# Proposed Temporary Specification for gTLD Registration Data – WORKING DRAFT

(Revised – as of 14 May 2018)
Prepared by: ICANN organization

The General Data Protection Regulation (GDPR) was adopted by the European Union (EU) in April 2016 and takes full effect on 25 May 2018 across the EU countries. Over the past year, ICANN organization (ICANN org) has consulted with contracted parties, European data protection authorities, legal experts, and interested governments and other stakeholders to understand the potential impact of the GDPR to Personal Data that is Processed by certain participants in the gTLD domain name ecosystem (including Registry Operators and Registrars) pursuant to ICANN policies and contracts between ICANN and such participants that are subject to the GDPR.

This Temporary Specification for gTLD Registration Data (Temporary Specification) establishes temporary requirements to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR. Consistent with ICANN's stated objective to comply with the GDPR, while maintaining the existing WHOIS system to the greatest extent possible, the Temporary Specification maintains robust collection of Registration Data (including Registrant, Administrative, and Technical contact information), but restricts most Personal Data to layered/tiered access. Users with a legitimate and proportionate purpose for accessing the non-public Personal Data will be able to request such access through Registrars and Registry Operators. Users will also maintain the ability to contact the Registrant or Administrative and Technical contacts through an anonymized email or web form. The Temporary Specification shall be implemented where required by the GDPR, while providing flexibility to Registry Operators and Registrars to choose to apply the requirements on a global basis based on implementation, commercial reasonableness and fairness considerations. The Temporary Specification applies to all registrations, without requiring Registrars to differentiate between registrations of legal and natural persons. It also covers data processing arrangements between and among ICANN, Registry Operators, Registrars, and Data Escrow Agents as necessary for compliance with the GDPR.

This Temporary Specification was adopted by resolution of the ICANN Board of Directors (ICANN Board) on [TBD], pursuant to the requirements for the establishment of Temporary

Policies and Temporary Specification or Policies (as such terms are defined in ICANN's registry agreements and registrar accreditation agreements). An advisory statement containing a detailed explanation of the ICANN Board's reasons for adopting this Temporary Specification is available here <<TBD>>.

## Table of Contents

# 1. Scope

1.1. Terms used in this Temporary Specification are defined in Section 2.

1.2. This Temporary Specification applies to all gTLD Registry Operators and ICANN-accredited Registrars.

1.3. The requirements of this Temporary Specification supersede and replace the requirements contained in Registry Operator's Registry Agreement and Registrar's Registrar Accreditation Agreement regarding the matters contained in this Temporary Specification. To the extent there is a conflict between the requirements of this Temporary Specification and the requirements of Registry Operator's Registry Agreement and Registrar's Registrar Accreditation Agreement, the terms of this Temporary Specification SHALL control, unless ICANN determines in its reasonable discretion that this Temporary Specification SHALL NOT control.

# 2. Definitions and Interpretation

The terms "MAY", "MUST", "MUST NOT", "REQUIRED", "RECOMMENDED", "SHALL", "SHALL NOT", "SHOULD NOT" and "SHOULD" are used to indicate the requirement level in accordance with RFC 2119, which is available at http://www.ietf.org/rfc/rfc2119.txt.

"Consent", "Controller", "Personal Data", "Processing", and "Processor" SHALL have the same definition as Article 4 of the GDPR.

"gTLD" SHALL have the meaning given in the Registrar Accreditation Agreement.

"Interim Model" means the Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation published at https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf and as may be amended from time to time.

"Registered Name" SHALL have the meaning given in the Registrar Accreditation Agreement.

"Registered Name Holder" SHALL have the meaning given in the Registrar Accreditation Agreement.

"Registrar Accreditation Agreement" means any Registrar Accreditation Agreement between a Registrar and ICANN that is based on that certain 2013 Registrar Accreditation Agreement approved by the ICANN Board on June 27, 2013 ("2013 Registrar Accreditation Agreement") or any successor to such agreements that is approved by the ICANN Board.

"Registration Data" means data collected from a natural and legal person in connection with a domain name registration.

"Registration Data Directory Services" refers to the collective of WHOIS, Web-based WHOIS, and RDAP services.

"Registry Agreement" means any gTLD registry agreement between Registry Operator and ICANN, including any Registry Agreement that is based on the new gTLD Registry Agreement approved by the ICANN Board on 2 July 2013, as amended ("Base Registry Agreement").

If a term is capitalized but not defined in this Temporary Specification, such term SHALL have the meaning given to it in the Registry Agreement or Registrar Accreditation Agreement, as applicable.

Unless otherwise specifically provided for herein, the term "or" SHALL NOT be deemed to be exclusive.

When Registry Operator and Registrar are referenced together in a provision of this Temporary Specification, each such provision represents a separate requirement and obligation of each Registry Operator and each Registrar pursuant to its respective Registry Agreement or Registrar Accreditation Agreement.

## 3. Policy Effective Date

This Temporary Specification is effective as of _____.

## 4. Lawfulness and Purposes of Processing gTLD Registration Data

4.1. ICANN's mission, as set forth in Bylaws Section 1.1(a), is to "coordinate the stable operation of the Internet's unique identifier systems." Section 1.1 (a) describes in specificity what this mission entails in the context of names. While ICANN's role is narrow, it is not limited to technical stability. Specifically, the Bylaws provide that ICANN's purpose is to coordinate the bottom-up, multistakeholder development and implementation of policies "[f]or which

uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS including, with respect to gTLD registrars and registries" [Bylaws, Section 1.1(a)(i)], which is further defined in Annex G-1 and G-2 of the Bylaws to include, among other things:

- resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names);
- maintenance of and access to accurate and up-to-date information concerning registered names and name servers;
- procedures to avoid disruptions of domain name registrations due to suspension or termination of operations by a registry operator or a registrar (e.g., escrow); and
- the transfer of registration data upon a change in registrar sponsoring one or more registered names.

