No.	Permissible Purposes Principles
1.	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.
2.	There must be clearly defined permissible/impermissible uses of the RDS.
3.	The RDS must support defined permissible purposes, including uses that involve: • Identifying the Registrant and contacts designated for a given purpose; • Communicating with contacts designated for a given purpose; • Using data published by Registries about Domain Names; and • Searching portions of registration data required for a given purpose.
4.	The RDS must be designed with the ability to accommodate new users and permissible purposes that are likely to emerge over time. • An application process must be defined. • Applications must be reviewed against defined criteria • Applications that pass review must be evaluated and approved by a multistakeholder review board as determined by a policy development process • Approved applications must be added to the RDS privacy policy and scheduled for implementation periodically (e.g., quarterly, annually) as defined by policy Note: See Section VI Data Elements for process to add new data elements.
5.	All identified permissible purposes should be accommodated by the RDS *in some manner*, with the exception of known malicious Internet activities that must be actively deterred. The EWG's recommended permissible purposes are summarized in Table 1, RDS Users and Purposes, and Figure 3, Permissible Purposes.
6.	gTLD registration data should 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.
7.	Every Registrant must have the ability to access all public and gated information published in the RDS about their domain name, including designated contact data.
No.	**Purpose-Based Contact Principles**
8.	At least one Purpose-Based Contact (PBC) must be provided for every registered domain name which makes public the union of all mandatory data elements for all mandatory PBCs. This PBC must be syntactically accurate and operationally reachable to meet the needs of every codified permissible purpose.
9.	During domain name registration, the Registrant's Contact ID[1] must be used as the default PBC ID for each purpose. The Registrant must be informed of all permissible purposes and given an opportunity to publish other PBC IDs for each purpose, including replacing the Registrant's Contact ID for any or all purposes.
10.	A Purpose-Based Contact does not have to be the Registrant, and access to the Registrant's information may be highly gated as per other policies. Note that a PBC does not necessarily represent a person but rather a designated point of contact for various purposes.

[1] Contact IDs are identifiers associated with blocks of contact data to enable retrieval and update, introduced in Section IV(a), Data Elements, and defined in Section V(d), Operational Framework for Contact IDs.

11.	A domain name must not be activated (put into the global DNS) until a valid PBC ID is provided for every applicable purpose. If a PBC 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 PBC ID update to occur. As per Principle #9 above, the Registrant's Contact ID must be used as the default PBC ID for each purpose. Failure to provide a valid PBC ID beyond that time could lead to suspension and/or deletion of the domain name in a codified process. (See Section V for Validation requirements.)
12.	PBC ID's can optionally be provided for every permissible purpose, with varying defined requirements for data elements that need to be collected and published for each type of PBC in order to fulfill the needs of associated permissible purposes.
13.	A process and policies must be developed enabling Registrant-designated contacts to opt-in/opt-out of having their Contact IDs published as PBC IDs 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.
14.	Any system for providing "Purpose-Based Contacts" must be flexible and allow for new purposes and contact types to be created and published in the RDS. (See Section III(c) for further detail about adding new purposes.)
No.	**Purpose-Based Contact Use Authorization Principles**
15.	Each PBC'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.
16.	Policies and processes must prevent unauthorized use of PBCs.
17.	Either the PBC or the Registrant must be able to rescind approval at a later time. (See Section V, Validation for details)
18.	Registrants must be able to easily designate themselves as PBC's for their domain names without external/third party approval.
No.	**Data Element Principles**
19.	The RDS must accommodate purpose-driven disclosure of data elements. (See Section III for a list of permissible purposes and associated Purpose-Based Contacts (PBCs).)
20.	Not all data collected is to be public; disclosure must depend upon Requestor and Purpose.
21.	Public access to an identified minimum data set must be made available, including PBC data published expressly to facilitate communication for this purpose.
22.	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 • Auditing/Compliance to ensure that gated access is not abused
23.	Only the data elements permissible for the declared purpose must be disclosed (i.e., returned in responses or searched by Reverse and WhoWas queries).
24.	The only data elements that must be collected are those with at least one permissible purpose.

