Los Angeles Headquarters
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA
+1 310 301 5800
+1 310 823 8649

23 May 2018

RE: Input on the Proposed Temporary Specification for gTLD Registration Data

Mr. Roberto Viola
Director General, DG Communications Networks, Content & Technology

Ms. Paraskevi Michou
Director General, DG Migration and Home Affairs

Ms. Tiina Astola
Director General, DG Justice and Consumers

Dear Mr. Viola, Ms. Michou, and Ms. Astola,

Thank you for your 17 May 2018 letter providing additional input on ICANN's proposed Temporary Specification for gTLD Registration Data. The Commission's willingness to "to play a facilitating role" in ICANN's continued dialogue with the Article 29 Working Party/European Data Protection Board concerning changes to the WHOIS system to comply with the General Data Protection Regulation (GDPR) is most appreciated.

Update on Status of the Temporary Specification for gTLD Registration Data

On 17 May 2018, the ICANN Board of Directors adopted the Temporary Specification for gTLD Registration Data ("Temporary Specification"). The Temporary Specification, a copy of which is attached to this letter, will be effective as of 25 May 2018. The requirements in the Temporary Specification provide ICANN organization with the ability to continue to enforce its contractual requirements concerning WHOIS, although in a changed way to account for the GDPR.

As noted during our previous discussions, ICANN's mission and mandate as stated in our Bylaws has led to the WHOIS obligations expressed in ICANN community-developed consensus policies and agreements that ICANN has with gTLD registry operators and registrars. These obligations require each of the 2,500 registry operators and registrars (as independent data controllers) to operate public, query-based access to registration data via WHOIS services. ICANN's role is that of a coordinator of the decentralized databases (operated by the gTLD registries and registrars) that make up WHOIS. [ICANN itself does not have a database with the WHOIS data]. Because WHOIS is embedded in ICANN's governing corporate documents, ICANN has been entrusted by the community to continue to play a coordinator role with respect to this global public service. Absent clarity on GDPR as it relates to ICANN's ability to continue to enforce WHOIS-related requirements, many of the gTLD registries and registrars may cease providing WHOIS services, which are cost centers and the risk of non-compliance with legal obligations may pose additional risk that the contracted parties are unwilling to take.

The Board's approval of the Temporary Specification will assist in having a unified approach for ICANN organization to enforce its contractual requirements concerning WHOIS. However, because the GDPR is a new regulation and has yet to be tested [through the court system], there are differing viewpoints about what is permitted under the law with regards to the continued collection, retention and publication of gTLD registration data that make up the WHOIS databases. ICANN understands from discussions with some of the contracted parties that gTLD registrars for at least 5 - 10 % of domain names will cease collecting the full set of registration data (including for example, email and street addresses of administrative and technical contacts associated with the domain name) due to different interpretations of what is required and permitted by the GDPR. At least one of the contracted parties (established in Europe) has informed ICANN that it also intends to delete certain personal data it has already collected from registrants because it believes that retaining that data is in violation of the GDPR. In the event this occurs, ICANN would take all measures to ensure the WHOIS does not become fragmented, including possible legal action in a European court to prevent any potential loss of data, and to help clarify the scope of the GDPR in relation to ICANN's agreements with registries and registrars.

The uncertainty about the scope of changes needed to ICANN's existing agreements to comply with the law presents a challenge to ICANN because it is either expressed or implied in ICANN's agreements that contracted parties must comply with all applicable laws. While ICANN has the authority to enforce its *contractual* mandates, there are limitations to its authority to require WHOIS as there is no legal mandate for WHOIS for gTLDs – only what is established in ICANN's Bylaws and what is able to be enforced through our contracts.

Because ICANN's authority rests with its contracts and not because of a legal mandate, even if ICANN were to bring a contractual compliance enforcement action and initiate de-accreditation proceedings against a registrar for an uncured violation, for example, the lack of clarity about the interpretation of the law constrains whether ICANN could sustain its position that there is in fact a breach of contract.