4.2. The Bylaws articulate that issues surrounding the provision of Registration Data Directory Services (RDDS) by Registry Operators and Registrars are firmly within ICANN's mission. The Bylaws provide further insight into the legitimate purposes designed to be served by RDDS. For example, the Bylaws specifically obligate ICANN, in carrying out its mandate, to "adequately address issues of competition, consumer protection, security, stability and resiliency, malicious abuse issues, sovereignty concerns, and rights protection" [Bylaws Section 4.6 (d)]. While ICANN has neither the authority nor expertise to enforce competition or consumer protection laws, and is only one of many stakeholders in the cybersecurity ecosystem, the provision of RDDS for legitimate and proportionate uses is a critical and fundamental way in which ICANN addresses consumer protection, malicious abuse issues, sovereignty concerns, and rights protection – enforcing policies that enable consumers, rights holders, law enforcement and other stakeholders to access the data necessary to address and resolve uses that violate law or rights.

4.3. Accordingly, ICANN's mission directly involves facilitation of third party Processing for legitimate and proportionate purposes related to law enforcement, competition, consumer protection, trust, security, stability,

resiliency, malicious abuse, sovereignty, and rights protection. ICANN is required by Section 4.6(e) of the Bylaws, subject to applicable laws, to "use commercially reasonable efforts to enforce its policies relating to registration directory services," including by working with stakeholders to "explore structural changes to improve accuracy and access to generic top-level domain registration data," "as well as consider[ing] safeguards for protecting such data." As a result, ICANN is of the view that the collection of Personal Data (one of the elements of Processing) is specifically mandated by the Bylaws. In addition, other elements of the Processing Personal Data in Registration Data by Registry Operator and Registrar, as required and permitted under the Registry Operator's Registry Agreement with ICANN and the Registrar's Registrar Accreditation Agreement with ICANN, is needed to ensure a coordinated, stable and secure operation of the Internet's unique identifier system.

4.4. However, such Processing must be in a manner that complies with the GDPR, including on the basis of a specific identified purpose for such Processing. Accordingly, Personal Data included in Registration Data may be Processed on the basis of a legitimate interest not overridden by the fundamental rights and freedoms of individuals whose Personal Data is included in Registration Data, and only for the following legitimate purposes:

4.4.1. Reflecting the rights of a Registered Name Holder in a Registered Name and ensuring that the Registered Name Holder may exercise its rights in respect of the Registered Name;

4.4.2. Providing access to accurate, reliable, and uniform Registration Data based on legitimate purposes not outweighed by the fundamental rights of relevant data subjects, consistent with GDPR;

4.4.3. Enabling a reliable mechanism for identifying and contacting the Registered Name Holder for a variety of legitimate purposes more fully set out below;

4.4.4. Enabling a mechanism for the communication or notification of payment and invoicing information and reminders to the Registered Name Holder by its chosen Registrar;

4.4.5. Enabling a mechanism for the communication or notification to the Registered Name Holder of technical issues and/or errors with a

Registered Name or any content or resources associated with such a Registered Name;

4.4.6. Enabling a mechanism for the Registry Operator or the chosen Registrar to communicate with or notify the Registered Name Holder of commercial or technical changes in the domain in which the Registered Name has been registered;

4.4.7. Enabling the publication of technical and administrative points of contact administering the domain names at the request of the Registered Name Holder;

4.4.8. Supporting a framework to address issues involving domain name registrations, including but not limited to: consumer protection, investigation of cybercrime, DNS abuse, and intellectual property protection;

4.4.9. Providing a framework to address appropriate law enforcement needs;

4.4.10. Facilitating the provision of zone files of gTLDs to Internet users;

4.4.11. Providing mechanisms for safeguarding Registered Name Holders' Registration Data in the event of a business or technical failure, or other unavailability of a Registrar or Registry Operator;

4.4.12. Coordinating dispute resolution services for certain disputes concerning domain names; and

4.4.13. Handling contractual compliance monitoring requests, audits, and complaints submitted by Registry Operators, Registrars, Registered Name Holders, and other Internet users.

4.5. In considering whether Processing of Personal Data contained in Registration Data is consistent with Article 6(1)(f) of the GDPR[1], the GDPR requires ICANN to balance the legitimate interests described above with the interests, rights, and freedoms of the affected data subject. ICANN finds that the Processing is proportionate for the following reasons:

[1] Article 6(1)(f) of the GDPR permits Processing where "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data…."

4.5.1. The Processing of the limited Personal Data identified in this Temporary Specification is necessary to achieve the legitimate interests identified, as documented in many stakeholder comments and submissions over the course of a 12-month community consultation. This Processing specifically includes the retention of Personal Data already collected and the ongoing collection of Personal Data;

4.5.2. The tiered/layered access framework for RDDS identified in the Interim Model, and implemented in this Temporary Specification, is specifically designed to minimize the intrusiveness of Processing while still permitting necessary Processing;

4.5.3. Processing under the tiered/layered access framework as required by this Temporary Specification minimizes the risk of unauthorized and unjustified Processing;

4.5.4. This Temporary Specification contains requirements to ensure that Registered Names Holders are notified about the contemplated Processing and about their rights with respect to such Processing;

4.5.5. This Temporary Specification contains requirements to ensure that appropriate records of Processing activities will be maintained to meet the accountability obligations set forth in the GDPR.

# 5. Requirements Applicable to Registry Operators and Registrars

5.1. **Publication of Registration Data**. Registry Operator and Registrar MUST comply with the requirements of, and MUST provide public access to Registration Data in accordance with, Appendix A attached hereto ("**Appendix A**").