25.	Each data element must be associated with a set of permissible purposes. • An initial set of acceptable uses, permissible purposes, and data element needs are identified by this report (see Section III and Annex D). • Each permissible purpose must be associated with clearly-defined data element access and use policies. • As specified in Section III, 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. • 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.
26.	The list of minimum data elements to be collected, stored and disclosed must be based on known use cases (reflected in this document) and a risk assessment (to be completed prior to RDS implementation).
27.	All Registries and Validators must store the full set of data elements that they collect/provide to the RDS. (See also Section VII, Possible RDS Models.)
No.	**Data Collection Principles**
28.	In support of the overarching legal principles given in Section VI, 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.[2]
29.	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, as follows: **Undeclared** – Applies by default if none of the following options are selected and shall be treated by the RDS in a manner similar to natural person. **Privacy/Proxy Provider** – Must be selected for domain names registered using an accredited Privacy/Proxy Provider. When selected, a Contact ID of an accredited Privacy/Proxy Provider must also be supplied to enable relay/reveal request escalation to the PP PBC. **Legal Person** – May be selected for domain names registered to entities that are NOT natural persons NOR proxy providers. When selected, a Contact ID of a designated Business PBC must also be supplied to facilitate consumer inquiries and complaints. (See note below this table.) **Natural Person** – May be selected for domain names registered to natural persons. When selected, neither Privacy/Proxy PBC nor Business PBC shall be defined, and

[2] There was near unanimous support for this text, with one EWG member dissenting.

	Registrant Name and addresses shall be treated as personal information in compliance with Data Protection laws applicable to the data subject's jurisdiction. e. Registrant Contact ID A unique ID assigned to each Registrant Contact [Name+Address] during validation (refer to Section V_Improving_Data_Quality for a more detailed definition of Contact ID and how it is created through a Validator and used for DN registration) f. Registrant Postal Address Includes the following data elements: 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)
30.	a. To improve both Registrant privacy and contactability, Registrars must collect and Registrants must provide Purpose-Based Contacts (PBCs) for every registered domain name. b. Registrants may optionally designate Privacy/Proxy-supplied PBCs or authorized third party PBCs for specified permissible purposes (see Section III). c. To meet the communication needs associated with each permissible purpose, PBCs created through a Validator and subsequently associated with a domain name must satisfy the following minimum mandatory data element requirements: Tech Contact: Email Address Admin Contact: Organization, Email Address Legal Contact: Organization, Email Address, Phone, Postal Address Abuse Contact: Email Address, Telephone Number Business Contact[3]: Organization, Postal Address Privacy/Proxy Provider Contact[4]: Organization, Email Address, Contact_URL, Abuse_URL d. If a Registrant does not designate a PBC for each mandatory permissible purpose, the Registrant's own Contact ID must be used by the default for those PBCs. (Note that the Registrant can avoid this by using an accredited Privacy/Proxy service, or by designating PBCs.) When the Registrant's Contact ID is used as a PBC ID, collection and disclosure requirements on the Registrant's data may be increased to satisfy the above-stated PBC mandatory data element needs.
31.	To avoid collecting more data than necessary, all other Registrant-supplied data not enumerated in principles #29 or 30 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.

[3] Contact is mandatory only if Registrant Type = Legal Person

[4] Contact is mandatory only if Registrant Type = Privacy Proxy Provider

32.	To maximize Internet stability, the following mandatory data elements must be provided by Registries and Registrars to the RDS: 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
33.	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.
34.	Validators, Registries and Registrars may collect, store, or disclose additional data elements for internal use that is never shared with the RDS.[5]
No.	**Data Disclosure Principles**
35.	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.
36.	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.
37.	To maximize reachability, all PBCs must be public by default. • Contact Holders[6] can opt into making any PBC data element gated, except those required to satisfy the designated purpose (further detailed in Table 5).

[5] Examples include the IP address used by the customer at the time of registration, a link to request generation of an EPP transfer key for a domain name, and payment data associated with the customer's account. Internal use data is not standardized by the RDS but rather privately defined by Registries and Registrars.

[6] Per Section III(g), RDS Contact Use Authorization, designated PBCs must authorize use of a Contact ID within a given domain name registration. In doing so, Contact Holders also agree to public/gated use of their data for that purpose. However, if a pre-validated PBC does not contain the mandatory/public data elements to meet a given purpose, that PBC cannot be designated for that purpose in a domain name registration.

