Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation – WORKING DRAFT FOR CONTINUED DISCUSSION

(The "Cookbook", 8 March 2018)
Prepared by: ICANN organization

1. Executive Summary

1.1. The General Data Protection Regulation (GDPR) was adopted by the European Union (EU) in April 2016 and takes effect on 25 May 2018 uniformly across the EU countries. Over the past several months, ICANN organization (ICANN org) has consulted with contracted parties, European data protection authorities, legal experts, and interested governments and community stakeholders to understand the potential impact of the GDPR to personal data that participants in the gTLD domain name ecosystem collect, display and process (including registries and registrars) pursuant to ICANN contracts and policies.

1.2. This document presents a unified plan and approach for how ICANN and the industry of more than 1,000 generic top-level domain (gTLD) registries and registrars could continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR. The plan attempts to balance the values of the existing practices and policy work that that has established the current WHOIS system with the new law.

1.3. The plan is presented in the form of an "Interim Compliance Model" for handling registration data, including registration directory services (e.g. WHOIS)[1]. Notably, to comply with the GDPR the plan requires a shift from the current requirement for gTLD registries and registrars to provide open, publicly available WHOIS services to an approach requiring a layered/tiered access model for WHOIS.

1.4. Discussions with various parts of the community about the Interim Compliance Model suggest that there is convergence on key elements of the model, including layered/tiered access for WHOIS; developing an accreditation program for access to full WHOIS data (in consultation with the Governmental Advisory Committee, data protection authorities and contracted parties with full transparency to the ICANN community); and which elements of WHOIS data should only be available to accredited users. Also, there are some competing views on the requirements of the GDPR and a few key elements in the model, namely:

(i) whether or not registrars must continue to collect the contact details for administrative and technical contacts and transmit them to the registry and escrow provider;

(ii) whether or not anonymized email addresses should be substituted for the email addresses for registrant, administrative, and technical contacts in public WHOIS;

[1] This document uses the term "WHOIS" for ease of reference but is intended to cover Registration Data Directory Services generally.

(iii) whether or not registries and registries should be permitted to optionally apply the model on a global basis;

(iv) whether or not the model should apply to contact details supplied by registrants who are legal persons; and

(v) which elements of WHOIS data should be published in public WHOIS while an accreditation program for layered/tiered access is being developed.

1.5. This document is a working draft of the Interim Compliance Model and may be updated as conversations with the community and data protection authorities progress in the coming weeks, in particular with respect to the competing community views outlined above.

1.6. The Interim Compliance Model does not replace the multistakeholder policy development process and implementation activities that are underway, including efforts to enhance privacy and proxy services available to registrants, updates to ICANN's Procedure for Handling WHOIS Conflicts with Privacy Law, and community activities working to develop a new policy framework to support potential next-generation registration directory services to replace WHOIS. ICANN org will continue to support the community's work on these efforts.

2. Background Information

2.1. ICANN org has engaged with its community members, including contracted parties, governments, including data protection authorities (DPAs), law enforcement, intellectual property representatives and civil society to address the GDPR's impact on ICANN's contracts, and particularly on the collection, retention and display of registration data in the WHOIS services.

2.2. In preparing for the GDPR's May 2018 enforcement date, the ICANN community collectively engaged with European data protection commissioners at ICANN58 in March 2017. At that session, representatives from various community groups and high-level European data protection experts exchanged views with ICANN on privacy and data protection implications of processing WHOIS data, third-party access to personal data, and the issue of accountability for the processing of personal data.[2]

2.3. Following this discussion, at the direction of ICANN President and CEO Göran Marby, ICANN org formed an internal GDPR Task Force comprised of senior leaders and subject matter experts to focus on the GDPR's impact on ICANN's contracts with registries and registrars and potential impacts on community members who rely on the availability of

[2] https://icann58copenhagen2017.sched.com/event/9nnl/cross-community-discussion-with-data-protection-commissioners

WHOIS. Throughout the process, ICANN org has emphasized that whatever the outcome of discussions related to the GDPR, any solution presented would be interim and would not replace the ongoing community-led policy development process related to a Next Generation Registration Directory Service, or existing policies related to registration data in its current form in the WHOIS services.

2.4. At ICANN59 in June 2017, an ad hoc group[3] of community members together with representatives from the ICANN Board of Directors, met to discuss how best to capture the various uses of the current WHOIS services. After receiving submissions from members of the ad hoc group and others, a Personal Data "Use" Matrix was published for community input in July 2017.[4] This document was instrumental in helping to establish the purposes of processing defined in the Interim Compliance Model.

2.5. ICANN org discussed this matrix and next steps in a webinar in October 2017.[5] Following this webinar, ICANN org published the first in a series of three memos by European law firm Hamilton. The first memo highlighted the potentially challenging areas with existing requirements for registries and registrars to provide open, publicly available WHOIS services.[6] The memo concluded that the WHOIS system has to become adaptable to address the GDPR, as well as other changing regulations around the world.

2.6. At ICANN60 in October 2017, after discussions with stakeholders from across the community, ICANN org issued a "Statement from Contractual Compliance", indicating that it would defer taking action against any registry or registrar for noncompliance with contractual obligations related to the processing of personal data under certain conditions.[7] The Statement came in response to questions regarding the timing of ICANN's contractual enforcement in light of the GDPR. Also, at the meeting in Abu Dhabi, ICANN org solicited questions for the next Hamilton memo, which was published in December 2017.[8] Some questions answered in Hamilton memo were in response to questions presented in the ICANN Governmental Advisory Committee (GAC) Communique issued in Abu Dhabi.[9]

2.7. A final memorandum from Hamilton was published later in December.[10] This memo laid out a possible WHOIS model that may be in compliance with the GDPR. This model emphasized the need for tiered or layered access to registration data. ICANN org called for comments on this analysis and suggestions for a path forward. The feedback received, in addition to submitted community-proposed models for compliance, were

[3] https://www.icann.org/en/system/files/files/minutes-gdpr-28jun17-en.pdf
[4] https://www.icann.org/news/blog/personal-data-use-matrix-now-available-for-public-review
[5] https://www.icann.org/resources/pages/data-protection-meetings-2017-12-08-en
[6] https://www.icann.org/en/system/files/files/gdpr-memorandum-part1-16oct17-en.pdf
[7] https://www.icann.org/resources/pages/contractual-compliance-statement-2017-11-02-en
[8] https://www.icann.org/en/system/files/files/gdpr-memorandum-part2-18dec17-en.pdf
[9] https://gac.icann.org/advice/communiques/public/gac-60-abu-dhabi-communique.pdf
[10] https://www.icann.org/en/system/files/files/gdpr-memorandum-part3-21dec17-en.pdf

taken together to help ICANN org draft three possible models for compliance.[11] The purposes of these models, published on 12 January 2018, was to continue to help advance community discussions to settle on a final compliance model. Additional community feedback was received on the three proposed models, both as written correspondence[12] and via a webinar[13] on 2 February 2018. ICANN org followed-up on these discussions by publishing on 28 February 2018 a high-level summary of the proposed final interim model, including a proposal for an accreditation program for continued access to full Thick WHOIS data for accredited users/entities.[14]

2.8. ICANN org continues to engage with contracted parties, DPAs, other government representatives, as well as other stakeholders as we chart a course forward. We were grateful to receive technical input on our proposed compliance models from the European Union in February 2018.[15] Together with input received from across the community, this feedback has guided us toward the proposed final interim model outlined below.

3. WHOIS and Registration Data Processing Today

3.1. WHOIS traces its roots to 1982, when the Internet Engineering Task Force published a protocol for a directory service for ARPANET users. Initially, the directory simply listed the contact information that was requested of anyone transmitting data across the ARPANET. As the Internet grew, WHOIS began to serve the needs of different stakeholders such as domain name registrants, law enforcement agents, intellectual property and trademark owners, businesses and individual users. But the protocol remained fundamentally based on those original IETF standards. This is the WHOIS protocol that ICANN inherited when it was established in 1998.[16]

3.2. Every year, millions of individuals, businesses, organizations and governments register domain names. Each one must provide identifying and contact information which may include: name, address, email, phone number, and administrative and technical contacts. This information is often referred to as "WHOIS data."

3.3. Based on existing consensus policies and contracts with ICANN org, registries and registrars currently are required to provide unrestricted public access to accurate and complete WHOIS information, subject to applicable laws. Additionally, registration data is required to be transferred between registries and registrars as well as data escrow agents for a number of purposes including, to activate and administer domain names

[11] https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf
[12] https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en
[13] https://www.icann.org/resources/pages/data-protection-meetings-2017-12-08-en
[14] https://www.icann.org/en/system/files/files/proposed-interim-model-gdpr-compliance-summary-description-28feb18-en.pdf
[15] https://www.icann.org/en/system/files/correspondence/viola-to-marby-07feb18-en.pdf
[16] https://whois.icann.org/en/about-whois

and to provide redundant instances of registration data to safeguard against the event of a technical or business failure of a registry or registrar.

4. The Need for Interim Change

4.1. The changing legal landscape of data protection laws in jurisdictions around the world has given new prominence and urgency to the long-standing debate about ICANN's policies and agreements requiring free public query-based access to WHOIS. In April 2016, the European Parliament, the European Council and the European Commission adopted a set of rules that will impose new obligations on all companies and organizations that collect and maintain any "personal data" of residents of the European Union. This new regulation, the General Data Protection Regulation (GDPR), replaces the 1995 EU data protection directive and harmonize the data protection rules uniformly throughout the European Union. The GDPR will take effect on 25 May 2018.

4.2. ICANN's Bylaws require that, "Subject to applicable laws, ICANN shall use commercially reasonable efforts to enforce its policies relating to registration directory services and shall work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data."[17] . Also, it is either expressed or implied in ICANN's agreements that the contracted party must comply with all applicable laws.

4.3. Many gTLD registries and registrars are concerned about whether the current ICANN policies and contracts requiring them to collect, create, retain, escrow, and publish a variety of data elements related to registry/registrar operations, domain name registrations, and registrants are in conflict with the GDPR. Registries and registrars requested that ICANN commission a report from "independent counsel" to provide registries and registrars legal guidelines on how to interpret and apply the new law to "provide clear recommendations on how contracted parties operating in the EU can ensure compliance".

4.4. ICANN org has gathered input from the Internet community, including governments and data protection authorities, to understand the scope of interim changes that may be needed to existing practices and requirements concerning registration data while the community considers a longer-term solution through its policy development activities. This interim model for compliance with the ICANN's policies and agreements in relation to the GDPR is outlined in **Section 7** of this document.

[17] ICANN Bylaws, Section 4.6(e)(i))

5. Summary of Community Comments, Legal Analysis, and Response to Community Comments

5.1. The following are summaries of community comments received in response to ICANN org's publication for discussion of a document titled "Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation" dated 12 January 2018 (the "ICANN Proposal"). The summary of comments also includes feedback from various parts of the community during discussions with ICANN org about the ICANN Proposal.

5.2. The summary is organized by the high-level framework elements addressed in each of the compliance models included in the ICANN Proposal. It provides background about each of the elements, including whether there any existing ICANN requirements included in policies or agreements with registries and registrars. After summarizing community comments on the specific framework element, a legal analysis is included to respond to the comments and to provide justification for how the element is treated in the Interim Compliance Model outlined in **Section 7**.

5.3. Data Collection, Processing and Retention

5.3.1. **Purpose Limitation – What is the purpose for the processing activities at issue?**

Background

5.3.1.1. WHOIS is used for many purposes. Under ICANN's existing agreements[18], WHOIS may be used for any lawful purposes except to enable marketing or spam, or to enable high volume, automated processes to query a registrar or registry's systems, except as reasonably necessary to register domain names or modify existing registrations. Aside from this general requirement about the use of WHOIS, there is no existing written policy articulating the purposes of WHOIS.