5.2. **Registrar and Registry Operator Service Level Agreement**. Registry Operator and Registrar MUST comply with the additional requirements and the updated Registration Data Directory Services Service Level Agreements set forth in Appendix B attached hereto ("**Appendix B**").

5.3. **Data Escrow**. Registry Operator and Registrar MUST comply with the additional requirements concerning Registration Data escrow procedures set forth in Appendix C attached hereto ("**Appendix C**").

5.4. **Data Processing Requirements**. Registry Operator and Registrar MUST comply with the requirements of, and MUST Process Personal Data in accordance with the terms and conditions set forth in Appendix D attached hereto ("**Appendix D**").

5.5. **International Data Transfers between Registry Operator, Registrar, and ICANN**. In the course of performing the requirements under this Temporary Specification, the Registry Agreement, and Registrar Accreditation Agreement, Registry Operator, Registrar and/or ICANN MAY be required to transfer Personal Data to a country that is not deemed adequate by the European Commission per Article 45(1) of the GDPR. In such a case, ICANN, Registry Operator, and/or Registrar MUST transfer Personal Data on the basis of adequate safeguards permitted under Chapter V of the GDPR, including the use of Standard Contractual Clauses (2004/915/EC) (or its successor clauses), and ICANN, Registry Operator and/or Registrar MUST comply with such appropriate safeguards.

5.6. **Uniform Rapid Suspension (URS)**. Registry Operator and Registrar MUST comply with the additional requirements for the 17 October 2013 URS High Level Technical Requirements for Registries and Registrars set forth in Appendix E attached hereto ("**Appendix E**").

5.7. **ICANN Contractual Compliance**. Registry Operator and Registrar MUST provide reasonable access to Registration Data to ICANN upon reasonable notice and request from ICANN for the purpose of investigating compliance-related inquiries and enforcement of the Registry Agreement, Registrar Accreditation Agreement, and ICANN Consensus Policies.

## 6. Requirements Applicable to Registry Operators Only

6.1. **Bulk Registration Data Access to ICANN**. Registry Operator MUST comply with, and MUST provide ICANN with periodic access to Registration Data in accordance with Appendix G attached hereto ("**Appendix G**").

6.2. **Registry Monthly Reports**. Registry Operator MUST comply with the additional requirements for Registry Monthly Reports as set forth in Appendix H attached hereto ("**Appendix H**").

6.3. **Registry-Registrar Agreements**.

6.3.1. Registry Operator MUST include Processing provisions in its Registry-Registrar Agreement with Registrar concerning the handling of Personal Data in a manner that complies with Article 28 of the GDPR.

6.3.2. Registry Operator MAY amend or restate its Registry-Registrar Agreement to incorporate data Processing terms and conditions substantially similar to the requirements provided at <<https://www.icann.org/resources/pages/gtld-registration-data-specs-en>> without any further approval of ICANN, provided that Registry Operator MUST promptly deliver any such amended or restated Registry-Registrar Agreement to ICANN. Upon ICANN's receipt thereof, such amended or restated Registry-Registrar Agreements will be deemed to supplement or replace, as applicable, the approved Registry-Registrar Agreement that is attached as an appendix (if any) to Registry Operator's Registry Agreement.

# 7. Requirements Applicable to Registrars Only

7.1. **Notices to Registered Name Holders Regarding Data Processing**. Registrar SHALL provide notice to each existing, new or renewed Registered Name Holder stating:

7.1.1. The specific purposes for which any Personal Data will be Processed by the Registrar;

7.1.2. The intended recipients or categories of recipients of the Personal Data (including the Registry Operator and others who will receive the Personal Data from Registry Operator);

7.1.3. Which data are obligatory and which data, if any, are voluntary;

7.1.4. How the Registered Name Holder or data subject can access and, if necessary, rectify Personal Data held about them;

7.1.5. The identity and the contact details of the Registrar (as controller) and, where applicable, of the Registrar's representative in the European Economic Area;

7.1.6. The contact details of Registrar's data protection officer, where applicable;

7.1.7. The specified legitimate interest for Processing under Article 6(1)(f) of the GDPR;

7.1.8. The recipients or categories of recipients of the Personal Data, if any;

7.1.9. Where applicable, the fact that the Registrar intends to transfer Personal Data: (i) to a third country or international organization and the existence or absence of an adequacy decision by the Commission; or (ii) in the case of transfers referred to in Articles 46 or 47 of the GDPR, or the second subparagraph of Article 49(1) of the GDPR, reference to the appropriate or suitable safeguards and how to obtain a copy of them or where they have been made available.

7.1.10. The period for which the Personal Data will be stored, or if it is not possible to indicate the period, the criteria that will be used to determine that period;

7.1.11. The existence of the right to request from the Registrar access to, and rectification or erasure of Personal Data, or restriction of Processing of Personal Data concerning the Registered Name Holder or data subject, or to object to Processing, as well as the right to data portability;

7.1.12. Compliance with Article 6(1)(a) and Article 9(2)(a) of the GDPR, where the Registrar relies on consent of the Registered Name Holder for Processing;

7.1.13. The right of the Registered Name Holder or data subject to lodge a complaint with a relevant supervisory authority;

7.1.14. Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Registered Name Holder is obliged to provide the Personal Data, and the possible consequences of failure to provide such Personal Data; and

7.1.15. The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the data subject.

The requirements of this Section 7.1 shall supersede and replace the requirements of Section 3.7.7.4 of the Registrar Accreditation Agreement.

7.2. **Additional Publication of Registration Data.**

7.2.1. As soon as commercially reasonable, Registrar MUST provide the opportunity for the Registered Name Holder to provide its Consent to publish the additional contact information outlined in Section 2.3 of Appendix A for the Registered Name Holder.

7.2.2. Registrar MAY provide the opportunity for the Admin/Tech and/or other contacts to provide Consent to publish additional contact information outlined in Section 2.4 of Appendix A.