Request for Guidance from the Commission

With this background, ICANN would like to ask whether the Commission could advise on and assist with potential avenues available for ICANN to be viewed under the law as the coordinator for the WHOIS system for gTLD registrars and registries. ICANN acknowledges the sentiment expressed in the Commission's letter that, "ICANN plays a key role as the 'guardian' of the domain name system at the core of the Internet and is responsible for ensuring the security, stability and resilience of some key technical Internet functions." In this role of "guardian" of the WHOIS system, would the Commission see opportunities for ICANN beyond (1) its role as one of the "controllers" with respect to WHOIS, or (2) its contractual enforcement role, to assume a greater responsibility under the law with a view to be able to ensure the continued coordination for WHOIS services? In particular, this request comes in light of the sentiment expressed in the Commission's letter noting that there is an opportunity for ICANN to "show leadership" and for ICANN to explore all paths to "be proactive, and ensure that the system will actually operate to mitigate risks of potential or actual harm to people and the security and stability of the Internet."

At a minimum, ICANN reiterates a request made to the Article 29 Working Party that ICANN would ask to be included in all discussions and actions of the privacy regulators with the other WHOIS data controllers.

Work to Develop a Unified Access Model

At the same time, we are working with community to address the remaining open issues identified in the Annex of the Temporary Specification (page 32), including work to develop a unified access model that complies with the GDPR. The unified access model would provide certified user groups, such as law enforcement agencies, access to non-public WHOIS data based on pre-defined criteria, limitations and safeguards.

ICANN's work on an approach for a unified access model began early on in discussions with the community about developing an interim GDPR compliance model. These community discussions included consultation with the ICANN's Governmental Advisory Committee about public policy considerations that should be taken into account in the development of such a model. On 28 February 2018, ICANN published a summary description of a proposed interim compliance model ("Proposed Interim Model for GDPR Compliance, the "Calzone Model"), which included a proposed approach for providing access to non-public WHOIS data based on discussions to-date with the community. As described in that paper at pages 7 -8:

> *The user groups eligible for the accreditation program, and the process for providing access to the non-public WHOIS data would be developed in consultation with the Governmental Advisory Committee (GAC) so that public policy considerations are taken into account. As a starting place, individual governments could provide to the GAC a list of authorized law enforcement authorities and other governmental agencies certified for access to non-public WHOIS data. For entities other than law enforcement agencies, the GAC could develop codes of conduct which would establish the standardized criteria, limitations, and responsibilities for granting access to non-public WHOIS data to the accredited parties. Selection of the accredited parties could be facilitated by designated expert groups.*

The approach in the Calzone Model was further refined in ICANN's publication titled "Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation, the "Cookbook" 8 March 2018 (see Section 7.2.9) and is the subject of ongoing community discussions.

Recognizing the ongoing work to develop a unified access model, the Temporary Specification includes requirements for registries and registrars to have ready the technical means to implement a unified access model so that it may be implemented as soon as the model is developed by the community with guidance from the European Data Protection Board and [ICANN's Governmental Advisory Committee]. (See Appendix A, Section 1.1.)

Also, ICANN takes note of the Commission's invitation to "consider and possibly integrate models for the accreditation system currently being developed by relevant stakeholders (e.g. by

the business community).” We have prepared a timeline (attached) showing our plan of action with respect to the important work of developing a unified access model and continued engagement by the Commission on this matter would be welcomed to help make sure there is sufficient time to implement the model. As noted on the timeline, gTLD registries and registrars are required to have the technical means to implement a unified access model by December 2018.

Next Steps

ICANN will continue to take all measures to maintain a globally uniformly accessible WHOIS and appreciates the support and partnership from the Commission and your communication to us on the importance of this issue. We look forward to continuing to work with you, the community, the data protection authorities, and interested stakeholders recognizing that the Commission “urge[s] ICANN to keep working beyond [25 May] in an iterative way to incorporate changes on the basis of this ongoing dialogue, as well as input from the community.” As such, clarity and recognition of ICANN’s role with respect to WHOIS will greatly assist with this. We will continue to work to find a mutually agreeable time for a telephone conference to continue our discussion on these important matters.

