authoritative Data	PRs relating to the goal of ensuring the reliability of the data, or the holdings most likely to be authoritative
AD	Accountability	PRs relating to the goal of accountability of the management of RDS
B	Functions	PRs relating to a broad range of functions of the RDS, or activities that are envisaged as taking place with the data
BA	Search & Query	PRs relating to the function of searching and querying in the RDS
BB	Certification & Authorization	PRs relating to certification functions with the RDS ecosystem, including potential end users and contracted parties
BC	Compliance	PRs relating to compliance with contractual or policy requirements (see "Compliance" Charter Question)
C	Potential Use of Data	PRs relating to the broad spectrum of potential use of the registration data (see "Purpose" Charter Question)
CA	Research	PRs related to research, including market research, legal research, consumer protection, academic, etc.
CB	Surveillance	PRs related to the broad use of RDS for surveillance purposes, including surveillance for compliance, for spotting cyber abuse, IP and trademark trends, etc.
CC	Investigation	PRs related to investigation, including LE, IP rights holders & agents, & cyber-security
D	Data Elements	PRs related to the data elements themselves (see "Data Elements" Charter Question)
DA	Contactability	PRs related to the characteristic of contactability, across a range of data elements
DB	Accuracy	PRs related to the characteristic of accuracy in data (see "Data Accuracy" Charter Question)
E	Legal Requirements	PRs related to legal requirements, in the broad sense, referring to statutes and treaties but not contracts
EA	Privacy & DP Law	PRs related to privacy and data protection law, including relevant aspects of human rights law and other sectoral statutes (eg. telecom law) (see "Privacy" Charter Question)
EB	IP Law	PRs related to IP and trademark law

EC	Jurisdiction Issues	PRs related to jurisdictional issues, cross border enforcement of law, etc.
ED	Free Expression	PRs related to the right of free expression, whether established in sectoral statutes or charters of rights.
F	Technical Requirements	PRs related to the technical requirements of the system and its various components (see "System Model" Charter Question)
G	Security Requirements	PRs related to security requirements, including technical and organizational security issues.
H	Confidentiality Requirements	PRs related to the duty of confidentiality and related issues, other than as required by data protection law (eg. could include policy and best practice)
I	ICANN Policies	PRs that relate to existing or desired ICANN policy writ large
IA	Policy Issues	PRs that relate to specific policy issues
IB	Registrar Transfer	PRs that relate to registrar transfer issues
IC	RPM	PRs that relate to rights protection measures specified by ICANN
ID	Privacy/Proxy	PRs that relate to the Privacy/Proxy services policy and associated issues
J	Contractual Issues	PRs that relate to contractual requirements and issues
K	Implementation Issues	PRs that relate to implementation issues associated with the RDS (see "Phase 3" for each Charter Question)
KA	Cost	PRs that relate to cost issues associated with the implementation of new or existing RDS policy (includes policy set through RAA) (see "Cost" Charter Question)
L	Abuse & Mitigations	PRs related to abuse issues and the mitigations deemed necessary
M	Risk	PRs related to a broad set of risks associated with the RDS, including anticipated change in policy (see "Risk" Charter Question)
MA	Registrants' Risk	PRs related to the risks of registrants
MB	Trademark & IP Owners' Risk	PRs related to the risks of trademark and IP owners
MC	Contracted Parties Risk	PRs related to the risks of contracted parties
MD	Governments Risk	PRs related to the risks of governments, notably LEAs

KEYWORD (K) COLUMN - Tags or keywords that can be FILTERED to group similar possible requirements into subsets.

The table below describes how proposed keywords were applied to group related possible requirements. Note that each possible requirement may be mapped to more than one keyword, and letters were assigned sequentially to keywords during mapping – for example, "aa" is not a subgroup of "a" - it is just the next letter assigned after "z." The PDP WG may refine or add to the initial keyword values below to examine new subsets.