7.2.3. Where such Consent is sought by Registrar, the request for Consent SHALL be presented in a manner which is clearly distinguishable from other matters (including other Personal Data Processed based on a legitimate interest). The request for Consent SHALL be in an intelligible and easily accessible form, using clear and plain language. The Registered Name Holder SHALL have the right to withdraw its Consent at any time. The withdrawal of Consent SHALL NOT affect the lawfulness of Processing based on Consent obtained before the withdrawal.

7.2.4. Registrar MUST publish the additional contact information outlined in Sections 2.3 and 2.4 of Appendix A for which it has received Consent.

7.3. **Uniform Domain Name Dispute Resolution Policy**. Registrar MUST comply with the additional requirements for the Rules for the Uniform Domain Name Dispute Resolution Policy set forth in Appendix F attached hereto ("**Appendix F**").

7.4. **Transfer Policy**. Registrar MUST comply with the supplemental procedures to the Transfer Policy set forth in Appendix I attached hereto ("**Appendix I**").

# Appendix A: Registration Data Directory Services

## 1. Registration Data Directory Services

This Section modifies the relevant requirements of following: (i) the Registration Data Directory Service (WHOIS) Specification of the 2013 Registrar Accreditation Agreement; (ii) in the case of a Registry Agreement that is modeled after the Base Registry Agreement, Section 1 of Specification 4 of the Base Registry Agreement; (iii) in the case of a Registry Agreement that is not modeled on the Base Registry Agreement, the provisions of such Registry Agreement that are comparable to the provisions of Section 1 of Specification 4 of the Base Registry Agreement; and (iv) provision 10 of the Registry Registration Data Directory Services Consistent Labeling and Display Policy.

1.1. Registrar and Registry Operator MUST operate a Registration Data Access Protocol (RDAP) service. ICANN and the community will define the appropriate profile(s) by 31 July 2018. ICANN will subsequently give notice to implement such service, and Registrar and Registry Operator SHALL implement the service no later than 135 days after being requested by ICANN. Registrar and Registry Operator MAY operate a pilot RDAP service before the date upon which an RDAP service is required.

1.2. **RDDS Search Capabilities**

1.2.1. Where search capabilities are permitted and offered, Registry Operator and Registrar MUST: (1) ensure such search capability is in compliance with applicable privacy laws or policies; (2) only permit searches on data otherwise available to the querying user, based on the user's access level; (3) only provide results otherwise available to the querying user based on the user's access level; and (4) ensure such search capability is otherwise consistent with the requirements of this Temporary Specification regarding access to public and non-public Registration Data.

1.2.2. Where search capabilities are permitted and offered, Registry Operator and Registrar MUST offer search capabilities on the web-based Directory Service and the RDAP service (when implemented).

## 2. Requirements for Processing Personal Data in Public RDDS Where Processing is Subject to the GDPR

2.1. Registry Operator and Registrar MUST apply the requirements in Section 4 of this Appendix to Personal Data included in Registration Data where:

(i) the Registrar or Registry Operator is established in the European Economic Area (EEA) as provided in Article 3(1) GDPR and Process Personal Data included in Registration Data;

(ii) the Registrar or Registry Operator is established outside the EEA and offers registration services to Registered Name Holders located in the EEA as contemplated by Article 3(2) GDPR that involves the Processing of Personal Data from registrants located in the EEA; or

(iii) the Registrar or Registry Operator is located outside the EEA and Processes Personal Data included in Registration Data and where the Registry Operator or Registrar engages a Processor located within the EEA to Process such Personal Data.

2.2. For fields that Sections 2.3 and 2.4 of this Appendix requires to be "redacted", Registrar and Registry Operator MUST provide in the value section of the redacted field text substantially similar to the following: "REDACTED FOR PRIVACY". Prior to the required date of implementation of RDAP, Registrar and Registry Operator MAY: (i) provide no information in the value section of the redacted field; or (ii) not publish the redacted field.

2.3. In responses to domain name queries, Registrar and Registry Operator MUST treat the following Registrant fields as "redacted" unless the Registered Name Holder has provided Consent to publish the Registered Name Holder's data:

- Registry Registrant ID
- Registrant Name
- Registrant Street
- Registrant City
- Registrant Postal Code
- Registrant Phone
- Registrant Phone Ext
- Registrant Fax
- Registrant Fax Ext

2.4. In responses to domain name queries, Registrar and Registry Operator MUST treat the following fields as "redacted" unless the contact (e.g., Admin, Tech) has provided Consent to publish the contact's data:

- Registry Admin/Tech/Other ID
- Admin/Tech/Other Name
- Admin/Tech/Other Organization
- Admin/Tech/Other Street
- Admin/Tech/Other City
- Admin/Tech/Other State/Province
- Admin/Tech/Other Postal Code
- Admin/Tech/Other Country
- Admin/Tech/Other Phone
- Admin/Tech/Other Phone Ext
- Admin/Tech/Other Fax
- Admin/Tech/Other Fax Ext

2.5. In responses to domain name queries, in the value of the "Email" field of every contact (e.g., Registrant, Admin, Tech):

2.5.1. Registrar MUST provide an email address or a web form to facilitate email communication with the relevant contact, but MUST NOT identify the contact email address or the contact itself.

2.5.1.1. The email address and the URL to the web form MUST provide functionality to forward communications received to the email address of the applicable contact.

2.5.1.2. Registrar MAY implement commercially reasonable safeguards to filter out spam and other form of abusive communications.

2.5.1.3. It MUST NOT be feasible to extract or derive the email address of the contact from the email address and the URL to the web form provided to facilitate email communication with the relevant contact.

2.5.2. Registry Operator MUST provide a message substantially similar to the following: "Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name."