Sincerely,

Göran Marby
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers (ICANN)

Temporary Specification for gTLD Registration Data

Adopted on 17 May 2018 by ICANN Board Resolutions 2018.05.17.01 – 2018.05.17.09

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 where commercially reasonable to do so or where it is not technically feasible to limit application of the requirements to data governed by the GDPR. 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 17 May 2018, 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: https://www.icann.org/en/system/files/files/advisory-statement-gtld-registration-data-specs-17may18-en.pdf.

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. For purposes of clarity, unless specifically addressed and modified by this Temporary Specification, all other requirements and obligations within Registry Operator's Registry Agreement and Registrar's Registrar Accreditation Agreement and consensus policies remain applicable and in force

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 25 May 2018.

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 interests 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 interests 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

[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…."

freedoms of the affected data subject. ICANN finds that the Processing is proportionate for the following reasons:

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 acknowledge that in its implementation of a Registration Data Access Protocol (RDAP) service, they MUST comply with additional Service Level Agreements. ICANN and the contracted parties will negotiate in good faith the appropriate service levels agreements by 31 July 2018. If the contracted parties and ICANN are unable to define such Service Level Agreements through good

faith negotiations by such date, ICANN will require Registrar and Registry Operator to comply with Service Levels that are comparable to those service levels already existing in their respective agreements with respect to RDDS.

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

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 C attached hereto ("**Appendix C**").

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 D attached hereto ("**Appendix D**").

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 F attached hereto ("**Appendix F**").

6.2. **Registry Monthly Reports**. ICANN and Registry Operators will negotiate in good faith appropriate additional reporting requirements with respect to its implementation of RDAP by 31 July 2018. If ICANN and Registry Operators are unable to define such additional reporting requirements through good faith negotiations by such date, ICANN will require Registry Operator to comply with additional reporting requirements that are comparable to those already existing in its Registry Agreement with respect to RDDS.

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 applicable requirements of 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 (which itself contains EU Model Clauses to govern international data transfers, where applicable between the respective parties) 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 E attached hereto ("**Appendix E**").

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

8. Miscellaneous

8.1. **No Third-party Beneficiaries**. This Temporary Specification will not be construed to create any obligation by either ICANN, Registry Operator, or Registrar to any non-party to this Temporary Specification, including Registered Name Holder.

8.2. **Modifications to Temporary Specification**. Implementation details of this Temporary Specification MAY by modified upon a two-thirds vote of the ICANN the Board to make adjustments based on further inputs from the Article 29 Working Party/European Data Protection Board, court order of a relevant court of competent jurisdiction concerning the GDPR, applicable legislation or regulation, or as a result of the Board-GAC Bylaws Consultation concerning GAC advice in the San Juan Communiqué about WHOIS and GDPR.

8.3. **Severability**. This Temporary Specification SHALL be deemed to be severable; the invalidity or unenforceability of any term or provisions of this Temporary Specification SHALL NOT affect the validity or enforceability of the balance of this Temporary Specification or any other term hereof, which SHALL remain in full force and effect.

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 whether the user only has access to data publicly available in RDDS or whether the user has access to non-public Registration Data; (3) only provide results otherwise available to the querying user based on whether the user only has access to data publicly available in RDDS or whether the user has access to non-public Registration Data; 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 (except where Registry Operator operates a "thin" registry) and Registrar MUST apply the requirements in Sections 2 and 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."

2.6. Notwithstanding Sections 2.2, 2.3, 2.4, and 2.5 of this Appendix, in the case of a domain name registration where a privacy/proxy service used (e.g. where data associated with a natural person is masked), Registrar MUST return in response to any query full WHOIS data, including the existing proxy/proxy pseudonymized email.

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 (i) where it has a commercially reasonable purpose to do so ,or (ii) where it is not technically feasible to limit application of the requirements as provided in Section 2.1 of this Appendix.

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 concerning the GDPR, 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 C**.

Appendix B: 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. ICANN Approval

Registry Operator MAY amend or restate its respective Data Escrow 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 and Registrar MUST promptly deliver any such amended or restated Data Escrow Agreement to ICANN. Upon ICANN's receipt thereof, such amended or restated Data Escrow Agreement will be deemed to supplement or replace, as applicable, the approved Data Escrow Agreement that is attached as an appendix (if any) to Registry Operator's Registry Agreement.