38.	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 (further defined in Section V) 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)
39.	To balance simplicity and reachability, if a Registrant does not supply a mandatory PBC, the Registrant must be informed that his or her Contact ID will be used as that PBC, and Registrant data elements will be published as the domain name's Tech Contact, Admin Contact, Legal Contact, and Abuse Contact. The Registrant can avoid this disclosure by specifying one or more third party PBCs or by using an accredited Privacy/Proxy service (in which case those addresses will be supplied by the service provider).
40.	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.
No.	**Data Access Principles**
41.	A minimum set of data elements, at least in line with the most stringent privacy regime, must be accessible by unauthenticated RDS users.
42.	Multiple levels of authenticated data access must be supported, consistent with stated permissible purposes.
43.	RDS user access credentials must be tied to an auditable accreditation process, as further defined in Section IV(c), RDS User Accreditation.
44.	Access must be non-discriminatory (i.e., the process must create a level playing field for all requestors, within the same purpose).
45.	To deter misuse and promote accountability: • All data element access must be based on a stated purpose; • Access to gated data elements must be limited to authenticated requestors that assert a permissible purpose; and • Requestors must be able to apply for and receive credentials for use in future authenticated data access queries.
46.	Some type of accreditation must be applied to requestors of gated access: • When accredited Requestors query data, their purpose must be stated every time a request is made. • Different terms and conditions may be applied to different purposes. • If accredited requestors violate terms and conditions, penalties must apply.

47.	To raise the standard of gTLD registration data protection, all RDS queries/responses must make use of commonly-available message encryption and authentication measures to protect the confidentiality and integrity of data in transit.
48.	To meet the needs of authenticated RDS users with permissible purposes, the RDS 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.
49.	To meet the needs of authenticated RDS users with permissible purposes, the RDS 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 to the RDS.
50.	The RDS must support innovative services that make use of RDS data elements, as follows. • 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 RDS data use. • 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 RDS data use.
51.	All disclosures of gated data elements must occur through defined RDS access methods (including those described above). The entire RDS 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.
52.	Disclosures may occur through interactive display and other RDS access methods. • To make data easier to find and access in a consistent manner, a central point of access (e.g., web portal) must be offered. • Secure access to public data must be available to all requestors through an unauthenticated query method (at minimum, via secure website). • Secure access to gated data must be supported through secure web and other access methods and formats (e.g., RDAP xml responses, SMS, email), based on authenticated requestor and purpose. • Requestors must be able to obtain authoritative data from the RDS in real-time when needed. • The RDS must accommodate automation for large-scale lookups for various use cases and permissible purposes.
53.	To be truly global, the RDS must accommodate the display of registration data in multiple languages, scripts and character sets, including Internationalized domain names (IDNs).
54.	The RDS should support all future GNSO-defined transliteration policies for gTLDs.
55.	The RDS should enable collection and display of registration data elements in local languages.
No.	**RDS User Accreditation Principles**
56.	Non-accredited, unauthenticated access to non-gated (i.e., public) data must be possible in real-time.
57.	Accreditation of RDS Users for access to RDS data does not have to happen in real-time for all use cases and/or requesters.
58.	The RDS must only apply the minimum "accreditation scheme" necessary to provide RDS User access to gated data elements for the stated purpose.[7]

[7] For example, this accreditation does not need to require multi-factor, sworn statements, or need to serve as a be-all-and-end-all system to get most types of data.

59.	There must be no requirement to "pre-approve" or provide credentials to every potential user of the RDS. A request and fulfilment process can be created for each "type" of accredited RDS User (i.e., RDS User community).
60.	Accreditation for RDS users seeking access to data for permissible purposes could be granted in three ways. • None (i.e., unauthenticated access to public data only, as above). • Self-accreditation by the person/entity requesting the data, such as a system where the user simply states who they are, the data they are requesting and why, and then is granted access to that level of data. For example, this might apply to Registrants needing access to their own domain name's data for Domain Name Control purposes, where their self-attestation is tied to the actual registration of a domain name, qualifying them for credentials to access that information in the RDS. • Accreditation by some trusted third party (i.e., RDS User Accreditor, see principle #64 below).
61.	Whenever possible, any third party RDS accreditation process should leverage existing accreditation processes within each RDS user community identified in Section III as one that would need credentialing.
62.	These third party accreditation processes must be vetted by an authority responsible for implementing and enforcing RDS User Accreditation policy (for example, ICANN, a multistakeholder panel) and reviewed on a periodic basis.
63.	Any organization serving as an RDS User Accreditor must have a signed agreement with ICANN and/or the RDS 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.
64.	Accreditors may take on one or both of the following responsibilities. • An RDS User Accrediting Body may define and manage a user community, including establishing criteria for membership, setting credentialing requirements, and defining and enforcing its own terms and conditions of membership. • An RDS Users Accreditation Operator may offer a platform used by Accrediting Bodies, 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. A given Accreditor can, but is not required to, take on both responsibilities.
65.	Accreditors that wish to participate in handling RDS requests for data on behalf of their members may do so in two ways: • An Accreditor may provide proxied access to the RDS via their own authentication system and accept full responsibility for compliant usage. Although the Accreditor will be held accountable in the event of abuse, requests proxied through Accreditors in this manner must be authenticated in a way that enables auditing and abuse complaint resolution pertaining to an individual user's access. • An Accreditor may provide access to the RDS via their own authentication system, but simply relay authenticated requests to the RDS. Requests forwarded through the Accreditor in this manner must uniquely identify the RDS user, who is responsible for compliant usage and will be held directly accountable in the event of abuse.