5.3.1.2. ICANN's Registrar Accreditation Agreement also requires registrars to provide notice to each new or renewed domain name holder stating the purposes for collection of any personal data.[19]

5.3.1.3. The ICANN Proposal outlined a more specific purpose description WHOIS, which purposes included enabling a reliable mechanism for identifying and contacting the registrant and providing a framework to address appropriate law enforcement needs.

[18] Registrar Accreditation Agreement, Section 3.3.5.
[19] Registrar Accreditation Agreement, Section 3.7.7.4.1.

Community Comments

5.3.1.4. In general, commentators did not object to the draft purpose description included in the ICANN Proposal. Some suggested that the description be expanded to more fully set forth all of the purposes for WHOIS data, including unambiguously stating that anti-abuse and compliance activities are legitimate purposes for processing WHOIS data. Also, it was noted that it was important to include a purpose statement about making zone files available to ICANN as this provides essential disaster recovery and compliance capabilities. Some commentators suggested that ICANN reconsider the purpose description to ensure that the description does not focus on the uses of WHOIS, but rather the purposes of WHOIS.

5.3.1.5. Some commentators suggested that none of the purposes included in the ICANN Proposal requires having a Thick WHOIS at the registry level. They suggest that further explanation in the purpose description would be required to justify a requirement for registrars to transfer full Thick WHOIS data to registries.

5.3.1.6. Others contended that the description appropriately sets forth the legitimate purposes, and that the ICANN Proposal should be used as an interim working description while the community works on a final statement as part of the policy development process considering the next generation of WHOIS.

Legal Analysis and Response to Community Comments

5.3.1.7. 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…."[20] This purpose limitation of the GDPR is a foundational principle that must be addressed in the Interim Compliance Model.

5.3.1.8. Taking into account this purpose limitation, it is first necessary to determine the particular purposes for which the WHOIS system as a whole is intended to be used. Such purposes should not be confused with the actual uses of the WHOIS system. These purposes are listed in the revised purpose description in **Section 7.2.1**.

5.3.1.9. Furthermore, it is necessary to determine if such purposes of the WHOIS system are compatible with the original purpose of collecting registrant

[20] Art. 5, Section 1(b) GDPR

personal data, which is performing the domain name registration under the agreement with the registrant, or whether such purposes will require a separate legal basis from the one that allowed the original collection of registrant data. While the legal basis for the processing for the original purpose is mainly "processing necessary for the performance of a contract"[21], the purposes of the WHOIS system relies on the legal basis of "processing necessary for the legitimate interests"[22] of the controller(s) of the WHOIS system and third parties that request access to certain WHOIS data, such as law enforcement authorities.

5.3.1.10. ICANN org takes on board the comments from the community that the purpose description should be revised to include registration data processing activities beyond operating a WHOIS system. In this regard, the purpose description include in the Interim Compliance Model has been expanded to more fully address the processing activities identified by the community comments. Refer to **Section 7.2.1** to review the revised purpose description.

5.3.2. Data Collection/Data Minimization Principle – What data is collected from the registrant?

Background

5.3.2.1. ICANN agreements require registrars (or through a reseller) to collect from registrants certain data associated with registering and administering a domain name. Some of this data may constitute personal data. For example, contact details, including names, phone numbers, postal address, and email addresses for the administrative and technical contacts associated with the domain name registration are required to be collected.

5.3.2.2. A question to be addressed in the Interim Compliance Model is whether all of the data elements required to be collected from registrants under existing ICANN policies and agreements can continued to be collected in light of the GDPR. The ICANN Proposal proposed that registrars must collect from registrants, but not necessarily publish, all personal data currently included in Thick registration data.

[21] Art. 6(1)(b) GDPR
[22] Art. 6(1)(f) GDPR

Community Comments

5.3.2.3. Some commentators suggested that the current data collection practices should be maintained to ensure the data is available for combating abuse, fraud, and malware, even if the information may only be revealed through accredited access, a subpoena or other valid legal instrument. Other commentators explained that there is a continued need for each element of the current Thick WHOIS data set, and continued collection of these elements is consistent with the defined purposes of WHOIS included in the ICANN Proposal. Although supportive of continued collection of Thick WHOIS data, one commenter noted that this practice should only be considered an interim solution, and there should be a proper analysis and complete Privacy Impact Assessment to determine which data fields are needed for specific purposes.

5.3.2.4. Although several commenters supported continued collection of Thick WHOIS data, other commenters asserted that to be compliant with the GDPR, the data that is collected needs to be limited in relation to the purposes for which they are processed. In this light, commentators highlighted that there are outdated fields that should no longer be collected, and ICANN must revise its related requirements. For example, commentators suggested that applying the principle of data minimization requires ICANN org to reassess the necessity of requiring the collection of administrative and technical contact data for all registrations, noting that in more than 90% of the cases, the data included for each contact is identical to the registrant data. These commentators advise that it should no longer be an ICANN requirement for registrars (or through their resellers) to collect from registrants administrative and technical contacts, or billing contacts for those registries who have requirements to do so. The commentators also assert that obtaining data of the non-registrant contacts (e.g. administrative and technical contacts) introduces additional GDPR compliance risk because these contacts may not have a contractual relationship with the registry or registrar. Others note that fax numbers and the physical address of the technical contact are also data elements that are outdated and should no longer be collected.

5.3.2.5. Other commentators have indicated that administrative and technical contact details, even if different in only a small proportion of registrations, have continued relevance in light of the purposes identified for the WHOIS system.

Legal Analysis and Response to Community Comments

5.3.2.6. Under the GDPR, personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."[23] This principle of data minimization is an additional foundational principle that must be addressed in the Interim Compliance Model.

5.3.2.7. ICANN org reviewed each element of registration data required to be collected or generated as part of the domain name registration process taking into account the data minimization principle of the GDPR. This review included looking at previous inputs from the community to develop a gTLD data flow matrix[24], which identified the various uses and more than 70 purposes related to registration data required by ICANN policies and contracts, including purposes identified by registrants, Internet users, and other third parties. Also, ICANN org considered the feedback received in various discussions with and comments from the community. The goal of this exercise was to understand whether there are personal data elements that were no longer relevant in light of the purposes defined for the WHOIS system and other processing activities related to registration data. Based on this analysis, which is included more fully in **Attachment 1**, the Interim Model maintains the existing requirements for registries and registrars to continue to collect the full set of registration data.

5.3.2.8. In some initial discussions about the model, the Registry Registrant ID was discussed as a data field that could potentially no longer be required because it was not clear that there was a continued purpose to justify the field in light of the working description of the purposes of WHOIS included in the ICANN Proposal. It was determined however that the Registry Registrant ID field may have a continued purpose (although not necessarily for publication) in light of RFC 5730[25], which requires that a globally unique identifier must be assigned to every object when the object is created, including contacts/registrants. Additionally, the Registry Registrant ID, implemented using the Repository Object Identifier (ROID), is anticipated to be used for ensuring that variant second-level labels are allocated to the same registrant under a TLD and its variant TLDs, if variant TLDs are eventually agreed by the ICANN Board for delegation.

5.3.2.9. ICANN org also considered the recommendation to revisit the existing requirement for registrars to collect administrative and technical contact

[23] Art. 5(1)(c) GDPR

[24] https://www.icann.org/resources/pages/gtld-registration-dataflow-matrix-2017-07-24-en

[25] http://tools.ietf.org/html/rfc5730

data for all registrations. As noted above, ICANN reviewed each element of registration data and found that maintaining this requirement in the interim model arguably does not result in the collection of much additional data, given that the contact information for administrative and technical contacts is identical to the registrant data in most cases.

5.3.3. **Accuracy of Registration Data**

Background

5.3.3.1. The Registrar Accreditation Agreement includes accuracy requirements such as the validation and verification of some data elements, and the provision of notice to registrants about how to access, and if necessary rectify the data held about them. For example, Section 3.7.7.4.4 of the 2013 Registrar Accreditation Agreement requires that registrars provide notice to registrants stating "[h]ow the Registered Name Holder of data subject can access and, if necessary, rectify the data held about them." Additionally, the WHOIS Data Accuracy Program Specification establishes steps that a registrar must take to validate and verify certain data elements when a domain name is registered, or transferred, for example.

5.3.3.2. The ICANN Proposal did not include any changes to existing requirements in the Registrar Accreditation Agreement.

Community Comments

5.3.3.3. Some commentators have argued that the accuracy principle of the GDPR requires registries and registrars to undertake additional steps to validate the accuracy of the data supplied by the registrant. They propose that data accuracy requirements should be expressly included in any interim compliance model. Other commentators assert that the accuracy principles of the GDPR do not equate to an obligation to verify each individual element of WHOIS information provided by the registrant, and no new requirements are needed to address this aspect of the GDPR.

Legal Analysis and Response to Community Comments

5.3.3.4. The GDPR requires that personal data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay."[26] In

[26] Art. 5(1)(d) GDPR

addition, it is important to note that compliance with local laws is expressed or implied in ICANN's agreements with contracted parties.

5.3.3.5. In principle this accuracy principle is similar in its scope and content to the accuracy principle stated in currently applicable European data protection law[27] and contemplated in the Registrar Accreditation Agreement. (The current Registrar Accreditation Agreement already includes accuracy requirements such as the validation and verification of some data elements, and the provision of notice to registrants about how to access, and if necessary rectify the data held about them.) Also, ICANN has other accuracy related initiatives such as WHOIS Accuracy Reporting System project. The GDPR therefore does not require the introduction of a new verification or validation requirements.

5.3.4. **Data Transfer (to Registry) – What data must the registrar transfer to the registry?**

Background

5.3.4.1. ICANN org's existing contracts and policies require registrars to transfer to registries full Thick registration data.[28] The ICANN Proposal called for this requirement to be maintained to allow for the continued availability of consistent output of registration data from registries and registrars across the WHOIS system.

Community Comments

5.3.4.2. Several commentators supported the approach outlined in the ICANN Proposal to continue requiring registrars to transfer full Thick registration data to the registry. Other commentators argued that the ICANN Proposal does not include sufficient legal grounds to justify the requirement for registrars to transfer data to the registry.

Legal Analysis and Response to Community Comments

5.3.4.3. ICANN org's current contracts and policies require registrars to transfer Thick registration data to the registry. As discussed in the Final Report on the Thick Whois Policy Development Process (21 October 2013)[29], this requirement for Thick data is intended to enhance accessibility and enhance stability by having the data at both the registrar and the registry. Additionally, having the full Thick WHOIS data at the registrar and registry

[27] Art. 6 (1)(d) European Data Protection Directive
[28] https://www.icann.org/resources/pages/thick-whois-transition-policy-2017-02-01-en
[29] https://gnso.icann.org/en/issues/whois/thick-final-21oct13-en.pdf

allows for redundancy in the system to protect registrants such that if "a registrar were to go out of business or experience long-term technical failures rendering them unable to provide service, registries maintaining thick Whois have all the registrant information at hand and could transfer the registrations to a different (or temporary) registrar so that registrants could continue to manage their domain names. A thick Whois model also reduces the degree of variability in display formats. Furthermore, a thick registry is better positioned to take measures to analyze and improve data quality since it has all the data at hand."

5.3.4.4. The transfer of full Thick WHOIS data from a registrar to a registry can be justified based upon the legitimate interests[30] of the various stakeholders who have an interest in the accessibility and stability of the domain name system, including registrars and registries, that the Thick WHOIS data promotes. The GDPR expressly acknowledges processing of personal data "to the extent strictly necessary and proportionate for the purposes of ensuring network and information security" as a legitimate interest,[31] which is an interest very similar to the interest in the accessibility and stability of the domain name system as the overarching reason for maintaining a Thick WHOIS system. The transfer of the Thick WHOIS data by registrars to registries further this interest by allowing continued availability of consistent output of registration data from registries and registrars across the WHOIS system. The Interim Compliance Model's tiered access approach accommodates the interests or fundamental rights and freedoms of the data subject reflected in the domain name registration by limiting public access to the entire Thick WHOIS data.