## 3. Additional Provisions Concerning Processing Personal Data in Public RDDS Where Processing is not Subject to the GDPR

Registry Operator and Registrar MAY apply the requirements in Section 2 of this Appendix where it has a commercially reasonable purpose to do so.

## 4. Access to Non-Public Registration Data

4.1. Registrar and Registry Operator MUST provide reasonable access to Personal Data in Registration Data to third parties on the basis of a legitimate interests pursued by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Registered Name Holder or data subject pursuant to Article 6(1)(f) GDPR.

4.2. Notwithstanding Section 4.1 of this Appendix, Registrar and Registry Operator MUST provide reasonable access to Personal Data in Registration Data to a third party where the Article 29 Working Party/European Data Protection Board, court order of a relevant court of competent jurisdiction, applicable legislation or regulation has provided guidance that the provision of specified non-public elements of Registration Data to a specified class of third party for a specified purpose is lawful. Registrar and Registry Operator MUST provide such reasonable access within 90 days of the date ICANN publishes any such guidance, unless legal requirements otherwise demand an earlier implementation.

## 5. Publication of Additional Data Fields

Registrar and Registry Operator MAY output additional data fields, subject to the Data Processing requirements in **Appendix D**.

# Appendix B: Registrar and Registry Operator Service Level Agreement

This Appendix modifies the following: (i) Section 2 of the Registration Data Directory Service (WHOIS) Specification in the 2013 Registrar Accreditation Agreement; and (ii) Registry Agreement requirements concerning Service Level Agreements.

This Appendix will become effective on the day that offering RDAP becomes a requirement pursuant to **Appendix A**.

1. The following additional requirements supplement the existing requirements in Section 2 of the Registration Data Directory Service (WHOIS) Specification of the 2013 Registrar Accreditation Agreement and Specification 10 of the Base Registry Agreement:

   1.1 "Registration Data Directory Services" (RDDS) refers to the collective of WHOIS, Web based WHOIS, and RDAP services.

   1.2 The following definition is added to the performance specifications for Registry Operator and Registrars: "RDAP-query RTT" means the RTT of the sequence of packets from the start of the TCP connection to its end, including the reception of the HTTP response for only one HTTP request. If implementing a multiple-step process to get to the information, only the last step shall be measured. If the RTT is 5-times or more the corresponding SLR, the RTT will be considered undefined.

   1.3 The definition for "RDDS query RTT" means: The collective of "WHOIS query RTT", "Web-based-WHOIS query RTT", and "RDAP-query RTT".

2. The following requirements apply to Registry Operators with a Registry Agreement not modeled on the Base Registry Agreement. Such Registry Operator SHALL comply with the following performance specifications:

   **2.1. Service Level Agreement Matrix**

| | Parameter | SLR (monthly basis) |
|---|---|---|
| **RDAP** | RDAP availability | ≤ 864 min of downtime (≈98%) |

| | | |
|---|---|---|
| | RDAP query RTT | ≤ 2000 ms, for at least 95% of the queries |
| | RDAP update time | ≤ 60 min, for at least 95% of the probes |

Registry Operator is encouraged to do maintenance for the different services at the times and dates of statistically lower traffic for each service. However, note that there is no provision for planned outages or similar periods of unavailable or slow service; any downtime, be it for maintenance or due to system failures, will be noted simply as downtime and counted for SLA purposes.

## 2.2. RDAP

2.2.1 **RDAP Availability.** Refers to the ability of the RDAP service for the TLD, to respond to queries from an Internet user with appropriate data from the relevant Registry System. If 51% or more of the RDAP testing probes see any of the RDAP services as unavailable during a given time, the RDAP will be considered unavailable.

2.2.2 **RDAP query RTT.** Refers to the RTT of the sequence of packets from the start of the TCP connection to its end, including the reception of the HTTP response for only one HTTP request. If implementing a multiple-step process to get to the information, only the last step SHALL be measured. If the RTT is 5-times or more the corresponding SLR, the RTT will be considered undefined.

2.2.3 **RDAP update time.** Refers to the time measured from the reception of an EPP confirmation to a transform command on a domain name, host or contact, up until the servers of the RDAP services reflect the changes made.

2.2.4 **RDAP test.** Means one query sent to a particular "IP address" of one of the servers of one of the RDAP services. Queries SHALL be about existing objects in the Registry System and the responses MUST contain the corresponding information otherwise the query will be considered unanswered. Queries with an RTT 5 times higher than the corresponding SLR will be considered as unanswered. The possible results to an RDAP test are: a number in milliseconds corresponding to the RTT or undefined/unanswered.

2.2.5 **Measuring RDAP parameters.** Every 5 minutes, RDAP probes will select one IP address from all the public-DNS registered **"**IP addresses**"** of the

servers for each RDAP service of the TLD being monitored and make an **"**RDAP test**"** to each one. If an **"**RDAP test**"** result is undefined/unanswered, the corresponding RDAP service will be considered as unavailable from that probe until it is time to make a new test.

2.2.6 **Collating the results from RDAP probes.** The minimum number of active testing probes to consider a measurement valid is 10 at any given measurement period, otherwise the measurements will be discarded and will be considered inconclusive; during this situation no fault will be flagged against the SLRs.

2.2.7 **Placement of RDAP probes.** Probes for measuring RDAP parameters SHALL be placed inside the networks with the most users across the different geographic regions; care SHALL be taken not to deploy probes behind high propagation-delay links, such as satellite links.

## 2.3. Covenants of Performance Measurement

2.3.1 **No interference.** Registry Operator SHALL NOT interfere with measurement Probes, including any form of preferential treatment of the requests for the monitored services. Registry Operator SHALL respond to the measurement tests described in this Specification as it would to any other request from an Internet user for RDAP.