66.	As defined in Section IV(b), Principle #50, the RDS must provide real-time access to credentialed requestors via multiple methods. Requests may be authenticated by the appropriate Accreditation Operator, and RDS access credentials issued during accreditation must be suitable for use with all defined access methods.[8]
67.	Best practices may be defined for credential management; Accreditors must be expected to adhere to best practices.
68.	The RDS must require individual credentials for authenticated access.
69.	Authenticated RDS access must not be transitive (i.e., an authenticated RDS user shall not share gated data with others outside of its accreditation).
70.	A process for responsible revelation of gated data to further the original purpose it was requested for must be created and enforced. (For example, enabling an IP Owner investigating trademark infringement to file a UDRP complaint, allowing an OpSec user investigating possible criminal activity to notify law enforcement.)
71.	An organization seeking access to RDS data could apply for RDS User accreditation and have all people using the RDS in their organization covered by that one accreditation.[9] Each such organization is responsible for managing accredited access within its own organization. Misuse of the system by members of an accredited RDS User organization would lead to sanctions against the organization as a whole.
72.	A single RDS user playing different roles may have multiple credentials in order to access different types of data for different purposes. However, it is highly desirable from a usability perspective to provide a single credential per RDS User that could be used for multiple purposes, as long as each purpose was stated per access as defined in Section IV(b).
73.	Audits and data analytics must be used to identify abuse of the system and access credentials.
74.	An appeals process must be defined to allow RDS users to refute abuse allegations when seeking to reactive/reinstate RDS access credentials.
75.	Every Registrant must receive a credential to be able to examine their own contact data as stored by the RDS in relation to domain names that are registered to them. (See Section III, Domain Name Control purpose.)
76.	A process for adding additional RDS User Accreditors that either supplement current processes or offer new, innovative ways to provide user accreditation for approved purposes of the RDS must be established. Such RDS User Accreditors must meet the minimum requirements as described in the principles enumerated here.
No.	**Principles for Contact IDs and Associated Data**
77.	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.
78.	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 RDS).[10]

[8] Authentication interfaces must be defined during implementation. For example, for some credential methods the RDS might use a standard framework such as the Security Assertion Markup Language (SAML) to enable authentication by the Accreditation Operator that issued that credential.

[9] It is up to the organization to ensure the integrity of any issued credentials for accessing the RDS.

[10] NOTE: Registrars can and are presumed likely to become accredited Validators in order to provide validation services for contacts associated with domain names they register.

79.	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.
80.	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.
81.	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 PBCs or Registrants must be developed to support this new paradigm.
82.	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 RDS data.
No.	**Principles for Interaction between Contact Holders and Validators**
83.	For any given Contact ID, a Contact Holder may choose any Validator[11].
84.	Oversight and accountability policies related to the management of Contact IDs must be developed.
85.	Contact Holders must be able to modify the contact information associated with a Contact ID through the issuing Validator.
86.	Validators must use Contact Holder authentication to deter unauthorized modification of contact information associated with a Contact ID.
87.	Validators may offer multiple levels of Contact Holder authentication, ranging from basic PIN authentication to two-factor authentication. 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.
88.	Validators must publish their policies on authentication in a manner that can be utilized globally for reputation management. This will encourage better accuracy and accountability for listed contact information.
89.	Validators must be able to validate contact information submitted in the Contact Holder's native language. This should improve accuracy of native-language data and support scalability of the domain name registration system into a multi-lingual environment. For example, Registrars could work with Validators in various localities to provide expanded validation services to large numbers of Registrants and designated contacts without having to invest in costly tools to validate data in languages unfamiliar to their own staff.
No.	**Principles for Contact Validation**
90.	All contact data elements associated with a Contact ID must be validated at a syntactic level. This represents a base-level of validation that must be achievable by any entity in the industry.
91.	All mandatory contact data elements associated with a Contact ID for a particular purpose must be validated operationally[12] before that Contact ID can be included in domain name registration data for that purpose.