5.3.4.5. As discussed above, there exists a legitimate basis for the continued requirement for registrars to transfer to registries full Thick WHOIS data as part of the Interim Compliance Model.

5.3.4.6. ICANN org takes on board the comment that the purpose description for the data processing activities should be revised to take into account the processing activity of transferring full Thick WHOIS data from the registrar to the registry. The updated version of the purpose description is included in **Section 7.2.1**.

5.3.4.7. ICANN org is aware that some registries require registrars to transfer additional registration data, for example, to verify that a registrant meets certain eligibility or nexus requirements for having domain name in the specific TLD. Other registries require the registrar to collect and transfer

[30] Art. 6 (1)(f) GDPR
[31] Recital 49 GDPR

billing contact information. Provisions concerning the collection and use of billing contacts or other optional registry-specific elements would need to be addressed in Registry Registrar Agreements.

5.3.4.8. Mechanisms for ensuring binding measures of protection and addressing cross-border transfers would be included in relevant agreements discussed in further detail in **Section 7.2.11**.

5.3.5. **Data Transfer (to Data Escrow Agents) – What data must registries and registrars transfer to the data escrow agents?**

Background

5.3.5.1. Under the data escrow provisions of the Registry Agreement and the Registrar Accreditation Agreement, all gTLD registries and ICANN-accredited registrars must regularly deposit a backup copy of their gTLD registration data with an independent entity acting as a data escrow agent. The data held in escrow may be released to in incumbent registrar/registry upon certain trigging events, such as termination of a registrar's accreditation agreement or expiration of the accreditation agreement without renewal to facilitate transfer of registrations from the failed registrar to another registrar, or a registry operator failure to provide certain critical registry functions. The ICANN Proposal maintained the requirement for registries and registrars to transfer to data escrow agents personal data included in Thick registration data. Full transfer would be required to continue to provide a safeguard for registrants in the event of a business or technical failure of a registrar or registry.

Community Comments

5.3.5.2. Several commentators supported the approach outlined in the ICANN Proposal to continue requiring registries and registrars to transfer full Thick registration data to data escrow agents for the purpose of protecting registrants in the event of registry or registrar failure or termination. Commentators also noted that ICANN org should work to designate a data escrow provider in Europe to reduce the risk faced by European registries and registrars escrowing data outside of Europe.

Legal Analysis and Response to Community Comments

5.3.5.3. ICANN is charged with oversight of the security and stability of the Internet's domain name system. As a function of this responsibility, ICANN requires gTLD registries and accredited registrars to deposit with ICANN, or a designated agent, certain registration records. Upon expiration

without renewal or termination of registrar or registry, the deposited registration records may be utilized to provide transitional registrar services prior to transferring management of the domain name registrations to another registrar, or the registry database to a successor registry operator.

5.3.5.4. Similar to the transfer of full Thick WHOIS data from a registrar to a registry, the transfer of full Thick WHOIS registration data from a registrar or a registry to a data escrow provider can be justified based upon the legitimate interests[32] of the stakeholders who have an interest in the accessibility and stability of the domain name system, as the transfer to a data escrow provider is necessary to ensure transitional services to registrants in case of registrars or registries failing to perform. Therefore, there exists a legitimate basis for the continued requirement for registries and registrars to transfer to data escrow agents full Thick WHOIS data. Because the purpose of processing this data is to protect registrants in the event of loss or unavailability of the registration data from the sponsoring registrar or registry, the full Thick WHOIS data set is necessary to be transferred to the data escrow provider to fulfill this purpose. ICANN org's existing requirements with registries and registrars include limitations on processing the data to serve the given purpose. For example, Section 3.6 of the Registrar Accreditation Agreement requires that "(1) the data shall be received and held in escrow, with no use other than verification that the deposited data is complete, consistent, and in proper format, until released to ICANN; [and] (2) the data shall be released from escrow upon expiration without renewal or termination of this Agreement…." These safeguards balance the need for maintain the escrow of Thick WHOIS data with the interest and fundamental rights and freedoms of the individual registrant (if a natural person) or agents of the registrant (if a legal person).

5.3.5.5. Mechanisms for ensuring binding measures of protection and addressing cross-border transfers would be included in relevant agreements discussed in further detail in **Section 7.2.11**.

5.3.6. **Data Retention – How long must data be retained by registries, registrars and data escrow agents?**

Background

5.3.6.1. The Registrar Accreditation Agreement includes a requirement for registrars to retain certain records relating to a domain registration, which

[32] Art. 6 (1)(f) GDPR.

may include personal data for two (2) years following the domain registration's deletion or transfer away to a different registrar. The Registrar Accreditation Agreement also includes a provision by which registrars may request a waiver from compliance with specific data collection and/or retention requirements if a requirement violates applicable law. Additionally, registrars must use a data escrow agent that will keep and safeguard each deposit of registration data for at least one (1) year.

5.3.6.2. There is no specific ICANN-required retention period under the Registry Agreement, but registries must use a data escrow that will keep and safeguard each deposit of registration data for one (1) year.[33]

5.3.6.3. The ICANN Proposal included a range of retention periods from maintaining the current requirements, to reducing the requirement for registrars to maintain the data for a minimum of 60 days beyond the life of the registration to allow time for any domain name redemption or grace periods after the expiration or transfer of a domain name to run their course, for example, but to be purged shortly thereafter.

5.3.6.4. To develop the Interim Compliance Model, ICANN org has evaluated whether any interim changes need to be made to retention requirements to comply with the GDPR.

Community Comments

5.3.6.5. Community commentators expressed a range of views about appropriate data retention periods. Some commentators supported the position that ICANN org should maintain the status quo retention periods, noting that there is no legal justification for why there needs to be a change to the existing requirements. Also, those supporting existing retention periods highlight that historical WHOIS data is critical to legitimate investigative interests that serve the public interests, including law enforcement and cybercrime investigations that are increasingly global in nature. Additionally, commentators note that ICANN has an existing procedure for contracted parties to request exemptions from existing retention periods if they are in conflict with local law, and as a result, no new requirements or changes are needed to address the GDPR.

5.3.6.6. Other commentators argued that the retention periods should be longer than 2 years and could even be as long as 3 -15 years. These commentators note that retention periods should be long enough to

[33] Registry Agreement, Specification 2, Part B.4.

enable a victim to report a suspected crime by a registrant and allow law enforcement to carry out an investigation. Others noted that a longer retention period is needed to support the purpose of facilitating investigations into infringement of intellectual property.

5.3.6.7. Some commentators argued that the GDPR requires a change from the status quo and that ICANN must reduce the existing data retention requirements in light of the GDPR. These commentators argue that data retention requirements should be left to the contracted parties and their individual business needs, since they are more familiar with local applicable laws and their own business practices. A commentator suggested that a 60-day retention period might be justified at the registrar level as that would be sufficient time for transfer disputes, chargeback controls, and other compliance issues to have run their course. Other commentators, however, noted that even a 60-day retention period may be too long in light of the purposes for which the data was collected.

Legal Analysis and Response to Community Comments

5.3.6.8. Under the GDPR, personal data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed…."[34]

5.3.6.9. As highlighted in the community comments, there exists a legitimate basis for the continued requirement for retention periods related to processing activities associated with registration data. The question is: what is the appropriate length of the retention periods taking into account the purposes for processing the data? **Attachment 2** provides details about the legal basis for retention requirements. Based on this analysis, the legitimate interests of the controllers, data subjects, and third parties justifies maintaining the existing data retention requires, including the existing arrangements for requesting data retention waivers that have already been tailored to comply with European data protection and retention laws.

[34] Art. 5(1)(e) GDPR

5.4. Scope of Applicability of the Interim Compliance Model

5.4.1. **Must the Interim Compliance Model be applied globally or only to European Economic Area?**

Background

5.4.1.1. ICANN agreements with registries and registrars include a single set of rules/obligations and do not distinguish between the location of the registry, registrar, or registrant. One question to be addressed in the Interim Compliance Model is whether it should be applied globally so that the same rules apply across the board no matter the location of the registrant, registrar or registry, or whether the interim changes should be more narrowly applied only where there exists the required nexus to the European Economic Area to trigger the requirements of the GDPR.

Community Comments

5.4.1.2. There are competing community views on this element of the Interim GDPR Compliance Model. Some commentators argue that there should be a harmonized approach and all registration data should be protected, regardless of where someone resides or whether the data flows through or is processed in the European Economic Area. Some noted that not applying the model on a global basis would put registries and registrars at greater risk for non-compliance with the GDPR. Commentators highlight that applying the model globally would promote clarity, predictability and interoperability, which leads to supporting the public interest and the stability of the Domain Name System. Also, some commentators note that it would be technically and administratively difficult, especially in light of the GDPR enforcement deadline, to change the registration system of registries and registrars so that different rules are applied to different registrations.

5.4.1.3. Other commentators have raised concerns that permitting the model to be applied on a global basis is an over-application of the GDPR and not consistent with ICANN org's stated objective to maintain the existing WHOIS system to the greatest extent possible. Some commentators with this view note that despite arguments to the contrary, there are methods that could be used to identify registrations with the required nexus to the European Economic Area and thus it is not technically impossible or impracticable to limit the implementation of the model only where it would be required because of the GDPR. For example, commentators suggest that there could be an additional WHOIS field for a registrant to

self-identify as an EU resident, as well as verification process for the registrar.

5.4.1.4. Some commentators supportive of only applying the model where there is a nexus to the European Economic Area have advised ICANN org to review the language in the ICANN Proposal used to describe how the territorial scope of the GDPR maps to the location and processing activities of registrants, registries, and registrars.

Legal Analysis and Response to Community Comments

5.4.1.5. Relevant to the data processing activities in the domain name ecosystem, the GDPR applies to "the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not." Additionally, the GDPR applies to "the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union…."[35] The GDPR Recitals provide guidance on how to determine whether a controller or processor outside of the European Economic Area is offering goods or services to data subjects who are in the EEA. The "mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union."[36]

5.4.1.6. Given this, the GDPR would apply in the context of registrants, registries and registrars where:

(i) the registrar and/or registry are established in the European Economic Area (EEA) and process personal data included in registration data;

[35] Art. 3 GDPR
[36] Recital 23 GDPR

(ii) the registrar and/or registry are established outside the EEA and offer services to registrants located in the EEA involving the processing of personal data from registrants located in the EEA; or

(iii) the registrar and/or registry are located outside the EEA and process non-EEA personal data included in registrations, where registry and/or registrar engage a processor located within the EEA to process such personal data.

5.4.1.7. It is a particular feature of the GDPR to provide for extra-territorial application to controllers and processors outside of the EU already when their processing activities are related to offering goods or services to data subjects in the EU. Other than under currently applicable law, non-EU processors can be subject to direct application of the GDPR under these circumstances, and it is furthermore not required that the non-EU controller or processor makes use of equipment located in a member state for the purpose of processing personal data.[37] The rationale behind the broadened territorial scope of the GDPR was to ensure the protection of EU data subjects in cases in which controllers or processors not established in the EU nevertheless address their business activities to EU data subjects. With regard to the WHOIS system, however, the extra-territorial reach of the GDPR leads to difficulties in determining the exact scope of application of the GDPR. Registrars will hardly want to exclude the EU from their service offerings. At the same time providing for different rules for processing registrant data is difficult in practice. Also taking into account that an increasing number of countries, for example, in the Asia-Pacific region and in South America have adopted or are in the processing of adopting GDPR-like data protection regimes, adopting GDPR requirements as the global standard for WHOIS data processing activities in connection with the WHOIS system may provide for greater uniformity and consistency for these other jurisdictions.