## 2.4. Domain name used for RDAP monitoring

2.4.1 Registry Operator SHALL provide ICANN a domain name to be used for RDAP testing.

# Appendix C: Supplemental Data Escrow Requirements

## 1. Data Processing Requirements

Registry Operator and Registrar MUST respectively ensure that any data escrow agreement between Registry Operator and the Escrow Agent and/or Registrar and the Escrow Agent includes data Processing requirements consistent with Article 28 of the GDPR. Such Escrow Agent MUST provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that Processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

## 2. International Transfers

In the course of performing the requirements under the agreement with the Escrow Agent, it may be necessary for the Escrow Agent to Process Personal Data in a country that is not deemed adequate by the European Commission per Article 45(1) of the GDPR. In such a case, the transfer and Processing will be on the basis of adequate safeguards permitted under Chapter V of the GDPR, including the use of Standard Contractual Clauses (2004/915/EC) (or its successor clauses), and the Escrow Agent and Controller MUST comply with such appropriate safeguards.

## 3. Additional Requirements

In addition to the above requirements, the data escrow agreement may contain other data Processing provisions that are not contradictory, inconsistent with, or intended to subvert the required terms provided above.

# Appendix D: Data Processing Requirements

In accordance with the Interim Model and in particular in accordance with section 7.2.11.3. of the GDPR which states that each contracting party with ICANN is acting as an independent "Controller" (as defined in Article 2 of the GDPR) for purposes of GDPR compliance, Registrars and Registry Operators will each comply with the following Processing requirements:

**1. Principles for Processing**

Each Controller will observe the following principles to govern its Processing of Personal Data contained in Registration Data, except as required by applicable laws or regulations. Personal Data SHALL:

1.1. only be Processed lawfully, fairly, and in a transparent manner in relation to the Registered Name Holders and other data subjects ("lawfulness, fairness, and transparency");

1.2. be obtained only for specified, explicit, and legitimate purposes, and SHALL NOT be further Processed in any manner incompatible with those purposes ("purpose limitation");

1.3. be adequate, relevant, and not excessive in relation to the purposes for which they are Processed ("data minimization");

1.4. be accurate and, if necessary, kept current, as appropriate to the purposes for which they are Processed ("accuracy");

1.5. not be kept in a form that permits identification of the Registered Name Holder and other data subjects for longer than necessary for the permitted purposes ("storage limitation"); and

1.6. be Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality").

Each Registrar and Registry Operator SHALL be responsible for, and be able to demonstrate compliance with principles (1.1) to (1.6) ("accountability"). The Registrar or Registry Operator SHALL inform ICANN immediately if such Registrar or Registry Operator (i) cannot abide by the Processing principles outlined in Section 1 of this Appendix, or (ii) receives a complaint by a Registered Name Holder or other data subject that the Registrar or Registry Operator has failed to abide by such principles.

## 2. Lawfulness of Processing

For Personal Data Processed in connection with the Registration Data Directory Services, such Processing will take place on the basis of a legitimate interests of the Controller or of the third party or parties to whom the Personal Data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal Data, in particular where the data subject is a child. For other Personal Data collected for other purposes, such Personal Data SHALL NOT be Processed unless a legal basis specified under Article 6(1) GDPR applies.

## 3. Specific Controller Processing requirements

In addition to the general principles and requirements for lawful Processing, each Controller SHALL comply with the following specific requirements:

3.1. **Implementing appropriate measures.** Implementing appropriate technical and organizational measures to ensure and to be able to demonstrate the Processing is performed in compliance with the GDPR, such as appropriate data protection policies, approved code of conducts or approved certification mechanisms. Such measures SHALL be reviewed regularly and updated when necessary by the Controller;

3.2. **Engaging only selected Processors.** Engaging only selected Processors and implementing a contract with each Processor that sets out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of data subjects and the obligations and rights of the Controller. The engagement of Processor must comply with Article 28 of the GDPR;

3.3. **Designating a Data Protection Officer.** Designating a "Data Protection Officer" where required by Article 37 of the GDPR or Member State national data protection law;

3.4. **Maintaining a record of Processing.** Maintaining a record of the Processing activities under the Controller's responsibility in accordance with Article 30 of the GDPR;

3.5. **Providing transparent information.** Taking appropriate measures to provide any information referred to in Articles 13 and 14 of the GDPR and any communication under Articles 15 to 22 and 34 of the GDPR relating to Processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language;

3.6. **Facilitating of the exercise of data subject rights.** Facilitating the exercise of data subject rights under Articles 15 to 22 of the GDPR. In the cases referred to in Article 11(2) of the GDPR, the Controller SHALL NOT refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22 of the GDPR, unless the Controller demonstrates that it is not in a position to identify the data subject;

3.7. **Implementing measures for data protection by design and by default.** Implementing appropriate technical and organizational measures, both at the time of the determination of the means for Processing and at the time of the Processing itself, which are designed to implement data protection principles, in an effective manner and to integrate the necessary safeguards into the Processing in order to meet the requirements of the GDPR and to protect the rights of data subjects. Implementing appropriate technical and organizational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are Processed.

3.8. **Implementing appropriate security measures.** Implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk of data Processing, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons;

3.9. **Developing procedures for breach notification.** Developing procedures for breach notification to ensure compliance with the obligations pursuant to Articles 33-34 of the GDPR. Any notifications provided in connection with Articles 33-34 of the GDPR SHALL also be provided to ICANN.

3.10. **Observing conditions for international data transfers.** Observing conditions for international data transfers so that any transfer of Personal Data which are undergoing Processing or are intended for Processing after transfer to a third country or to an international organization SHALL take place only if the conditions laid down in Chapter V of the GDPR are complied with, including for onward transfers of Personal Data from the third country or an international organization to another third country or to another international organization.

3.11. **Cooperating with Supervisory Authorities.** Cooperating with Supervisory Authorities, on request, in the performance of their tasks.