4. 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 C: Data Processing Requirements

This Appendix sets out the framework for the Processing and sharing of Registration Data containing Personal Data between the parties as Data Controllers or Data Processors, as identified in the matrix below, and defines the principles and procedures that the parties SHALL adhere to and the responsibilities the parties owe to each other. The parties collectively acknowledge and agree that Processing of Registration Data is to be performed at different stages, or at times even simultaneously, within the Internet's complex environment, by the parties. Thus, this Appendix is required to ensure that where Personal Data may be accessed, such access will at all times comply with the requirements of the GDPR. Unless defined in this Appendix, terms with initial capital letters have the meaning given under the GDPR.

gTLD Processing Activity	**Registrar Role/ Legal Justification**	**Registry Operator Role / Legal Justification**	**ICANN Role / Legal Justification**
Collection of registration data from Registered Name Holder	Controller (Consent and Performance of a Contract)	Controller (Legitimate Interest and Performance of a Contract)	Controller (Legitimate Interest)
Transfer of registration data from Registrar to Registry Operator or Registry Operator Back-end Service Provider	Processor (Performance of a Contract)	Controller (Legitimate Interests)	Controller (Legitimate Interests)
Transfer of registration data from Registry Operator to Data Escrow Agent	No role	Processor (Performance of a Contract)	Controller (Legitimate Interest)
Transfer of registration data from Registrar to Data Escrow Agent	Processor (Performance of Contract)	No role	Controller (Legitimate Interest)
Transfer of registration data to ICANN Contractual Compliance	Processor	Processor	Controller (Legitimate Interest)
Transfer of registration data to Emergency Back-end	No role	Processor (Performance of a Contract)	Controller (Legitimate Interest)

gTLD Processing Activity	Registrar Role/ Legal Justification	Registry Operator Role / Legal Justification	ICANN Role / Legal Justification
Registry Operator (EBERO)			
Public RDDS/WHOIS	Controller (Legitimate Interest)	Controller (Legitimate Interest)	Controller (Legitimate Interest)
Disclosure of non-public RDDS/WHOIS to third parties	Controller (Performance of a Contract [can also vary depending upon the requesting party])	Controller (Performance of a Contract [can also vary depending upon the requesting party])	Controller (Performance of a Contract)
Data retention	No role	Processor (Performance of a Contract)	Controller (Performance of a Contract)

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 (as outlined in Section 4 of this Temporary Specification), 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. The parties acknowledge and agree that they are responsible for maintaining appropriate organizational and security measures to protect such Personal Data shared between the parties in accordance with applicable laws. Appropriate organizational and security measures are further enumerated in Section 3.8 of this Appendix, and generally MUST include:

3.1.1. Measures to ensure that only authorized individuals for the purposes of this Appendix can access the Personal Data;

3.1.2. The pseudonymisation and encryption of the Personal Data, where necessary or appropriate;

3.1.3. The ability to ensure continued confidentiality, integrity, availability and resilience of its processing systems and services;

3.1.4. The ability to restore the availability and access to Personal Data in a timely manner;

3.1.5. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data; and

3.1.6. Measures to identify vulnerabilities with regard to the processing of Personal Data in its systems;

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, which SHALL specifically include the following obligations:

3.5.1. The parties SHALL ensure that their privacy notices are clear and provide sufficient information to Data Subjects in order for them to understand what of their Personal Data the Parties are sharing, the circumstances in which it will be shared, the purposes for the data sharing and either the identity with whom the data is shared or a description of the type of organization that will receive the Personal Data;

3.5.2. The parties undertake to inform Data Subjects of the purposes for which it will process their Personal Data and provide all of the information that it must provide in accordance with applicable laws, to ensure that the Data Subjects understand how their Personal Data will be processed by the Controller.