5.4.1.8. Taking the above into account, the Interim Compliance model requires registries and registrars to apply the model to collection and processing linked to the European Economic Area, while providing the option to apply the model beyond the European Economic Area. The option to apply the model on a global basis recognizes that there are data protection regulations similar to the GDPR in other jurisdictions and commentators have suggested that registries and registrars may need the flexibility to apply the changes more globally. Also, it could potentially put registries and registrars not established in the EEA at a competitive disadvantage if contracted parties do not have the option to apply the model on a global basis. Furthermore, it may be difficult in practice only to apply the changes

[37] Art. 4 (1)(c) European Data Protection Directive

to collection and processing linked to the European Economic Area depending upon how an individual registry or registrar has set up its systems.

5.4.1.9. Mechanisms for ensuring binding measures of protection and cross-border transfers would be included in relevant agreements discussed in further detail in Section 7.2.11.

5.4.2. **Does the GDPR apply to domain name registrations of legal persons?**

Background/Issue

5.4.2.1. ICANN agreements with registries and registrars do not include provisions requiring a distinction between the treatment of domain name registrations where the registrant is a natural person versus domain name registrations where the registrant is a legal person. One question to be addressed in the Interim Compliance Model is whether registrations of legal and/or natural persons would be affected.

Community Comments

5.4.2.2. There are competing community views on this element of the Interim Compliance Model. Some commentators have raised concerns that not distinguishing between registrations of legal and natural persons is an over-application of the GDPR and not consistent with ICANN org's stated objective to maintain the existing WHOIS system to the greatest extent possible. Also, these commentators note that the GDPR does not apply to processing of personal data which concerns legal persons, and as a result, the Interim Compliance Model should require registrars to distinguish between registrations of legal and natural persons, and making sure registrations of natural persons include less information in public WHOIS than registrations of legal persons. It was also noted that distinguishing between registrations of natural and legal persons is warranted from data protection and public safety perspectives.

5.4.2.3. Other commentators assert that registrations of both legal and natural persons would be impacted by the GDPR and thus should be within the scope of applicability of the Interim Compliance Model. These commentators highlight that registration data of a legal person could contain personal data of natural persons, which are within the scope of the GDPR. Additionally, some commentators note that differentiating between registrations of legal and natural persons is not manageable without significant administrative effort.

Legal Analysis and Response to Community Comments

5.4.2.4. The GDPR applies to the processing of personal data which is clearly defined as any information relating to an identified or identifiable natural person, the data subject.[38] Thus, registrations that include personal data of natural persons are subject to the GDPR. Still it is not always easy to draw a clear line between personal data relating to natural or to legal persons, for example, in case of natural persons with such a close financial, personal or commercial entanglement with the legal person so that information about the legal person can be related to such natural persons (e.g., in case of a sole proprietorship or a GmbH owned by one person).

5.4.2.5. Also, while it is true that the GDPR does not protect data pertaining to legal persons, several commentators have noted the registrations of legal persons may include personal data of natural persons. Also, it may be difficult in practice to check millions of registration records and distinguish between registrations of legal and natural persons.

5.4.2.6. Considering the above, the Interim Compliance Model will apply to all domain name registration personal data that is contained in the WHOIS system.

5.5. Public WHOIS

Background

5.5.1. Based on existing consensus policies and contracts with ICANN org, registries and registrars currently are required to operate a registration data directory service (e.g. WHOIS) providing free public query-based access to up-to-date data concerning active domain name registrations.[39]

5.5.2. ICANN org understands that current requirements for unrestricted public access to WHOIS cannot continue in light of the GDPR, and the ICANN Proposal included layered/tiered access to WHOIS data. A question to be addressed in the Interim Compliance Model is what data elements can continue to be published in public layer of WHOIS.

[38] Art. 4(1) GDPR

[39] Registry Agreement, Specification 4; Registrar Accreditation Agreement, Registration Data Directory Service (WHOIS) Specification

Community Comments

5.5.3. Commentators expressed a range of views about which data elements could continue to be published in public WHOIS.

Registrant Contact Data, Generally

5.5.4. Commentators expressed varying views on the degree to which contact information about the registrant should be required to be published in public WHOIS. Some commentators asserted that the registrant's data should be included from a public safety perspective. Others noted that publishing certain contact details of the registrant, including name and email address may be consistent with ICANN's mission. Some commentators highlight that registrants using their domain name for trade/commerce should be required to include more fulsome details about the registrant, and for example, a registrant that is a legal person should be required to include all or most of the contact details so that consumers are able to verify the entities they are transacting with online. Some commentators note that a registrant's phone number should also be required to be included in the public WHOIS because it is a unique data field and could be used when conducting reverse queries.

5.5.5. Others noted that applying the GDPR's principle of data minimization, not all information should be made publicly available, including the registrant's name. Some commentators supported an approach where each data element should be assessed to see whether it contains personal data and whether public access to such personal data is necessary and proportionate.

5.5.6. Some commentators request more guidance from DPAs on this issue, noting that registries and registrars would be assuming significant and likely unsustainable level of risk without assurances about what contact information can legally be included in public WHOIS.

5.5.7. There were two primary areas of focus of the community comments with respect to which minimum elements of contact data should be required to be published about the registrant: registrant email and registrant postal address. Commentators expressed competing views on these data elements, which are described below.

Registrant Postal Address

5.5.8. Some commentators argue that the elements of the registrant's postal address to identify the jurisdiction of the registrant should be required. They suggest that this should include the registrant's state/province and country. Others propose that additional elements of the postal address are necessary in order to establish jurisdiction, such as the particular city and/or postal code of the registrant. Also, some note that academic and non-profit researchers make use of domain name counts, domain name

geographies, and related metrics for academic and research purposes. Because of this, they propose that more of the address fields should be a required part of public WHOIS.

5.5.9. Other commentators argue that any publication of a registrant's address is an extreme intrusion into the data subject's rights given that purpose for having WHOIS data public, and hence this personal data should not be freely accessible to all in public WHOIS.

Registrant Email Address

5.5.10. Some commentators argued that the registrant's email address should continue to be available in the public WHOIS. The commentators highlight that making the registrant's email address publicly available supports a number of legitimate purposes including, contacting a victim of malware campaigns and analyzing patterns of malicious registrations. Various commentators report that the registrant's email address in public WHOIS is the most valuable piece of information in the WHOIS record for detecting bad faith or abuse, and preventing cyber threats, illegal activity, and consumer abuse. Some note that by only allowing access to accredited-users, it will make it more difficult to identify the true identities of criminal offenders and to conduct investigations and enforcement actions concerning criminal illegal activity. Also, email addresses are critical to the ability of consumers to verify the identity of those providing online goods and services. Commentators highlight that the registrant's email address is the data element most likely to be accurate because it is needed for the registrar to communicate with the registrant and verify information in the registration process.

5.5.11. Other commentators argue that the registrant's email address should only be included if the registrant provides voluntary and informed consent to do so, particularly where the registrant may desire to be contacted concerning domain name transfers and other inquiries that are in the interest of the data subject, without payment of a privacy or proxy service. Some commentators suggest that there are other technical methods of contacting a registrant, without including the registrant's actual email address in public WHOIS. For example, some suggested that a CAPTCHA-protected web form could be used to deliver email to the appropriate contact without need of a warrant or subpoena to be obtained to reveal the actual email address.

Administrative and Technical Contact Data

5.5.12. Several commentators suggest that at a minimum, the email addresses for the administrative and technical contacts should be included in the public WHOIS, noting that this would help ensure that the decentralized technical infrastructure of the DNS continues to operate in a secure and stable manner.

5.5.13. Some commentators suggest that it most cases, it may not be necessary to publish the contact details of the administrative and technical contacts because they are identical to the registrant's contact details. Other commentators note that a case-by-case

assessment should be undertaken to see if personal data is included in the administrative and technical contact data fields.

5.5.14. Other commentators suggested that it would be better to use "role contacts" for the registrant, administrative and technical contacts, as this would achieve the same purposes in a less-intrusive manner into the data subject's rights.

Legal Analysis and Response to Community Comments

5.5.15. Generally, the GDPR principles relating to processing of personal data requires that registrant personal data be processed lawfully and fairly, for a legitimate purpose, and that it be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed."[40] Hence, publishing the public WHOIS data that contains all personal data in the Think Whois data is not appropriately minimized given the general purposes identified above because these purposes can be satisfied with less personal data made available in the public WHOIS.

5.5.16. In light of these legal requirements, the Interim Compliance Model strikes a balance between the competing community viewpoints, the legitimate interest of stakeholders, and the rights of freedoms of data subjects whose personal data are included in public WHOIS. Specifically:

(i) The registrant "name" field will not be published in public WHOIS. However, the registrant "organization" would be required to be published (if applicable) so that registrations of legal entities would readily include the name of the entity.

(ii) The registrant's state/province and country will be published, but the address fields that could be used to more specifically identify the registrant would not be included in the public WHOIS (e.g. street, city, postal code). This would enable non-accredited users to determine the registrant's general location and likely jurisdiction but would generally not enable identification of the registrant.

(iii) The public WHOIS will include an anonymized email address or a web form from which messages could be forwarded to the registrant email address. This approach will enable non-accredited users to contact, but not identify, the registrant.

(iv) The registrant phone and fax would not be required to be published in public WHOIS.

(v) Similar to the registrant email field, the public WHOIS will include anonymized email addresses or a web form from which messages could be forwarded to the

[40] Art. 5(1)(a) GDPR; Art. 5(1)(b) GDPR; Art. 5(1)(c) GDPR.

administrative and technical contact email addresses. No other contact details of the administrative and technical contacts would be published in public WHOIS.

5.6. Access to Non-Public WHOIS – Accreditation Program

Background

5.6.1. As previously discussed, ICANN's existing consensus policies and contracts with registries and registrars require public query-based access to WHOIS. The layered/tiered access included in the Interim Compliance Model represents a shift from current requirements.

5.6.2. Some issues to be addressed in the Interim Compliance Model are: who can access non-public WHOIS data, and by what method? The ICANN Proposal and community discussions identified the following possible approaches for providing access to full WHOIS data to third-party requesters: (1) a self-certification approach where certain third-parties identify their legitimate purpose for access to the data and agree to use the data for the identified limited purpose, (2) a certification approach where certain third-parties identify their legitimate purpose for access to the data and agree to use the data for the identified limited purpose and in compliance with an approved code of conduct, (3) an accreditation approach where a defined set of third-party requesters are certified under an accreditation program have access to the data after being accredited/certified, and (4) a legal due process approach where access is only granted when required by applicable law, such as when the third-party requestor provides a subpoena or any other order from a court or other judicial tribunal of competent jurisdiction.

Community Comments

Self-certification Approach

5.6.3. Some commentators supported the self-accreditation approach, noting that self-certification is the only practical approach in the short-term to continue to provide access to full WHOIS data to those with a legitimate purpose. They suggest that a self-certification approach could follow a similar approach as requests from third-parties to access zone data files, which is not overly burdensome to provide access to users with a legitimate purpose.

5.6.4. Others found the self-accreditation approach to be overly burdensome for registries and registrars to review requests on a case-by-case basis. They suggest that if a self-certification approach is selected, there should be established criteria so that registries and registrars apply the rules consistently across all gTLDs. Also, they suggest that those who self-certify to their legitimate purpose for access to the full WHOIS data should be

given automatic access, or only minimally require a case-by-case review by registries and registrars in limited circumstances. In this way, they assert that access to critical data would not be significantly delayed and this would provide greater certainty to users and lessen the burden on registries and registrars. Others noted that registrars should not have discretion in responding to requests from third-parties because some may choose to shield criminals by refusing to share information in the name of protecting a registrant's privacy.

5.6.5. Other commentators questioned whether providing access through a self-certification approach would be a rigorous enough process to meet the mandates of GDPR, and suggested that additional input from DPAs may be needed about this approach.