[11] Per principle #88, Contact IDs identify both the Validator and the Contact Holder. This should be implemented in a way that enables Contact ID portability between Validators.

[12] Refer to SAC 058 and *ccTLD WHOIS Data Verification/Validation Survey Results Summary* for possible ways to implement operational validation and existing ccTLD practices.

92.	A Contact Holder may 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)[13].
93.	Given costs involved with optional identity validation, a low-cost mechanism for economically disadvantaged Contact Holders to receive optional identity validation is desirable.
94.	In order to preserve associations and allow for a correction process, a Contact ID can have a status of "inaccurate" and remain in the system.
95.	Validation Status of the Contact ID must be tracked and published as appropriate when accessing RDS information, along with the most recent time the validation status was determined.
96.	Third parties may file inaccuracy reports to challenge the Validation Status of a Contact ID as described in Section V(c), triggering a standard remediation process that may result in the Contact ID being flagged as "inaccurate" and in further consequences for domain names using that Contact ID as a PBC.
97.	Active domains cannot have a mandatory contact with an "inaccurate" status without some sort of remediation. The scheme can be determined elsewhere, however.
98.	A minimum level of cross-field validation must be checked for all contact data elements associated with Contact IDs where cross-field validation is applicable (e.g. physical address).
99.	Revalidation of contact data must be carried out on a regular basis by the applicable Validator to ensure data is accurate at the declared level.
100.	If a Contact Holder provides optional data elements, those elements must be at least syntactically validated. Optional data elements would not be validated beyond syntax unless the Contact requests and presumably pays any costs associated with such validation.
101.	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. For example, elements like email, phone, and address could be operationally-validated, while a name or organization name could not be operationally-validated but could optionally be identity-validated.
102.	In addition, the Validator must determine and publish as an RDS data element the overall validation status achieved by each Contact ID. For example, if ALL mandatory data elements that can be operationally-validated pass those checks, the Contact's overall validation status would be "operationally validated." If ANY mandatory data element that can be operationally-validated fails, the Contact's overall validation status would be down-graded to "syntactically validated." If ALL mandatory data elements that can be identity-validated pass that optional check, that Contact's overall validation status would be upgraded to "identity validated." To promote accuracy and efficient communication, this overall validation status must be made available to RDS users as one new consolidated data element per Contact.[14]

[13] For example, optional identity validation could be a separately-priced add-on or bundled into domain name registration packages or offered as an incentive to high-volume customers. Refer to *RFI on Contact Data Validation and Verification Systems* for examples of commercial services that perform such validation.

[14] The EWG also considered publishing RDS data elements to convey the individual validation status of each individual contact data element (e.g., PBC email address status = operationally-validated, PBC name status = identity-validated). Publishing validation status at this granularity would require significant protocol, data element, and client application/GUI changes and so is not recommended at this time, but may warrant further study.