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. Appropriate technical and organizational measures to protect the Personal Data shared against unauthorized or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure, MAY include, but not limited to:

3.8.1. Ensuring IT equipment, including portable equipment is kept in lockable areas when unattended;

3.8.2. Not leaving portable equipment containing the Personal Data unattended;

3.8.3. Ensuring use of appropriate secure passwords for logging into systems or databases containing Personal Data shared between the parties;

3.8.4. Ensuring that all IT equipment is protected by antivirus software, firewalls, passwords and suitable encryption devices;

3.8.5. Using industry standard 256-bit AES encryption or suitable equivalent where necessary or appropriate;

3.8.6. Limiting access to relevant databases and systems to those of its officers, staff, agents, vendors and sub-contractors who need to have access to the Personal Data, and ensuring that passwords are changed and updated regularly to prevent inappropriate access when individuals are no longer engaged by the party;

3.8.7. Conducting regular threat assessment or penetration testing on systems; and

3.8.8. Ensuring all authorized individuals handling Personal Data have been made aware of their responsibilities with regards to handling of Personal Data.

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. Where a party is not the Data Controller, it must communicate any data security breach immediately

after discovery thereof and will provide immediate feedback about any impact this incident may/will have on the Controller and any Personal Data shared with the Controller. Such notification will be provided as promptly as possible.

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. A party may only transfer Registration Data including Personal Data relating to EU individuals to outside of the EU (or if such Personal Data is already outside of the EU, to any third party also outside the EU), in compliance with the terms this Section 3.10, and the requirements of applicable laws.

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

Appendix D: Uniform Rapid Suspension

This Appendix contains supplemental requirements for the 17 October 2013 URS High Level Technical Requirements for Registries and Registrars and URS Rules effective 28 June 2013.

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.

2. URS Rules

Complainant's complaint will not be deemed defective for failure to provide the name of the Respondent (Registered Name Holder) and all other relevant contact information required by Section 3 o the URS Rules if such contact information of the Respondent is not available in registration data publicly available in RDDS or not otherwise known to Complainant. In such an event, Complainant may file a "Doe" complaint and the Examiner shall provide the relevant contact details of the Registered Name Holder after being presented with a "Doe" complaint.

Appendix E: Uniform Domain Name Dispute Resolution Policy

This Appendix contains supplemental requirements for the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules").

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.

1.2. Complainant's complaint will not be deemed defective for failure to provide the name of the Respondent (Registered Name Holder) and all other relevant contact information required by Section 3 o the UDRP Rules if such contact information of the Respondent is not available in registration data publicly available in RDDS or not otherwise known to Complainant. In such an event, Complainant may file a "Doe" complaint and the Provider shall provide the relevant contact details of the Registered Name Holder after being presented with a "Doe" complaint.

Appendix F: 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 G: 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 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

The purpose of this Annex is to set forth implementation issues raised during the course of development of this Temporary Specification for which the ICANN Board encourages the community to continue discussing so that they may be resolved as quickly as possible after the effective date of the Temporary Specification. This Annex does not create new or modified requirements for Registrar or Registry Operator, nor is it intended to direct the scope of the Policy Development Process, which will be initiated as a result of the Board's adoption of this 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. On 17 May 2018, the ICANN Board adopted the Temporary Specification for generic top-level domain (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 and Registry Agreements to bring them into compliance with the European Union's General Data Protection Regulation (GDPR). Absent these modifications, ICANN, Registry Operators, and Registrars would not be able to comply with both the law and ICANN agreements when the GDPR goes into effect on 25 May 2018. This would result in the inability of ICANN to enforce its contracts. This would also result in each Registry Operator and Registrar making their own determination regarding what gTLD Registration Data should be collected, transferred and published, leading to a fragmentation of the globally distributed WHOIS system. Fragmentation of the WHOIS system would jeopardize the availability of Registration Data, which is essential to ensuring the security and stability of the Internet, including to mitigate attacks that threaten the stable and secure operation of the Internet. As such, the Temporary Specification is needed prior to 25 May 2018 to preserve the security and stability of registry services, registrar services, and of the Domain Name System (DNS).

1.2. 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.