Accreditation Approach

5.6.6. Several commentators supported an accreditation approach, noting that as a compliance matter, it seemed to be a better solution than the self-certification approach. Some took note of possible benefits of an accreditation approach, which included: (i) ease of access to full WHOIS data, (ii) lessening the burden on registries and registrars to deal with requests, (iii) allowing for fair and consistent release of data across registries and registrars, and (iv) protecting confidentiality concerns associated with law enforcement investigations. Some commentators also made suggestions about which user groups should be accredited for access to full WHOIS data, which included law enforcement, intellectual property rights holders, and industry and academic partners.

5.6.7. Some commentators raised concerns about how practically an accreditation program would be implemented in time for compliance with the GDPR. Although supportive of an accreditation approach, they advise that ICANN and the community need to discuss an "interim" solution for providing access to full WHOIS data given the time constraints. One commentator suggested that layered access may be feasible if it is based on automatically qualified parties adhering to a code of conduct or other similar policy.

5.6.8. Other commentators made suggestions about how much data should be available to accredited users. Many suggested that access should be grant to the full WHOIS data set. Others commented that if an accreditation approach is adopted, there should be bulk access to all WHOIS records to detect and mitigate abuse. One commentator noted, however, that even if access is provided to accredited users, it may not need to be full access to WHOIS data. They highlighted that the need to disclosure information about the registrant, for example, could be alleviated through the use of registry-level contact forms, similar to the approach of some ccTLDs.

Legal Due Process Approach

5.6.9. Commentators suggested that instead of developing a complex, and potentially contentious accreditation program, ICANN should instead rely on existing legal mechanisms that would allow third-parties to have access to the data (i.e. warrant or subpoena). Some noted that this approach is the most protective from a data protection perspective.

5.6.10. Other commentators argued that it would be unreasonable and unacceptable to require third-parties to obtain a court order to be granted access to non-public WHOIS data. They note that such an approach could have a negative impact on many legitimate uses of WHOIS data. For example, some note that this approach could impede law enforcement and intellectual rights holders from being able to quickly identify possible criminal activity and infringement of protected marks. However, one commentator noted that the legal due process approach would be appropriate for law enforcement as law enforcement should only have access when required by law and subject to due process.

Legal Analysis and Response to Community Comments

5.6.11. In light of the community comments and legal considerations, to access registration data not published in the public WHOIS, the Interim Compliance Model will require registries and registrars to provide access to non-public registration data only for a defined set of third-party requestors certified under a formal ICANN-managed accreditation program. Under this approach, user groups with a legitimate interest and who are bound to abide by adequate measures of protection, for example law enforcement agencies and intellectual property lawyers, could access non-public WHOIS data based on pre-defined criteria and limitations under the formal accreditation program. This approach attempts to provide a method beyond legal due process to provide continued access to full Thick WHOIS data for legitimate purposes consistent with the GDPR.

5.6.12. It will be necessary to engage with EU data protection authorities to define and reach agreement on the accreditation approach that satisfies the requirements of the GDPR, which approach could include the certification of codes of conduct or participation in a data protection certification. The formal accreditation program would consider mechanisms contemplated by the GDPR, in particular under Art. 40 (with respect to consultation and approval of a "WHOIS data access code of conduct" for defined WHOIS stakeholders), Art. 41 (with respect to the function of an accredited supervising body to monitor compliance with a "WHOIS data access code of conduct"), and Art. 42 and Art. 43 (with respect of permitting certified controllers and processors to access non-public WHOIS data that are certified by accredited certification bodies). The formal accreditation program structure, participation terms, data access approach, and supervision will be developed and implemented to (i) ensure the adoption and

implementation of a code of conduct and participation terms on the basis of binding and enforceable commitments, including a showing of purpose and legitimate interest, (ii) require the application of appropriate safeguards on the access and further processing of the WHOIS data, (iii) impose binding obligations on the application of appropriate safeguards with respect to rights of data subjects, and (iv) as appropriate, require the accredited/certified controller/processor to submit to supervision and oversight concerning compliance.

5.6.13. Please refer to **Attachment 4** for additional details about the accreditation program.

5.7. Other Processing Activities Concerning Registration Data

ICANN policies and agreements with registries and registrars require processing of registration data, including personal data, other than for registration directory services/WHOIS. Some commentators noted that the ICANN Proposal did not address these processing activities and needed to do so in order to ensure that the Interim Compliance Models address all relevant activities. The following includes discussion of these additional processing activities.

5.7.1. Bulk Registration Data Access to ICANN

5.7.1.1. The Registry Agreement includes a requirement for registry operators to provide ICANN with certain registration data on a weekly basis.[41] The agreement states, "Registry Operator will provide, at least, 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, at least, it will provide: registrar name, registrar id (IANA ID), hostname of registrar Whois server, and URL of registrar."

5.7.1.2. This data is collected by ICANN org for the limited purposes of verifying and ensuring operational stability of registry services as well as to facilitate compliance checks on accredited registrars.

5.7.1.3. When submitting bulk registration data to ICANN, some registry operators submit full WHOIS data, instead of the minimum data set required by the agreement. In light of the limited purposes for which ICANN collects bulk access to registration data, the Interim Compliance Model will include a requirement that registries must only submit the specific minimum data set required by the agreement so that the data collection is minimized to what is required for the purposes articulated. The Interim Compliance Model will allow ICANN to either reject bulk registration data with full WHOIS data, or to remove full WHOIS date from the submission.

[41] Registry Agreement, Specification 4, Section 3.1.

5.7.2. Emergency Back-End Registry Operator

5.7.2.1. The establishment of Emergency Back-End Registry Operators, or EBEROs, are an important innovation of the New gTLD Program. The purpose of the EBERO program is to mitigate risks to the stability and security of the Domain Name System in the event of New gTLD operator failure. Several legacy gTLDs have also agreed to the EBERO program.

5.7.2.2. Emergency back-end registry operators are temporarily activated if a gTLD registry operator is at risk of failing to sustain any of the five critical registry functions, including WHOIS.

5.7.2.3. EBEROs are limited in the services they can provide. For example, EBEROs do not provide any additional services that a gTLD operator may have offered its customers, such as web hosting or network analytics. In the event ICANN designates an EBERO, the registry operator is required to provide ICANN or the EBERO with all data, including data escrowed with a Data Escrow Provider, regarding operations of the TLD.

5.7.2.4. Currently, ICANN has contracts with three entities who have agreed to serve as EBEROs.[42] Among other things, the agreements include provisions on required safeguards for handling personal data and how long data should be retained.

5.7.3. EBERO providers are data controllers under the GDPR and, form a data protection perspective, will be required to participate in the Interim Compliance Model in a similar manner as registries. ICANN org will work with EBERO providers to implement the necessary contractual binding commitments needed for compliance with the GDPR. Also, the purposes of processing will be revised to address processing activities associated with EBEROs.

5.7.4. Searchable WHOIS

5.7.4.1. Some registry operators WHOIS service includes web-based search capabilities by domain name, registrant name, postal address, contact names, registrar IDs, and Internet Protocol addresses without arbitrary limit. Boolean search capabilities also may be offered. This feature is commonly referred to as “searchable WHOIS”. When providing this service, registry operators must include appropriate precautions to avoid abuse of this feature (e.g. limiting access to legitimate authorized users),

[42] https://www.icann.org/resources/pages/ebero-2013-04-02-en

and to demonstrate compliance with any applicable privacy laws or policies.

5.7.4.2. The Interim Compliance Model will require changes to the Registry Agreements requiring relevant registries to implement access to searchable WHOIS services consistent with the Interim Compliance Model's approach concerning access to public and non-public WHOIS data.

5.7.5. Zone File Access

5.7.5.1. The Registry Agreement requires registry operators to enter into agreements with Internet users, which will allow such user to access an Internet host server or servers designated by the registry operator and download zone file data. For most registry operators, access to the zone files is facilitated and administered by a Centralized Zone Data Access Provider, which may be ICANN or an ICANN designee ("CZDA Provider").[43]

5.7.5.2. Internet users requesting access to the zone files through the Centralized Zone Data System (CZDS) provide personal data, including name, email, postal address, and phone number. This information is used for the purposes of providing credentials for users to access CZDS.

5.7.5.3. Additionally, registry operators are currently required to provide bulk access to the zone files to ICANN or its designee, and to Emergency Backend Registry Operations designed by ICANN in support of ICANN's security and stability mandate.

5.7.5.4. ICANN org will update the purposes of processing to address zone file access. ICANN org will also review the Terms of Use associated with the CZDS to ensure that the purposes of processing are clearly explained to the requesting party at the time of collection of the personal data, implement consent to processing, and confirm compliance with the GDPR's processing principles under Art. 5 GDPR.

6. Guiding Principles for the Interim Compliance Model

ICANN org's Interim Compliance Model takes into account the following:

6.1. The model represents an interim solution for compliance with existing ICANN agreements and policies. The selected model does not replace the multistakeholder policy development and implementation activities that are underway, including efforts

[43] Registry Agreement, Specification 4, Section 2.

to enhance privacy and proxy services available to registrants, updates to ICANN's Procedure for Handling WHOIS Conflicts with Privacy Law, and community activities working to develop a new policy framework to support potential next-generation registration directory services to replace WHOIS.

6.2. The model balances compliance with the GDPR while maintaining the existing WHOIS system and procedures concerning registration data to the greatest extent possible.

6.3. ICANN org is guided by its Bylaws in developing the Interim Compliance Model. With respect to WHOIS, ICANN's Bylaws require that, "Subject to applicable laws, ICANN shall use commercially reasonable efforts to enforce its policies relating to registration directory services and shall work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data."[44]

6.4. ICANN org acknowledges that it is either expressed or implied in all of ICANN org's agreements that the contracted party must comply with all applicable laws.

6.5. The Interim Compliance Model accounts for the range of views expressed by the ICANN community about impacts of GDPR on WHOIS and other gTLD registration data.[45] When developing the model, ICANN org considered the community work/input to develop the dataflow matrix of user stories for WHOIS,[46] input from data protection authorities, GDPR compliance models proposed by community members,[47] guidance from European ccTLD registry operators,[48] community discussions at ICANN meetings,[49] and other questions, input, and analyses submitted by ICANN stakeholders.

6.6. The Interim Compliance model requires layered/tiered access to WHOIS data. This is a shift from the current WHOIS system. This feature is embedded in the model based on the series of legal analyses from the Hamilton law firm[50] and the Article 29 Working Party feedback indicating that "ICANN and the registries would also not be able to rely on a legitimate interest for making available all personal data in WHOIS directories to the general public"[51]. This feedback suggests that legitimate interest possibly could be used as the basis for a limited public WHOIS.

---

[44] ICANN Bylaws, Section 4.6(e)(i) https://www.icann.org/resources/pages/governance/bylaws-en/#article4

[45] https://www.icann.org/resources/pages/data-protection-correspondence-2017-12-08-en

[46] https://www.icann.org/resources/pages/gtld-registration-dataflow-matrix-2017-07-24-en

[47] https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en

[48] https://www.icann.org/en/system/files/correspondence/plexida-to-sahel-29oct17-en.pdf

[49] https://schedule.icann.org/event/CbHj/cross-community-session-general-data-protection-regulation-gdpr-implications-for-icann

[50] https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en

[51] https://www.icann.org/en/system/files/correspondence/falque-pierrotin-to-chalaby-marby-06Dec17-en.pdf

6.7. The Interim Compliance Model represents ICANN org's analysis of what ICANN org would require for compliance with ICANN policies and agreements with registries and registrars. Nothing in this document is legal advice. Registries and registrars should continue to engage with their own legal counsel on how to comply with the GDPR and privacy laws in other jurisdictions.

7. Interim Compliance Model

7.1. Overview of the Interim Compliance Model

7.1.1. The Final Interim Model balances competing elements of models submitted by the community and discussed in comments to the ICANN-proposed models. Consistent with ICANN org's stated objective to identify the appropriate balance for a path forward to ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible, the Final Interim Model maintains robust collection of registration data (including registrant, administrative, and technical contact information), but restricts most personal data to layered/tiered access via an accreditation program to be developed in consultation with the Governmental Advisory Committee (GAC), DPAs and contracted parties with full transparency to the ICANN community. Layered/tiered access is a key feature of the model and is a significant change to the current WHOIS system.