103.	For any data element that has undergone validation, the timestamp of that validation must also be recorded and maintained by the Validator.
104.	The timestamp of the most recent change to the overall validation status for an entire Contact ID must be also be determined by the Validator and published as a new RDS data element per Contact.
No.	**Data Protection Principles**
105.	Mechanisms must be adopted to facilitate routine legally compliant data collection and transfer between actors within the RDS ecosystem.
106.	Standard contract clauses that are harmonized with privacy and data protection laws should be codified in a policy and enforced through contracts between all RDS ecosystem actors involved in handling personal information.
107.	An information system to apply data protection laws (i.e., a "rules engine") and localization of RDS 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 RDS ecosystem.
No.	**Law Enforcement Access Principles**
108.	The RDS must store data in jurisdiction(s) where law enforcement is globally trusted, regardless of implementation model.
No.	**Contractual Relationship Principles**
109.	A third party provider that is a non-governmental organization with global scope should operate the RDS.
110.	ICANN must enter into appropriate contracts with the third party provider of the RDS to enable availability, auditing and compliance.
111.	ICANN must enter into appropriate contracts with Validators, Privacy/Proxy Service Providers, Secured Credential Approvers, and others that may interact with the RDS (see Section III(c) Principle #1).
112.	ICANN must amend existing agreements (RAA, Registry Agreements) to accommodate the RDS and eliminate legacy requirements.
113.	The RDS must apply to all gTLD Registries, whether existing, or new. No grandfathering or special exemptions should be allowed.
No.	**Accountability and Audit Principles**
114.	All entities within the RDS ecosystem must be held accountable for one or more of the requirements set forth in Table 6: a) provide accurate and reliable registration information b) use the information only for the designated purpose c) secure the information collected, stored, or forwarded d) validate or authenticate the information when collected e) update previously provided information in a timely manner f) enforce RDS privacy policies and Terms of Use (ToU) g) detect abuse of registration information h) address and track complaints i) comply with established ToU and ToS policies j) establish mechanisms to deter third party data harvesting and bulk fraudulent account creation k) establish an on-going auditing and remediation process

	The following stakeholders[15] have accountability roles in the RDS ecosystem: a) RDS Users Seeking Data (USDs) - enumerated in Section III b) Registrants c) Registrars[16] d) Registries[17] e) Registration Directory Service Provider f) ICANN g) Privacy or Proxy Service Providers h) Secure Protected Credential Approver i) Validators j) RDS User Accreditors k) Purpose-Based Contacts l) Escrow Providers
115.	The RDS must establish procedures for handling complaints about unavailability of data, improper use of data, unauthorized access to data, privacy policy breaches, and inaccurate data entry; for example: Abuse Contact data elements, and a portal to capture complaints from USDs and Registrants.
116.	The RDS must establish escalated remedies for inaccurate data; for example: Email Warning, user/browser-visible Flag on Records, ICANN Compliance action, and other new incentives to encourage accuracy. (See Section V Improving Data Quality for accuracy requirements.)
117.	The RDS must establish escalated remedies for unauthorized access to data; for example: Email Warning, Rate Limiting, Temporary Blocking, Accreditation Suspension, Termination, and other deterrents. (See Section IV Improving Accountability for gated access requirements.)
118.	The RDS must establish escalated remedies for improper use of data; for example: Email Warning, Rate Limiting, Temporary Blocking, Accreditation Suspension, Termination, and other disincentives. (See Section III Users and Purposes for permissible purposes.)
119.	The RDS must establish audit mechanisms in order to detect abuse of RDS Access Credentials and ToU violations; for example: mechanisms to detect unusual behaviour patterns. (See Section IV Improving Accountability for RDS User Accreditation requirements.)
120.	The RDS must establish audit mechanisms in order to detect abuse of registration data for uses other than stated purposes; for example: mechanisms to detect unusual behaviour patterns. (See Section III Users and Purposes.)
121.	The RDS must establish audit mechanisms in order to detect abuse by Validators; for example: training of Validators, periodic random sampling of data to be checked to ensure proper validation. (See Section V Improving Data Quality)
122.	The RDS must establish audit mechanisms in order to detect abuse by RDS User Accreditors; for example: establish mechanisms to detect unusual behaviour patterns. (See Section IV Improving Accountability for definition of abuses.)
123.	The RDS must establish audit mechanisms in order to detect abuse by Privacy/Proxy Providers and Secure Credential Approvers; for example: establish mechanisms to detect unusual behaviour patterns. (See Section VI Improving Registrant Privacy for definition of abuses).