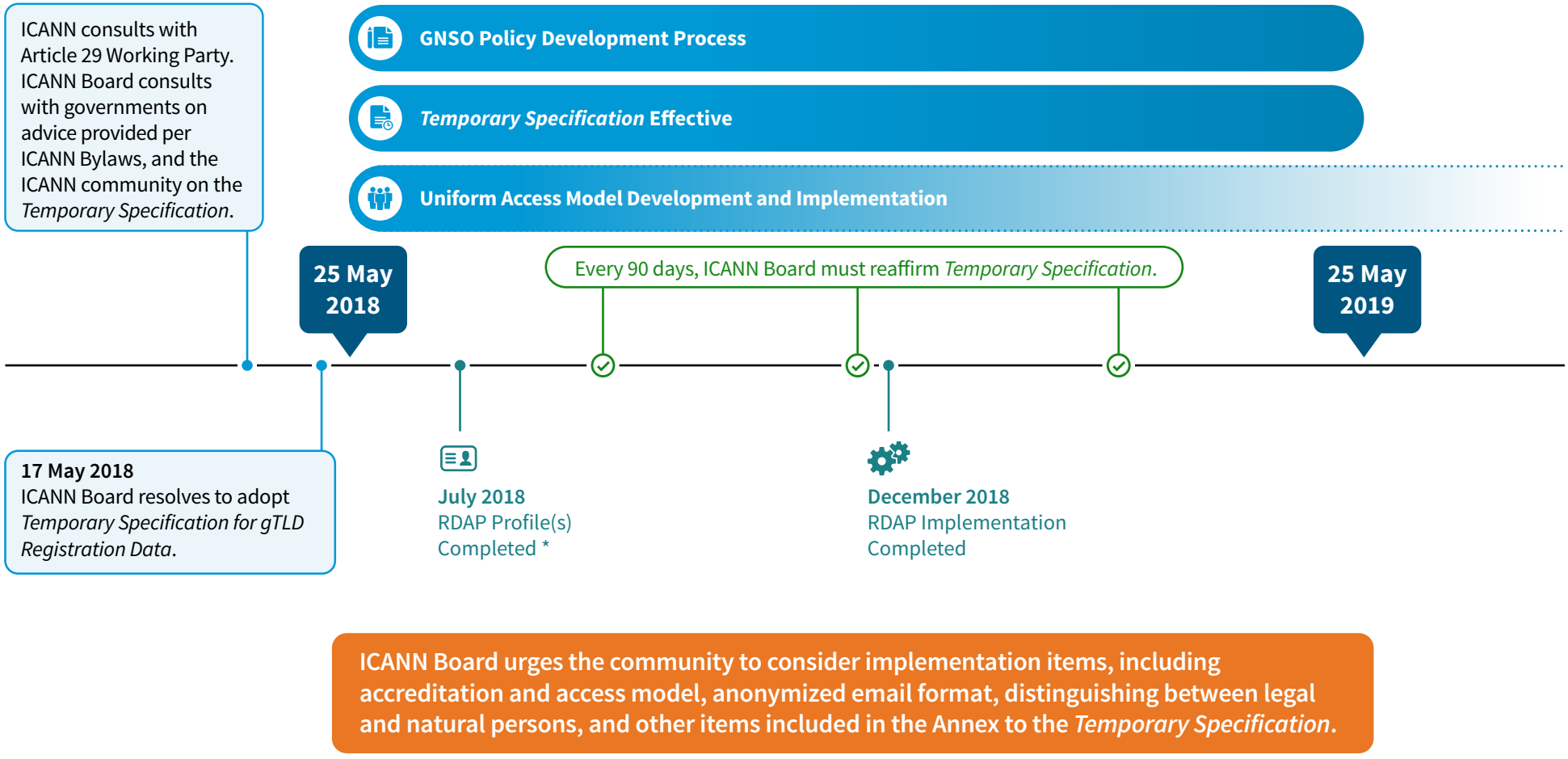
2.6. ICANN Org's Proposed Interim GDPR Compliance Model (Calzone). On 28 February 2018, ICANN org published the Proposed Interim GDPR Compliance Model (Calzone), which incorporated input from the community and feedback from data protection authorities. The Calzone provides a high-level summary of the 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)>>

Plan of Action to Implement *Temporary Specification for gTLD Registration Data*



GAC: Governmental Advisory Committee	**gTLD:** generic top-level domain	**GNSO:** Generic Names Supporting Organization	**RDAP:** Registration Directory Access Protocol

*** RDAP** enables users to access current registration data. It was created as an eventual replacement for the WHOIS protocol. RDAP provides for layered access to registration data.