7.1.2. Users without accreditation for full WHOIS access would maintain the ability to contact the registrant or administrative and technical contacts, either through an anonymized email, web form, or other technical and legal means. The Final Interim Model must be implemented where required because of a nexus to the European Economic Area, while providing flexibility to registries and registrars to apply the model on global basis based on implementability and fairness considerations. The model applies to all registrations, without requiring registrars to differentiate between registrations of legal and natural persons. The model includes binding contractual commitments between and among ICANN, registries, registrars, data escrow agents, and other contracting parties as necessary for compliance with the GDPR.

7.2. Interim Compliance Model

7.2.1. **Purposes of Processing**

In support of ICANN's mission to coordinate and ensure the stable and secure operation of the Internet's unique identifier system, personal data included in registration data may be processed for the following purposes:

7.2.1.1. Maintaining the availability of Registration Data Directory Services/WHOIS subject to applicable laws promotes trust and confidence in the Internet for all stakeholders. ICANN's Bylaws state: "Subject to applicable laws, ICANN shall use commercially reasonable efforts to enforce its policies relating to registration directory services and shall work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data."

7.2.1.2. For these reasons, it is desirable to have a WHOIS system, the purposes of which include:

a. Providing legitimate access to accurate, reliable, and uniform registration data;
b. Enabling a reliable mechanism for identifying and contacting the registrant;
c. Enabling the publication of technical and administrative points of contact administering the domain names at the request of the registrant;
d. Providing reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names;
e. 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;
f. Providing a framework to address appropriate law enforcement needs;
g. Facilitating the provision of zone files of gTLDs to Internet users;
h. Providing mechanisms for safeguarding registrants' registration data in the event of a business or technical failure, or other unavailability of a registrar or registry;
i. Coordinating dispute resolution services for certain disputes concerning domain names;
j. Handling contractual compliance complaints submitted by registries, registrars, registrants, and other Internet users.

7.2.2. **What data must be collected by the registrar at time of registration?**

Registrars must collect from registrants the full Thick WHOIS data. Continuing to collect, while not necessarily publishing the full Thick WHOIS data, will allow the existing data to be preserved while the community discussions continue on the next generation of WHOIS.

7.2.3. **What data must the registrar transfer to the registry?**

Registrars must transfer to the registry the full data set collected from the registrant. This will allow the continued availability of consistent output of registration data from registries and registrars across the WHOIS system.

7.2.4. **What data must registrars and registries transfer to the data escrow agents?**

Registries and registrars must continue to transfer the full data set collected from the registrant or transferred to the registry to the data escrow agent. Full transfer is required to continue to provide a safeguard for registrants in the event of a business or technical failure of a registrar or registry.

7.2.5. **How long must data be retained by registries, registrars and data escrow agents?**

No new retention requirements are required by the Interim Compliance Model. Registrars must continue to retain the registration data for two years beyond the life of the domain name registration, unless a shorter time has been granted by a data retention waiver from ICANN. This approach maintains existing arrangements and waivers that have already been tailored to comply with European data protection and retention laws.

7.2.6. **What is the scope of applicability of the model?**

Registries and registrars are required to apply the model to collection and processing linked to the European Economic Area. Registries and registrars, may, but are not required to apply the model beyond the European Economic Area. Specifically:

a. Registries and registrars must apply the model to personal data included in the registration data of natural and legal persons where:

i.

(i) the registrar and/or registry are established in the European Economic Area (EEA) and process personal data included in registration data;

(ii) the registrar and/or registry are established outside the EEA and offer services to registrants located in the EEA involving the processing of personal data from registrants located in the EEA; or

(iii) the registrar and/or registry are located outside the EEA and process non-EEA personal data included in registrations, where registry and/or registrar engage a processor located within the EEA to process such personal data.

b. Registries and registrars may, but are not be required to, apply the Interim Compliance Model to registrations without regard to location of the registrant, registry, registrar or a processor of the registration data.

7.2.7. **Does the model propose layered/tiered access?**

The Interim Compliance Model requires tiered/layered access to WHOIS data. This feature is based on the series of legal analyses from the Hamilton law firm and the Article 29 Working Party feedback indicating that "ICANN and the registries would also not be able to rely on a legitimate interest for making available all personal data in WHOIS directories to the general public". This feedback suggests that legitimate interest possibly could be used as the basis for a limited public WHOIS.

7.2.8. **What registration data must be published in public WHOIS?**

7.2.8.1. Registrars must provide registrants the opportunity to opt-in to publication of full contact details in the public WHOIS. The registrant's consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the registrant's agreement to the processing of personal data relating to him or her. The consent must be withdrawable at any time and otherwise consistent with the requirements of the GDPR (e.g., a domain name registration cannot be denied on the basis that the registrant has not consented to the publication of the full WHOIS data).

7.2.8.2. Unless the registrant otherwise grants permission, registries and registrars would be required to display in public WHOIS:

(i) the name of the Registered Name;
(ii) information about the primary and secondary nameserver(s) for the Registered Name;
(iii) information about the Registrar;
(iv) the original creation date of the registration;
(v) the expiration date of the registration; and
(vi) the following additional minimum data:

7.2.8.3. The registrant "name" field shall not be published in public WHOIS. However, the registrant "organization" is required to be published (if applicable) so that registrations of legal entities would readily include the name of the entity.

7.2.8.4. The registrant's state/province and country must be published, but the address fields that could be used to more specifically identify the registrant must not be included in the public WHOIS. This will enable non-accredited users to determine the registrant's general location and likely jurisdiction but will generally not enable identification of the registrant.

7.2.8.5. The public WHOIS must include an anonymized email address or a web form from which messages could be forwarded to the registrant email address.

7.2.8.6. The registrant phone and fax are not required to be published in public WHOIS.

7.2.8.7. The Admin and Tech contact names are not required to be published in public WHOIS.

7.2.8.8. The Admin and Tech contact phone and fax are not required to be published in public WHOIS.

7.2.8.9. The Admin and Tech contact phone and fax are not required to be published in public WHOIS.

7.2.8.10. The public WHOIS must include anonymized email addresses or a web form from which messages could be forwarded to the Admin and Tech contact email addresses.

7.2.8.11. A sample of the minimum WHOIS output fields is included in **Attachment 3**.

7.2.9. **Who can access non-public WHOIS data, and by what method?**

7.2.9.1. To access registration data not published in the public WHOIS, registries and registrars must provide access to non-public registration data only for a defined set of third-party requestors approved under a formal accreditation program administered by ICANN. Under this approach, approved user groups, such as law enforcement agencies and intellectual property lawyers, could access non-public WHOIS data based on pre-defined criteria and limitations that would be established as part of the formal accreditation program. This approach attempts to provide a method beyond legal due process to provide continued access to full Thick WHOIS data for legitimate purposes consistent with the GDPR.

7.2.9.2. 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) and relevant EU data protection authorities so that public policy considerations and data protection authority concerns 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 approved for access to non-public WHOIS data.

For entities other than law enforcement agencies, the GAC could develop "WHOIS data access 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, taking into consideration the GDPR certification programs contemplated under Art. 42 GDPR.

7.2.9.3. Should the accreditation program not be ready to be implemented at the same time as the layered access model, some commentators have suggested "self-certification" as an "interim" solution, however this would raise a number of questions that would need to be addressed to comply with the GDPR.

7.2.9.4. Registries and registrars would be permitted (but not required by ICANN), to provide additional access to non-public WHOIS as long as it complies with the GDPR and other applicable laws. This is an additional topic that could be the subject of binding contractual commitments between and among ICANN, registries, and registrars.

7.2.9.5. Additional details about the proposed accreditation program for continued access to full Thick WHOIS data are included in **Attachment 4**.

7.2.10. **Will the changes to WHOIS and other registration data processing activities impact other ICANN Consensus Policies or procedures?**

7.2.10.1. Transfer Policy. The Transfer Policy[52] relies on the gaining registrar having access to certain data elements in public WHOIS, including the names of the registrant and administrative contacts. The information in public WHOIS is used to verify who has the authority to approve or deny a transfer, and to contact the relevant parties. Given that the information needed to effectuate transfers will not be required to be included in public WHOIS under the Interim Compliance Model, registrars will be accredited for access to full WHOIS data for the limited purpose of facilitating transfers of domain names.

7.2.10.2. Dispute resolution policies and procedures. There are several gTLD dispute resolution procedures either required by ICANN policies or agreements. These dispute resolution mechanisms include for example, the Uniform Domain Name Dispute Resolution Policy (UDRP)[53], the Uniform Rapid Suspension System (URS), and the Registrar Transfer Dispute Resolution

[52] https://www.icann.org/en/resources/registrars/transfers
[53] https://www.icann.org/en/help/dndr/udrp

Policy[54]. Several of these dispute resolution providers rely on the availability of information in the public WHOIS to adjudicate disputes. Given that some of the information that may be needed to administer ICANN dispute resolution policies and procedures will not be required to be included in public WHOIS under the Interim Compliance Model, ICANN-approved dispute resolution service providers will be accredited under the formal accreditation program for access to full WHOIS data for the limited purpose of administering relevant dispute resolution procedures.

7.2.10.3. Registry Registration Data Directory Services Consistent Labeling and Display Policy. The Consistent Labeling and Display Policy requires all gTLD registries and registrars to consistently label and display WHOIS output fields.[55] Consistent with ICANN org's objective to maintain as much of the current WHOIS as possible in relation to the GDPR, registries and registrars should continue to follow the Consistent Labeling and Display Policy. For any data fields not required to be published in public WHOIS as a result of the Interim Compliance Model, the value for such fields must display "Redacted for Privacy Purposes".

7.2.10.4. Thick Whois Transition Policy for .COM, .NET and .JOBS. The Interim Compliance Model would continue with transfer of full Thick WHOIS data from the registrar to the registry. As a result, the existing Thick WHOIS policy [56] should continue to be implemented by all registries and registrars.

7.2.11. **How will ICANN implement compliance with the Interim Compliance Model?**

7.2.11.1. Besides the proposed changes in ICANN policies noted above, the Interim Compliance Model will be implemented on the basis of amendments to agreements with existing registries and registrars, and revised agreements for new registries and registrars, reflecting the revised approaches to WHOIS data publication and access.

7.2.11.2. ICANN will develop and implement WHOIS data protection agreements with registries, registrars, data escrow agents, CZDA Providers, Emergency Back-End Registry Operators, and other relevant third party contacting parties to implement (i) compliance with relevant GDPR requirements applicable to controller-to-controller data transfers, (ii) participation in the non-public WHOIS access accreditation program, (iii) address any controller-to-processor/sub-processor requirements, and (iv) cover the

[54] https://www.icann.org/resources/pages/tdrp-2012-02-25-en
[55] https://www.icann.org/resources/pages/rdds-labeling-policy-2017-02-01-en
[56] https://www.icann.org/resources/pages/thick-whois-transition-policy-2017-02-01-en

transfer of WHOIS data in a jurisdiction other than a jurisdiction in the EU, the EEA, or the European Commission-approved countries providing 'adequate' data protection.

7.2.11.3. ICANN has determined that each contracting party is acting as an independent controller in connection with the processing of WHOIS data. The contractual commitments contemplated above will address ICANN's and each contracting party's obligations as controllers and impose reasonable cooperation obligations to enable the exercise by data subjects of their data protection rights as set forth in the GDPR. Also, these contractual commitments will require the contracting parties to acknowledge and agree that each is acting independently as a data controller with respect of WHOIS data processed by the party and the parties are not joint controllers as defined in the GDPR.