# Appendix E: Uniform Rapid Suspension

This Appendix contains supplemental requirements for the 17 October 2013 URS High Level Technical Requirements for Registries and Registrars. All other requirements not specified herein remain applicable and in force.

## 1. URS High Level Technical Requirements for Registry Operator and Registrar

1.1. **Registry Operator Requirement**: The Registry Operator (or appointed BERO) MUST provide the URS provider with the full Registration Data for each of the specified domain names, upon the URS provider notifying the Registry Operator (or appointed BERO) of the existence of a complaint, or participate in another mechanism to provide the full Registration Data to the Provider as specified by ICANN. If the gTLD operates as a "thin" registry, the Registry Operator MUST provide the available Registration Data to the URS Provider.

1.2. **Registrar Requirement**: If the domain name(s) subject to the complaint reside on a "thin" registry, the Registrar MUST provide the full Registration Data to the URS Provider upon notification of a complaint.

# Appendix F: Uniform Domain Name Dispute Resolution Policy

This Appendix contains supplemental requirements for the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules"). All other requirements not specified herein remain applicable and in force.

## 1. Uniform Domain Name Dispute Resolution Policy

1.1. **Registrar Requirement**: The Registrar MUST provide the UDRP provider with the full Registration Data for each of the specified domain names, upon the UDRP provider notifying the Registrar of the existence of a complaint, or participate in another mechanism to provide the full Registration Data to the Provider as specified by ICANN.

# Appendix G: Bulk Registration Data Access to ICANN

This Appendix replaces the requirement in: (i) Section 3.1.1 of Specification 4 of each Registry Agreement that is modeled on the Base Registry Agreement; and (ii) the relevant provision in a Registry Agreement not based on the Base Registry Agreement to provide Bulk Registration Data Access to ICANN (also called "Whois Data Specification – ICANN" in some gTLD agreements).

1. **Contents.** Registry Operator MUST only provide the following data for all registered domain names: domain name, domain name repository object id (roid), Registrar ID (IANA ID), statuses, last updated date, creation date, expiration date, and name server names. For sponsoring registrars, Registry Operator MUST only provide: registrar name, registrar ID (IANA ID), hostname of registrar Whois server, and URL of registrar.

# Appendix H: Registry Operator Monthly Reports

Section 2 of Specification 3 of each Registry Agreement that is modeled on the Base Registry Agreement is updated to include the following fields in the Registry Functions Activity Report:

| Field # | Field Name | Description |
|---|---|---|
| 38 | rdap-queries | Total number of RDAP queries received during the period. |
| 39 | rdap-domain | Number of RDAP domain queries, authorized or not, received during the period. |
| 40 | rdap-entity | Number of RDAP entity queries, authorized or not, received during the period. |
| 41 | rdap-nameserver | Number of RDAP nameserver queries, authorized or not, received during the period. |
| 42 | rdap-help | Number of RDAP help queries, authorized or not, received during the period. |
| 43 | rdap-domain-authorized | Number of successfully-authorized RDAP domain queries received during the period. |
| 44 | rdap-entity-authorized | Number of successfully-authorized RDAP entity queries received during the period. |
| 45 | rdap-nameserver-authorized | Number of successfully-authorized RDAP nameserver queries received during the period. |
| 46 | rdap-help-authorized | Number of successfully-authorized RDAP help queries received during the period. |
| 47 | rdap-rate-limit | Number of RDAP queries refused due to rate limiting for the period. |
| 48 | rdap-search-domain | Number of RDAP domain search queries, authorized or not, for the period. |
| 49 | rdap-search-entity | Number of RDAP entity search queries, |

| | | |
|---|---|---|
| | | authorized or not, for the period. |
| 50 | rdap-search-nameserver | Number of RDAP nameserver search queries, authorized or not, for the period. |
| 51 | rdap-search-domain-authorized | Number of successfully-authorized RDAP domain search queries for the period. |
| 52 | rdap-search-entity-authorized | Number of successfully-authorized RDAP entity search queries for the period. |
| 53 | rdap-search-nameserver-authorized | Number of successfully-authorized RDAP nameserver search queries for the period. |
| 54 | rdap-truncated-authorization | Number of RDAP responses truncated due to lack of proper authorization. Includes both results and object truncation events. |
| 55 | rdap-truncated-load | Number of RDAP responses truncated due to server load. Includes both results and object truncation events. |
| 56 | rdap-truncated-unexplainable | Number of RDAP responses truncated due to unexplainable reasons. Includes both results and object truncation events. |

# Appendix I: Supplemental Procedures to the Transfer Policy

This Appendix provides supplemental procedures for the Transfer Policy applicable to all ICANN-accredited Registrars.

1. Until such time when the RDAP service (or other secure methods for transferring data) is required by ICANN to be offered, if the Gaining Registrar is unable to gain access to then-current Registration Data for a domain name subject of a transfer, the related requirements in the Transfer Policy will be superseded by the below provisions:

    1.1. The Gaining Registrar is NOT REQUIRED to obtain a Form of Authorization from the Transfer Contact.

    1.2. The Registrar of Record MAY deny a transfer if no response is received from the Registered Name Holder or Administrative Contact within the time allotted by the Transfer Policy.

    1.3. The Registrant MUST independently re-enter Registration Data with the Gaining Registrar. In such instance, the Gaining Registrar is NOT REQUIRED to follow the Change of Registrant Process as provided in Section II.C. of the Transfer Policy.

2. As used in the Transfer Policy:

    2.1. The term "Whois data" SHALL have the same meaning as "Registration Data".

    2.2. The term "Whois details" SHALL have the same meaning as "Registration Data".

    2.3. The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".

    2.4. The term "Whois" SHALL have the same meaning as "RDDS".

3. Registrar and Registry Operator SHALL follow best practices in generating and updating the “AuthInfo” code to facilitate a secure transfer process.