	Keyword (K) Name	Keyword (K) Definition
a	Purpose	Any PR that describes a purpose for data in the RDS or why defining purpose is important
b	Contact Data for Technical Resolution	Any PR that describes how registration data is used for resolving a technical issue
c	Registration Data Query, Search and Disclosure	Any PR that describes searching for registration data
d	Policy Needs	Any PR that describes a possible registration data or directory policy (existing or future)
e	Identifying own Data & Access	Any PR that describes the need for registrants to review registrant's own information
f	Contact Data for other than Technical Resolution	Any PR that describes using contact information for reasons other than listed in B.
g	Proxy	Any PR that describes a need for or use of privacy proxy services or processes
h	Extensibility	Any PR that describes a need for RDS policies and implementation to be extensible
i	Research (other than for legal investigation)	Any PR that describes research of registration data for purposes other than legal investigations.
j	Legal Investigation	Any PR that describes research of registration data for legal investigations.
k	Registrar Transfer Policy	Any PR that describes policies for the inter-registrar transfer of registration data.
l	Consent	Any PR that describes to a need for a data subject's consent
m	Controller/Processor/Processing or Transfer of Data	Any PR that describes the obligations of a data controller or obligations of a data processor
n	Accuracy of Data	Any PR that describes the need for accurate registration data, validation policies or accuracy incentives
o	Retention of Data	Any PR that describes registration data retention needs or policies
p	Use of data for Surveillance	Any PR that includes the word "surveillance." (This WP 29 PR could be grouped with proportionality but I created this group due to the sensitivity of surveillance)
q	Law Enforcement Investigation	Any PR that contains the words "law enforcement authority" or "law enforcement access."
r	Proportionality of Use of Data	Any PR that refers to the word "Proportionality" or "proportional"

s	Gated Data Access	Any PR describes a need for controlled or restricted access to registration data.
t	Public Data Access	Any PR that describes a need for public (unrestricted) access to registration data.
u	Access Policies, including Authenticated Access	Any PR that describes policies that control registration data access and/or authentication for that access. (in reviewing anything that was mapped to U should be
v	Abuse	Any PR that contains the word “Abuse”
x	Encryption	Any PR that describes the need for registration data encryption or confidentiality
y	Internationalization	Any PR that describes the need for internationalization of the registration data (e.g., translation, transliteration)
z	Audit or Logging	Any PR that describes the need for auditing or logging of registration data collection, access, update, and use.
aa	Validation of Contact Data	Any PR that describes a need or policy for validating contact data
ab	Applicable Law	Any PR that describes any law or jurisdictional issue that may pertain to registration data or directory services.
ac	Certification Authority (or any third party that has duty to validate)	Any PR that describes a need for entities, including CA’s, to validate registrant contact data to provide an ancillary service that depends on trustworthy identities?
ad	Transparency	Any PR that describes a need for domain name registration transparency
ae	Validators	Any PR that describes a need for or obligations of a registration data validator
af	Contact Validation & Agreement	Any PR that describes how contact data is or may be validated and the associated contractual issues.
ag	Cost	Any PR that references the word “cost.”
ah	Unique Contact Data	Any PR that describes a need for unique contact data or associated policies.
ai	Synchronized	Any PR that describes a need for registration data synchronization
aj	Authoritative Data	Any PR that describes a policy or need for a definition of authoritative registration data
ak	Stability Data Elements	Any PR that describes a policy pertaining to stability or consistency in registration data access?
al	Display	Any PR that describes how registration data is displayed to users
am	Format	Any PR that describes a standard format for data elements
an	Account information that is not RDS Data Elements	Any PR that describes data in a domain name registrant’s account that is not (today) considered gTLD WHOIS registration data
ao	Registrar Data Elements	Any PR that describes the need or policy for data elements that are supplied by a registrar
ap	Nameserver Data Elements	Any PR that describes the need or policy for Nameserver data elements

aq	RPM	Any PR that describes the need or policy for Domain Name System Rights protection Mechanisms (RPM) as it relates to registration data
ar	Registrar Access	Any PR that describes the need or policy for registrar access to specific data elements.
as	Privacy/Control of Data	Any PR that describes the need or policy for registrant privacy and control of their own registration data.
at	Notice to Data Owner	Any PR that describes a need or policy for registrants to be notified of activity related to registration data.
au	Accountability for Use of Data	Any PR that describes a need or policy for some entity to be "accountable."
av	Terms & Conditions	Any PR that describes a need or policy for terms and conditions to be associated with registration data collection, maintenance, or access.
ax	Geographical Location of Data	Any PR that describes a need for RDS policy that takes the geographical location of data storage or data subject into consideration.
ay	Contract	Any PR that describes an existing or possible requirement imposed by a contract, including registrar agreements, registry agreements, and other contracts associated with registration data.
az	Responsibility of Domain Name Registrant	Any PR that describes responsibilities of domain name registrants.
ba	Right to Privacy	Any PR that refers to the registrant's "right of privacy."
bb	Aggregated Data	Applied to a PR taken from a WP29 document regarding use of aggregated data. Could be combined with another group but called out to ensure this somewhat unique PR would not be overlooked.