8. Next Steps

ICANN org continues to have discussions with the community and data protection authorities about the Interim Compliance Model. ICANN org encourages that community to continue to provide input on this document as we move toward a final model. The Article 29 representatives noted the progress we have made in developing a plan of action to comply with the GDPR, and expressed their willingness to review the Proposed Interim Model in more detail, particularly regarding the purposes for the collection and publication of data, the data retention period, data processing agreements, and the justifications surrounding access to full registration data for accredited users. We are also looking forward to a deeper exchange with the Article 29 Working Party later in March on the rationale for the Interim Compliance Model.

9. Attachments

Attachment 1 – Legal Basis for Processing of gTLD Registration Data Elements[57]

	Category of Data Elements	**Specific Data Elements**	**Lawfulness of Processing**
1	Registered Name	Domain name; Registry Domain ID Domain Status	Art. 6(1)(a) GDPR – Consent from data subject whose personal data in included in the registration or from the agent as a representative of the registrant; Art. 6(1)(b) GDPR – Performance of a contract with the registrant (if a natural person) or an agent of the registrant (if a legal person) in the performance of a contract concerning the registration; Art. 6(1)(c) GDPR - In connection with legal reporting obligations of the registrar; and Art. 6(1)(f) GDPR – In connection with the legitimate interest of the registrar and WHOIS system stakeholders.
2	Information about the primary and secondary name server(s) for the Registered Name	Name Server; DNSSEC	N/A. Data is not Personal Data.

[57] The purpose for collection of these data elements are summarized in great detail at https://www.icann.org/en/system/files/files/gdpr-dataflow-matrix-whois-11sep17-en.pdf

	Category of Data Elements	Specific Data Elements	Lawfulness of Processing
3	Information about the registrar	Registrar WHOIS Server; Registrar URL; Registrar; Registrar IANA ID; Registrar Abuse Contact Email; Registrar Abuse Contact Phone; Reseller	For relevant personal data included in the data elements: Art. 6(1)(a) GDPR – Consent from data subject whose personal data in included in the registration as an agent of the registrar; Art. 6(1)(b) GDPR – Performance of a contract with the registrar; Art. 6(1)(f) GDPR – in connection with the legitimate interest of ICANN.
4	Original creation and expiration dates of the registration	Updated Date; Creation Date; Registry Expiry Date; Registrar Registration Expiration Date	To the extent associated with the name of the registrant, see No. 1 above. Otherwise not applicable.
5	Contact details about the registrant	Registry Registrant ID; Registrant Name; Registrant Organization; Registrant Postal Address; (Street, City, State/Province, Postal Code, Country); Registrant Phone and extension; Registrant Fax and extension;	Solely with respect to personal data included in the contact details of the registrant: Art. 6(1)(a) GDPR – Consent from data subject whose personal data in included in the registration or from the agent as a representative of the registrant; Art. 6(1)(b) GDPR – Performance of a contract with the registrant (if a natural person) or an agent of the registrant (if a legal person) in the performance of a contract concerning the registration;

	Category of Data Elements	Specific Data Elements	Lawfulness of Processing
		Registrant email	Art. 6(1)(c) GDPR - In connection with legal reporting obligations of the registrar; and Art. 6(1)(f) GDPR – In connection with the legitimate interest of the registrar and WHOIS system stakeholders.
6	Contact details about the administrative contact	Registry Admin ID; Admin Name; Admin Organization; Admin Postal Address; (Street, City, State/Province, Postal Code, Country); Admin Phone and extension; Admin Fax and extension; Admin email	Solely with respect to personal data included in contact details of the administrative contact in the registration: Art. 6(1)(a) GDPR – Consent from (i) the data subject who is also the administrative contact or (ii) consent of the data subject who serves as the administrative contact of the registrant and is submitting the registration, or (iii) consent of the data subject that will serve as the administrative contact obtained by the person submitting the registration; Art. 6(1)(b) GDPR – Performance of a contract with the registrant (if a natural person) or an agent of the registrant (if a legal person) in the performance of a contract concerning the registration; Art. 6(1)(c) GDPR - In connection with legal reporting obligations of the registrar; and Art. 6(1)(f) GDPR – In connection with the legitimate interest of the registrar and WHOIS system stakeholders.

	Category of Data Elements	Specific Data Elements	Lawfulness of Processing
7	Contact details about the technical contact	Registry Tech ID; Tech Name; Tech Organization; Tech Postal Address; (Street, City, State/Province, Postal Code, Country); Tech Phone and extension; Tech Fax and extension; Tech email	Solely with respect to personal data included in contact details of the technical contact in the registration: Art. 6(1)(a) GDPR – Consent from (i) the data subject who is also the technical contact or (ii) consent of the data subject who serves as the technical contact of the registrant and is submitting the registration, or (iii) consent of the data subject that will serve as the technical contact obtained by the person submitting the registration; Art. 6(1)(b) GDPR – Performance of a contract with the registrant (if a natural person) or an agent of the registrant (if a legal person) in the performance of a contract concerning the registration; Art. 6(1)(c) GDPR - In connection with legal reporting obligations of the registrar; and Art. 6(1)(f) GDPR – In connection with the legitimate interest of the registrar and WHOIS system stakeholders.

Attachment 2 – Legal Basis for Data Retention Requirements

Data Element	Explanation of Data Element	Legitimate purposes for Collection/Retention Lawful Basis	Recipient or categories of recipients[58]
1.1.1. First and last name or full legal name of Registrant	Identification of the registered owner (individual owner) or representative of the registered owner (legal person)	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks [Art. 6(1)(a) GDPR; Art. 6(1)(b) GDPR; Art. 6(1)(c) GDPR; Art. 6(1)(a) GDPR]	Registrar, Other Registrar (in case of replacement of the original Registrar), Registry Operator (in case of a thick Whois model under which the Registry maintains and provides both sets of data (Domain Name Data and Registrant Data)), Resellers (if used by Registrar), ICANN (under the conditions of Section 3.4.3 or Section 3.6 of 2013 RAA), Registrar's data escrow agent (Section 3.6 of 2013 RAA) Courts and Governmental authorities (pursuant to a valid subpoena, or administrative or court order), Dispute Resolution Panel and Dispute Resolution Provider (in the course of deciding about a request concerning a dispute under the TDRP), Banks or financial institutions (for payment processing purposes)
1.1.2. First and last name or, in the event Registrant is a legal person, the title of the	Identification of administrative and technical contact representative of the registered owner	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution	Registrar, Other Registrar (in case of replacement of the

[58] In some limited cases, ICANN is a recipient of the data, such as for contractual compliance investigations, and from an Emergency Backend Registry Operator in the event of registry failure.

Data Element	Explanation of Data Element	Legitimate purposes for Collection/Retention Lawful Basis	Recipient or categories of recipients[58]
Registrant's administrative contact, technical contact, and billing contact		of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks [Art. 6(1)(a) GDPR; Art. 6(1)(b) GDPR; Art. 6(1)(c) GDPR; Art. 6(1)(a) GDPR]	original Registrar), Registry Operator (in case of a thick Whois model under which the Registry maintains and provides both sets of data (Domain Name Data and Registrant Data)), Resellers (if used by Registrar), ICANN (under the conditions of Section 3.4.3 2013 RAA), Courts and Governmental authorities (pursuant to a valid subpoena, or administrative or court order), Dispute Resolution Panel and Dispute Resolution Provider (in the course of deciding about a request concerning a dispute under the TDRP)
1.1.3. Postal address of Registrant, administrative contact, technical contact, and billing contact	Means of contacting and identification of location of the administrative and technical contact representative of the registered owner	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks [Art. 6(1)(a) GDPR; Art. 6(1)(b) GDPR; Art. 6(1)(c) GDPR; Art. 6(1)(a) GDPR]	Registrar, Other Registrar (in case of replacement of the original Registrar), Registry Operator (in case of a thick Whois model under which the Registry maintains and provides both sets of data (Domain Name Data and Registrant Data)), Resellers (if used by Registrar), ICANN (under the conditions of Section 3.4.3 2013 RAA), Courts and Governmental authorities (pursuant to a valid subpoena, or administrative or court order), Dispute Resolution Panel and Dispute Resolution Provider (in the course of deciding about a

Data Element	Explanation of Data Element	Legitimate purposes for Collection/Retention Lawful Basis	Recipient or categories of recipients[58]
			request concerning a dispute under the TDRP)
1.1.4. Email address of Registrant, administrative contact, technical contact, and billing contact;	Means of electronically contacting the administrative and technical contact representative of the registered owner	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks [Art. 6(1)(a) GDPR; Art. 6(1)(b) GDPR; Art. 6(1)(c) GDPR; Art. 6(1)(a) GDPR]	Registrar, Other Registrar (in case of replacement of the original Registrar), Registry Operator (in case of a thick Whois model under which the Registry maintains and provides both sets of data (Domain Name Data and Registrant Data)), Resellers (if used by Registrar), ICANN (under the conditions of Section 3.4.3 2013 RAA), Courts and Governmental authorities (pursuant to a valid subpoena, or administrative or court order), Dispute Resolution Panel and Dispute Resolution Provider (in the course of deciding about a request concerning a dispute under the TDRP)
1.1.5. Telephone contact for Registrant, administrative contact, technical contact, and billing contact;	Means of contacting the administrative and technical contact representative of the registered owner	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks [Art. 6(1)(a) GDPR; Art. 6(1)(b) GDPR; Art. 6(1)(c)	Registrar, Other Registrar (in case of replacement of the original Registrar), Registry Operator (in case of a thick Whois model under which the Registry maintains and provides both sets of data (Domain Name Data and Registrant Data)), Resellers (if used by Registrar), ICANN (under the conditions of Section 3.4.3 2013 RAA), Courts and Governmental authorities (pursuant

Data Element	Explanation of Data Element	Legitimate purposes for Collection/Retention Lawful Basis	Recipient or categories of recipients[58]
		GDPR; Art. 6(1)(a) GDPR]	to a valid subpoena, or administrative or court order), Dispute Resolution Panel and Dispute Resolution Provider (in the course of deciding about a request concerning a dispute under the TDRP)
1.1.6. WHOIS information, as set forth in the WHOIS Specification	WHOIS registration data related to the domain name registration	Data Enabling Registrar to populate and make available to the public community the WHOIS register both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Abuse mitigation Facilitating domain name purchases and sales [Art. 6(1)(a) GDPR; Art. 6(1)(a) GDPR]	Registrar, Other Registrar (in case of replacement of the original Registrar), Registry Operator (in case of a thick Whois model under which the Registry maintains and provides both sets of data (Domain Name Data and Registrant Data) and provides for the Whois service as well), Resellers (if used by Registrar), ICANN (under the conditions of Section 3.4.3 2013 RAA), Courts and Governmental authorities (pursuant to a valid subpoena, or administrative or court order), Dispute Resolution Panel and Dispute Resolution Provider (in the course of deciding about a request concerning a dispute under the TDRP), Any third party with access to the Whois service
1.1.7. Types of domain name services purchased for use in connection with the Registration;	To understand the nature of the registration related services purchased	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, theft, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP)	Registrar, Other Registrar (in case of replacement of the original Registrar), Resellers (if used by Registrar), ICANN (under the

Data Element	Explanation of Data Element	Legitimate purposes for Collection/Retention Lawful Basis	Recipient or categories of recipients[58]
		Billing Billing disputes Chargebacks [Art. 6(1)(a) GDPR; Art. 6(1)(b) GDPR; Art. 6(1)(c) GDPR; Art. 6(1)(a) GDPR]	conditions of Section 3.4.3 2013 RAA), Courts and Governmental authorities (pursuant to a valid subpoena, or administrative or court order), Dispute Resolution Panel and Dispute Resolution Provider (in the course of deciding about a request concerning a dispute under the TDRP), Banks or financial institutions (for payment processing purposes)
1.1.8. To the extent collected by Registrar, "card on file," current period third party transaction number, or other recurring payment data	Section 1.1.8 focuses on data required for processing of recurring payments. Some (not all) Registrants provide Registrars with credit card numbers to retain as a "card on file," or with bank account information so that recurring payments such as monthly fees or automatic renewals can be billed periodically. The information retained would include whatever is required for the payment processor and credit card company to process the recurring payment transaction (typically credit card number, expiration date, name on card, address or postal code, sometimes security code). Alternatively, a Registrant might authorize recurring payments to be made by automatically	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration (to address hijacking, slamming and to facilitate resolution of transfer disputes in accordance with the TDRP) Billing Billing disputes Chargebacks [Art. 6(1)(a) GDPR; Art. 6(1)(b) GDPR; Art. 6(1)(c) GDPR; Art. 6(1)(a) GDPR]	Registrar, Other Registrar (in case of replacement of the original Registrar), Resellers (if used by Registrar), ICANN (under the conditions of Section 3.4.3 2013 RAA), Courts and Governmental authorities (pursuant to a valid subpoena, or administrative or court order), Dispute Resolution Panel and Dispute Resolution Provider (in the course of deciding about a request concerning a dispute under the TDRP), Banks or financial institutions (for payment processing purposes, including credit card companies and clearing houses)

Data Element	Explanation of Data Element	Legitimate purposes for Collection/Retention Lawful Basis	Recipient or categories of recipients[58]
	debiting the Registrant's bank account via an automated clearing house (ACH) bank debit, which would require storing the account holder's name, bank routing number and bank account number. Whether recurring payments are authorized to be charged by credit card or by bank debit, any recurring payment mechanism and associated retention of recurring payment information would require the Registrant's authorization to retain such information for recurring payments. When the Registrar submits a credit card transaction for processing of any payment, an authorization will generate an approval code, which the Registrar stores with the transaction. Banks of financial institutions may generate and provide to the Registrar a bank-generated transaction ID number for each payment made.		