4. Registry Operator MUST verify that the “AuthInfo” code provided by the Gaining Registrar is valid in order to accept an inter-registrar transfer request.

# Annex: Important Issues for Further Community Action

While the Temporary Specification provides modified requirements to the Registry and Registrar Accreditation Agreements and relevant consensus policies to address the immediate needs of GDPR compliance, the ICANN Board encourages the community to consider the implementation items set forth below that need to be resolved as quickly as possible after the effective date of the Temporary Specification.

1. Pursuant to Section 4.4, continuing community work to develop an accreditation and access model that complies with GDPR, while recognizing the need to obtain additional guidance from Article 29 Working Party/European Data Protection Board.

2. Addressing the feasibility of requiring unique contacts to have a uniform anonymized email address across domain name registrations at a given Registrar, while ensuring security/stability and meeting the requirements of Section 2.5.1 of Appendix A.

3. Developing methods to provide potential URS and UDRP complainants with sufficient access to Registration Data to support good-faith filings of complaints.

4. Consistent process for continued access to Registration Data, including non-public data, for users with a legitimate purpose, until the time when a final accreditation and access mechanism is fully operational, on a mandatory basis for all contracted parties.

5. Distinguishing between legal and natural persons to allow for public access to the Registration Data of legal persons, which are not in the remit of the GDPR.

6. Limitations in terms of query volume envisaged under an accreditation program balanced against realistic investigatory cross-referencing needs.

7. Confidentiality of queries for Registration Data by law enforcement authorities.

# Implementation Notes

## 1. Background on Board Adoption of Temporary Specification.

1.1. **[TENTATIVE – PENDING BOARD ACTION]** [On ___ May 2018, the ICANN Board adopted the Temporary Specification on gTLD Registration Data ("Temporary Specification") pursuant to the procedures for the establishment of temporary policies in ICANN's agreements with Registry Operators and Registrars.] The Temporary Specification provides modifications to existing requirements in the Registrar Accreditation Agreement and Registry Agreements about how gTLD registration data is collected, displayed, and Processed. It addresses immediate temporary changes that are needed to maintain the stability or security of Registrar Services, Registry Services, the DNS and/or the Internet. At risk, absent the Board's action in adopting the Temporary Specification, is the stable operation of the Internet, which relies on the basic concept that you cannot run a hierarchical and decentralized system like the Internet (a network or networks) if you cannot find the people who operate it to warn of problems and coordinate responses to operational issues. The WHOIS system makes this possible through the collection and publication of WHOIS registration data, which includes contact information for the Registrant, Administrative and Technical contacts as well as technical information associated with a domain name.

1.2. In particular, the Temporary Specification provides modified requirements to ensure continued availability of Registration Data Directory Services/WHOIS while complying with new legal regulations impacting how Personal Data in the domain name ecosystem is treated. This Temporary Specification avoids fragmentation of the WHOIS system by ensuring a common framework for continued provision and access to WHOIS services, which supports the critical role the WHOIS system plays in ensuring the operational integrity and continued trust upon which the DNS is built, and supports ICANN's mission to "to ensure the stable and secure operation of the Internet's unique identifier systems".

1.3. See the Advisory Statement: Temporary Specification for gTLD Registration Data for additional information on how the Temporary Specification preserves the WHOIS system in the context of security and stability, as well as steps ICANN has taken to build consensus support and to ensure that the Temporary Specification complies with the GDPR and addresses other public policy considerations.

## 2. References

2.1. gTLD Registration Dataflow Matrix and Information**.** With the help from Registrars and Registry Operators as well as interested stakeholders, ICANN collected information needed to help evaluate GDPR compliance in the context of registry, registrar, and registrant data. This information was used to inform legal analysis, as well as to engage with data protection authorities.

2.2. Hamilton Memoranda. At the request of the community, ICANN org commissioned European law firm Hamilton to produce three memoranda outlining the GDPR's impact on gTLD registration directory services. The memoranda concluded that WHOIS would have to change in light of the law, responded to community questions about the law, and provided examples of how WHOIS services may change to comply with the GDPR.

2.3. Statement from ICANN Contractual Compliance. On 2 November 2017, ICANN issued a statement from ICANN's Contractual Compliance Department regarding the ability of Registry Operators and Registrars to comply with their WHOIS and other contractual requirements related to domain name registration data in light of the European Union's General Data Protection Regulation (GDPR).

2.4. Community-Proposed Models for GDPR Compliance. In response to the Statement from ICANN's Contractual Compliance Department, several proposed models for GDPR compliance were submitted by various stakeholders.

2.5. ICANN Organization's Three Proposed Interim Compliance Model. On 12 January 2018, ICANN org published three proposed interim models for compliance and sought community input. The models reflected discussions from across the community and with data protection authorities, legal analyses and the proposed community models received to date.

2.6. ICANN Org's Proposed Interim GDPR Compliance Model (Calzone). On 28 February 2018, ICANN org published the Proposed Interim GDPR Compliance Model (Calzone), which incorporated input from the community and feedback from data protection authorities. The Calzone provides a high-level summary of the proposed model. In addition, ICANN org also published an updated Working Draft Non-Paper that compares ICANN- and community-proposed models.

2.7. ICANN Org's Proposed Interim GDPR Compliance Model (Cookbook). On 8 March 2018, ICANN Org published the Cookbook that contains the Proposed Interim GDPR Compliance Model and legal justification for collection and use of the WHOIS data included in the Calzone.

## 3. Legal Basis and Purposes of Processing gTLD Registration Data Elements

Under the GDPR, Personal Data may only be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. The legal basis and purposes of Processing gTLD Registration Data elements are detailed at <<https://www.icann.org/resources/pages/gtld-registration-data-specs-en)>>