[15] These roles and responsibilities extend to stakeholder agents, and assigns (e.g., Resellers)

[16] As defined by http://www.icann.org/en/resources/registrars/raa/approved-with-specs-27jun13-en.htm

[17] As defined by http://newgtlds.icann.org/en/applicants/agb/agreement-approved-09jan14-en.pdf

124.	RDS USDs must agree to the auditing of data access, use and provision of accurate identity and purpose information in Terms of Use (ToU).
125.	The RDS must establish a process for remediation, suspension or termination of Validators if data is not properly validated, stored and secured. (See Section V Improving Data Quality for VR requirements.)
126.	The RDS must establish a process for remediation, suspension or termination of Secure Credential Approvers if vetting is not proper or adequate. (See Section VII Improving Registrant Privacy for requirements.)
127.	The RDS must establish a process for remediation, suspension or termination of RDS User Accreditors if USDs are not properly accredited, stored and secured. (See Section IV Improving Accountability for RDS User Accreditor requirements.)
128.	ICANN must establish ToS policies for ensuring the Registries, Registrars, and Validators provide accurate, updated and timely data to the RDS. (See Section VI Legal and Contractual Considerations for RDS and Registry requirements, to be reflected in the RIA and RAA.)
129.	The RDS must establish an audit process for Registries, Registrars, and Validators and a process for reporting to ICANN if the Registry/Registrar/Validator is not providing accurate, updated and timely data. (See Section VI Legal and Contractual Considerations for RDS and Registry requirements, to be reflected in the RIA and RAA.)
130.	The RDS must establish audit mechanisms to ensure the ongoing quality and integrity of the data collected by the RDS and stored with the Escrow Provider. (See Section VIII Data Storage Escrow and Logging)
131.	ICANN must establish audit mechanisms in order to detect breaches of any ToCs by the RDS Provider. For example: allows unauthorized use of data, does not respond to complaints concerning abuse of data, abuse of credentials or abuse of validation. (See Section VI Legal and Contractual Considerations)
132.	ICANN must establish a process for remediation, suspension or termination of the RDS Provider if not fulfilling contractual responsibilities. For example: availability, reliability, privacy, access rights, and performance requirements. (See Section VI Legal and Contractual Considerations)
133.	ICANN must define and benchmark annual improvements made towards achieving the major goals of the RDS: (I) improved data quality, (ii) improved accountability, (iii) improved privacy. The RDS must demonstrate sustained progress in all three areas at similar rates, with a process to identify and remediate unforeseen problems that cause any area to improve more slowly than the others.
No.	**Privacy Principles**
134.	In addition to the privacy afforded by compliance with data protection laws, the RDS 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.
135.	There must be accreditation for Privacy/Proxy service providers and rules regarding the provision and use of accredited Privacy/Proxy services.
136.	Outside of domain names registered via accredited Privacy/Proxy services, all Registrants must assume responsibility for the domain names they register.

137.	ICANN must investigate the development of a single, harmonized privacy policy which governs RDS activities in a comprehensive manner, as discussed below.
No.	**Accredited Privacy/Proxy Services Principles**
	General
138.	ICANN must accredit Privacy and Proxy service Providers[18].
139.	At minimum, the accreditation program must continue the Privacy/Proxy commitments under the 2013 RAA Specification.
	Principles for Accredited Privacy Services
140.	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).
141.	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.
142.	Accredited Privacy services must provide the Registrar (using a PBC created through a Validator) 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.
143.	Accredited Privacy services must be obligated to relay emails received by the Registrant's forwarding email address to the Registrant.
	Principles for Accredited Proxy Services
144.	Entities and natural persons may register domain names using accredited proxy services that register domain names on behalf of the Proxy service customer.
145.	Accredited Proxy service providers must provide the Registrar (using a PBC created through a Validator) 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.
146.	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.
147.	Accredited Proxy services must provide the Registrar (using a PBC created through a Validator) 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.
148.	Accredited Proxy services must be obligated to relay emails received by the Registrant's forwarding email address as further described in Annex H.
149.	Accredited Proxy services must be obligated to respond to reveal requests in a timely manner as outlined in the escalation procedures described in Annex H.

[18] The GNSO has formed a working group to develop policies for Privacy/Proxy Service Accreditation. The EWG recommends that the RDS reuse any foundation established by the PPSAI WG, modified as needed to reflect RDS access methods and data elements – most notably, P/P published Purpose-Based Contacts.