Data Element	Explanation of Data Element	Legitimate purposes for Collection/Retention Lawful Basis	Recipient or categories of recipients[58]
1.2.1. Information regarding the means and source of payment reasonably necessary for the Registrar to process the Registration transaction, or a transaction number provided by a third-party payment processor	Section 1.2.1 focuses on source of payment information required for processing of the initial Registration transaction (without regard to whether recurring payments are authorized). The data would be similar to that in Section above (which deals with recurring payments). Banks or financial institutions may generate and provide to the Registrar a bank-generated transaction ID number for each payment made.	Registrar's internal use for administration of the contract with Registrant both during and for some period of time after the registration Maintain Registrar's tax and accounting records Billing Billing disputes Fraud prevention Chargebacks [Art. 6(1)(a) GDPR; Art. 6(1)(b) GDPR; Art. 6(1)(c) GDPR; Art. 6(1)(a) GDPR]	Registrar, Other Registrar (in case of replacement of the original Registrar), ICANN (under the conditions of Section 3.4.3 2013 RAA), Courts and Governmental authorities (pursuant to a valid subpoena, or administrative or court order), Dispute Resolution Panel and Dispute Resolution Provider (in the course of deciding about a request concerning a dispute under the TDRP), Banks or financial institutions (for payment processing purposes, including credit card companies and clearing houses)
1.2.2. Log files, billing records and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry- wide generally accepted standard practices within the industries in which Registrar operates, other	Section 1.2.2 focuses on records associated with communications between Registrar and the Registrant about the Registration with an emphasis on information regarding the source and destination of the communications. Most commercially available server software gathers certain information regarding website visits automatically and stores it in log	Fraud prevention Billing disputes Resolution of disputes between Registrar and Registry Operator or between two Registrars or between Registrar and Registrant regarding the status of a Registration, e.g., Registrant says it never authorized the transfer of a domain name from one Registrar to another Registrar; log files maintained by Registrar could show when and	Registrar, Other Registrar (in case of replacement of the original Registrar), Resellers (if used by Registrar), ICANN (under the conditions of Section 3.4.3 2013 RAA), Courts and Governmental authorities (pursuant to a valid subpoena, or administrative or court order)

Data Element	Explanation of Data Element	Legitimate purposes for Collection/Retention Lawful Basis	Recipient or categories of recipients[58]
records containing communications source and destination information, including, depending on the method of transmission and without limitation: (1) Source IP address, HTTP headers, (2) the telephone, text, or fax number; and (3) email address, Skype handle, or instant messaging identifier, associated with communications between Registrar and the Registrant about the Registration.	files. This information typically consists of an Internet Protocol (IP) address that consists at a minimum of a series of numbers, as well as browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp; this type of data is typically not linked to personally identifiable information and is used for aggregate analysis. In addition to this non- personally-identifiable data, some log files may include data identifying the source of the communication (IP address, telephone/text/fax number, email address or Skype handle or instant messaging identifier). In some cases that information may be linked to data about the particular user's behavior while on the website, including what the user has put in or taken out of their shopping cart, and what items the user purchases. The latter type of log file data may be important in the event of billing disputes or fraud, e.g., to show that the Registrant or someone using the Registrant's email address or IP address did in fact place a disputed order on a	from what source a request for transfer was made. [Art. 6(1)(a) GDPR; Art. 6(1)(b) GDPR; Art. 6(1)(c) GDPR; Art. 6(1)(a) GDPR]	

Data Element	Explanation of Data Element	Legitimate purposes for Collection/Retention Lawful Basis	Recipient or categories of recipients[58]
	particular date at a particular time.		
1.2.3. Log files and, to the extent collection and maintenance of such records is commercially practicable or consistent with industry-wide generally accepted standard practices within the industries in which Registrar operates, other records associated with the Registration containing dates, times, and time zones of communications and sessions, including initial registration.	Section 1.2.3 focuses on records associated with the Registration. This may include communications with the Registrant regarding the Registration (see Section 1.2.2 above), but may also include records of communications between the Registrar and the Registry Operator about the Registration. Most Registrars and Registry Operators utilize the Extensible Provisioning Protocol (EPP) to track, manage and reconcile the status of domain name registrations (e.g., statuses such as register, renew, modify, delete, transfer). Software used by Registrars and Registry Operators often maintain log files tracking EPP records such as when a Registration is first made, when it is transferred or deleted, when it is modified, etc. and assign unique authorization codes to events as a security measure to prevent unauthorized transfers, deletions or other abuse. Typical web server software can be configured to maintain html server logs, stored either on the Registrar's server or in cookies on the Registrant's browser or both, either in encrypted or unencrypted form,	Fraud prevention Billing disputes Resolution of disputes between Registrar and Registry Operator or between two Registrars or between Registrar and Registrant regarding the status of a Registration (e.g., Registrant says it never authorized the transfer of a domain name from one Registrar to another Registrar; log files maintained by Registrar could show when and from what source a request for transfer was made and if or when Registrar transmitted to the Registry Operator a request to transfer the registration. [Art. 6(1)(a) GDPR; Art. 6(1)(b) GDPR; Art. 6(1)(c) GDPR; Art. 6(1)(a) GDPR]	Registrar, Other Registrar (in case of replacement of the original Registrar), Registry Operator (in case of disputes between Registrar and Registry Operator regarding the status of a Registration), Resellers (if used by Registrar), ICANN (under the conditions of Section 3.4.3 2013 RAA), Courts and Governmental authorities (pursuant to a valid subpoena, or administrative or court order)

Data Element	Explanation of Data Element	Legitimate purposes for Collection/Retention Lawful Basis	Recipient or categories of recipients[58]
	and with the option of allowing the user (the Registrant) to allow or prevent storage in the form of cookies in its browser.		

Attachment 3 – Sample of Minimum WHOIS Output Fields

WHOIS Data Fields	ICANN Interim Compliance Model Legal and Natural persons
Domain Name	Display
Registry Domain ID	Display
Registrar WHOIS Server	Display
Registrar URL	Display
Updated Date	Display
Creation Date	Display
Registry Expiry Data	Display
Registrar Registration Expiration Date	Display
Registrar	Display
Registrar IANA ID	Display
Registrar Abuse Contact Email	Display
Registrar Abuse Contact Phone	Display
Reseller	Display
Domain Status	Display
Domain Status	Display
Domain Status	Display
Registry Registrant ID	Do not display
Registrant Name	Do not display
Registrant Organization	Display
Registrant Street	Do not display
Registrant City	Do not display
Registrant State/Province	Display
Registrant Postal Code	Do not display
Registrant Country	Display
Registrant Phone	Do not display
Registrant Phone Ext	Do not display
Registrant Fax	Do not display
Registrant Fax Ext	Do not display
Registrant Email	Anonymized email or web form
Registry Admin ID	Do not display
Admin Name	Do not display
Admin Organization	Do not display
Admin Street	Do not display
Admin City	Do not display
Admin State/Province	Do not display

WHOIS Data Fields	ICANN Interim Compliance Model Legal and Natural persons
Admin Postal Code	Do not display
Admin Country	Do not display
Admin Phone	Do not display
Admin Phone Ext	Do not display
Admin Fax	Do not display
Admin Fax Ext	Do not display
Admin Email	Anonymized email or web form
Registry Tech ID	Do not display
Tech Name	Do not display
Tech Organization	Do not display
Tech Street	Do not display
Tech City	Do not display
Tech State/Province	Do not display
Tech Postal Code	Do not display
Tech Country	Do not display
Tech Phone	Do not display
Tech Phone Ext	Do not display
Tech Fax	Do not display
Tech Fax Ext	Do not display
Tech Email	Anonymized email or web form
Name Server	Display
Name Server	Display
DNSSEC	Display
DNSSEC	Display
URL of ICANN Whois Inaccuracy Complaint Form	Display
>>> Last update of WHOIS database	Display

Attachment 4 –Access to Thick WHOIS Data Through Accreditation Program [59]

Access Framework	Eligibility	Administering Party	Oversight & Enforcement	Binding Approach
Accreditation through pre-defined criteria and limitations and legally binding terms	Public parties	GAC	GAC or such other "monitoring body" TBD that satisfies Art. 41 GDPR[2] Requests are submitted through the Accreditation Clearinghouse	Binding and enforceable commitments via contractual or other legally binding instruments, which include safeguards for data subject rights specified in the code of conduct
Accreditation through Code of Conduct[60] approved by competent supervisory authorities and legally binding terms	Private parties as designated by GAC. Including registries, registrars, escrow agents, dispute resolution providers	GAC or certification body[61] accredited by the supervisory authority under Art. 41 GDPR	Established procedures to monitor compliance Requests are submitted through the Accreditation Clearinghouse	Binding and enforceable commitments via contractual or other legally binding instruments, which include safeguards for data subject rights specified in the code of conduct
Accreditation[62] by a certification body and legally	Private parties	GAC or certification body accredited by the	GAC or certification body TBD that satisfies Art. 43 GDPR	Binding and enforceable commitments via contractual or

[59] As noted in the Interim Compliance Model, the accreditation program would be developed in consultation with the GAC, DPAs and contracted parties with full transparency to the ICANN community.
[60] WHOIS Data Access Codes of Conduct are permitted under Arts. 40-41 GDPR. ICANN's WHOIS Data Access Code of Conduct and the Independent Body's Code of Conduct under Arts. 40-41 GDPR may be aligned through consultation.
[61] The independent monitoring body under Arts. 40-41 GDPR may be the same entity as the certification body under Arts. 42-43.
[62] Certification is addressed in Arts. 42-43 GDPR.

Access Framework	Eligibility	Administering Party	Oversight & Enforcement	Binding Approach
binding terms		supervisory authority under Art. 42 GDPR	Requests are submitted through the Accreditation Clearinghouse	other legally binding instruments, which include safeguards for data subject rights specified in the code of conduct
Defined Legal Process for Recurring Data Access	Private parties, law enforcement, regulatory bodies	The entity receiving the request	Based on legal procedures	n/a
Bilateral, Multilateral, or Other International Agreements	Law enforcement, government entities, regulatory bodies identified by GAC	ICANN Accreditation Clearinghouse	GAC monitors compliance with ICANN's code of conduct and determines eligibility	n/a