No.	Principles for Secure Protected Credentials
150.	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.
151.	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.
152.	ICANN must facilitate the development or licensing of a Secure Credential Issuer that recognizes SCA approvals and generates corresponding Secure Credentials.
153.	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 RDS. No data about the at-risk entity using the secure credential-registered domain name would be known to the RDS, and some system of anonymous or proxy payment would have to be used.
154.	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.
155.	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 could be considered to mitigate risk.
156.	Policies and processes must be established for secure protected credential application approval and revocation. • The approval process must allow for zero or more attestors to sufficiently shield the at-risk entity's identity and location from the trusted Secure Credential Recipient that presents the application to the SCA. The number and identity of attestors is transparent to the RDS; the only party that directly interfaces with the SCA is the Secure Credential Recipient. • The revocation process must allow for similar shielding of the at-risk individual's identity and location while enforcing secure credential terms of service. The SCA must be accountable for investigating alleged DNS abuses involving secure credentials and enforcing Terms of Service. In the case of DNS abuse severe enough to warrant credential revocation, the SCA shall hold the Secure Credential Recipient accountable.
No.	**Model Design Principles**
157.	**Collection:** Today, Registrars or Registrar's Affiliates collect and store registration information from their own customers (Registrants). This process is inherently distributed. In addition to continuing to collect registration data from Registrants by Registrars or Affiliates, the EWG proposes collection of contact data by Validators.
158.	**Storage:** Multiple possible models exist for storing registration information across all gTLDs. The EWG identified several possible models, pinpointed two that appeared to be most promising, and chose one recommended model by applying the evaluation criteria reflected in Annex F.

159.	**Access:** To protect data subject privacy, a centralized interface must enable appropriate requestors to access registration information across all gTLDs, including unauthenticated public data access by anyone and authenticated gated data access by accredited users.
160.	**Protocol:** The RDS must use RDAP[19] or EPP (as appropriate for each interface) as the underlying directory access protocol to obtain registration information from storage locations, wherever that may be.
No.	Common Requirements for Storage, Escrow, and Logging
161.	Location, retention, privacy, and access policies must be developed.
162.	Storage, escrow, and logging policies and implementations must comply with local and international laws.
	Storage Principles
163.	To maintain redundant systems and eliminate the single point of failure, the data must reside at multiple locations (i.e., Validator, Registrar, Registry, Escrow Provider, and RDS Provider).
164.	Consistency must be maintained when data exists in multiple places.
165.	The RDS must maintain the data elements in a secure fashion, protecting the confidentiality and integrity of the data elements that are at risk from unauthorized disclosure or use.
166.	Transaction data must be stored indefinitely to maintain an accurate record of data changes over time and support WhoWas functionality, but no longer than limits (if any) required for compliance with applicable data protection laws. Orphaned contact information should also be purged periodically, in accordance with laws (e.g., one year after disassociation).
	Escrow[20] Principles
167.	Audits must be conducted of escrow data to test the format, integrity, and completeness of deposits.
168.	Escrow and audit of escrow may be easier to coordinate with a synchronized RDS model.
169.	Escrow data itself must be encrypted and opaque to auditors.
170.	Escrow data must be retained for a period of time that is consistent with the requirements of the Registrar Accreditation Agreement, individual gTLD Registry Agreements, and applicable data protection laws. Currently, this would be for the duration of the publishing entity's sponsorship of the data and for a period of two additional years thereafter or longer if required by the gTLD Registry Agreement, but no longer than the maximum allowed by law.
	Logging Principles
171.	RDS queries must be logged to provide records of how the system is used.
172.	Log aggregation may be needed to detect abuse directed at distributed systems.
173.	Changes must be logged to provide data element history over time.
174.	Access to operational RDS logs must be restricted to those trusted, authenticated, authorized individuals and entities with a specific purpose and "need to know." This must include authorized operators of the RDS itself (to confirm and trouble-shoot proper RDS operation) and authorized data protection entities (to monitor RDS compliance with data protection legislation.) (See also Section VIII(b), Law Enforcement Access.)

[19] http://tools.ietf.org/html/draft-ietf-weirds-rdap-query-02

[20] Escrow refers to encrypted system backup to a trusted third party (Escrow Provider) for purposes of recovery in the event of disaster, system failure, etc. Refer to the RAA for further details.

No.	Cost Principles
175.	Unauthenticated (non-gated) access to public data elements must be free.
176.	Authenticated (gated) access by law enforcement to authorized data elements (subject to due process) may be subject to special cost consideration.
177.	RDS design should strive for cost-efficiency and minimization, without compromising other goals.
178.	RDS should operate on a cost-recovery model.
179.	To facilitate migration from WHOIS, an RDS software development platform should be created and funded by ICANN to minimize RDS implementation costs on Registrars/Registries, Validators and RDS User Accreditors.
180.	Provision of this software development platform should not be unduly burdensome on other RDS users.