Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation – For Discussion

Prepared by: ICANN Org
Published on: 12 January 2018

Introduction

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 Org has consulted with contracted parties, European data protection authorities, legal experts, and interested community stakeholders to understand the potential impact 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 in light of the GDPR.

As discussed with the community during ICANN60 and in subsequent communications, ICANN Org has been working to develop potential interim compliance models for continued discussion with the community, while taking into account the existing legal analysis from Hamilton law firm, community input, and discussions with European data protection authorities. As noted in the Blog, this document presents three proposed interim models for handling registration data, including registration directory services (WHOIS), for registries and registrars to comply with ICANN agreements and policies in relation to the GDPR's effective date in May 2018.

Each of the proposed interim models differ, and are taken from inputs already received from the community. These models are intended to facilitate additional community discussion, and from that input either variations or modifications to one of these will be identified at the end of January for the path forward. The input from the community will contribute to assessing the viability of each of proposed models.

Approach to Developing Interim Compliance Models

ICANN Org's approach to develop the proposed interim compliance models takes into account the following:

1. **The proposed models represent potential interim solutions** for compliance with existing ICANN agreements and policies. The selected model will not replace the multistakeholder policy development 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.

2. ICANN Org, with multistakeholder input, is attempting 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**.

3. **ICANN Org is guided by its Bylaws** in developing proposed interim compliance models. 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." (Section 4.6(e)(i)).

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**.

5. The three proposed compliance models for discussion attempt to **account for the range of views expressed by the ICANN community** about impacts of GDPR on WHOIS and other gTLD registration data.[1] When developing the models, ICANN Org considered the community work/input to develop the dataflow matrix of user stories for WHOIS[2], GDPR compliance models proposed by community members[3], guidance from European ccTLD registry operators[4], community discussions at ICANN meetings[5], and other questions, input, and analyses submitted by ICANN stakeholders.

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

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

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

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

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

6. The proposed **compliance models propose a tiered/layered access to WHOIS data**. This is a shift from the current WHOIS system. This feature is embedded in each of the models based on the series of legal analyses from the Hamilton law firm[6] 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"[7]. This feedback suggests that legitimate interest possibly could be used as the basis for a limited public WHOIS.

7. The proposed compliance **models represent 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.

Proposed Interim Compliance Models

Framework Elements of Each Model

To develop the proposed compliance models, ICANN Org considered high-level framework elements to be addressed in each of the compliance models. The framework elements included:

1. Purpose – What is the purpose for the processing activities at issue?
2. Scope – To which registrations does the model apply?
3. Data Collection – What data must be collected by the registrar at time of registration?
4. Data Transfer (Registry) – What data must the registrar transfer to the registry?
5. Data Transfer (Escrow Agents) – What data must registrars and registries transfer to the data escrow agents?
6. Publicly available WHOIS – What registration data must be published in public WHOIS? What registration data must not be published in public WHOIS?
7. Non-public WHOIS – Who can access non-public WHOIS data, and by what method?
8. Data Retention – How long must data be retained by registries, registrars and data escrow agents?
9. Domain Name Transfers – How must domain name transfers be handled?
10. Rights of Data Subjects – How must rights of data subjects be handled in the registration system/process?
11. Incident Response Requirements – Who will have primary responsibility for providing mandatory notifications required by the GDPR?

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

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

For some elements, the models take a common approach to address the element. The commonalities across the three models are described in the section titled "Commonalities Across All Models".

For the other elements, this document provides an explanation about how each proposed model would address a particular element. **Appendix 1** includes a comparison chart to summarize how each element is treated across the proposed models.

Commonalities Across All Models

In the absence of indication from European data protection authorities that some personal data cannot be collected and transferred to registries and data escrow agents, the proposed interim models all propose that:

1. registrars may collect from registrants, but not necessarily publish, all personal data currently included in Thick registration data (based on performance of a contract and the legitimate interests pursued by the controller or by a third party);

2. registrars may transfer to registries personal data included in Thick registration data (based on performance of a contract and the legitimate interests pursued by the controller or by a third party)[8];

3. registrars and registries may transfer to data escrow agents personal data included in Thick registration data (based on performance of a contract and the legitimate interests pursued by the controller or by a third party)[9];

4. the minmum public WHOIS output proposed in each model is based on the legitimate interests pursued by the controller or a third party;

5. registrars must request from registrants specific and informed consent that is freely given, unambiguous, withdrawable at any time, and is otherwise consistent with the GDPR for publication of full Thick data[10]. If the registrant does not provide its consent, or later withdraws its consent, the minimum public WHOIS data that should be displayed is outlined in each model (see #4 – Commonailities Across All Models). At a minimum, the public display of WHOIS must include the registered domain name, information about the primary and secondary nameserver(s) for the registered name, information about the registrar, the original creation date of the registration, and the expiration date of the registration;

[8] Mechanisms would need to be developed for cross- boarder transfers of personal data.

[9] Mechanisms would need to be developed for cross- boarder transfers of personal data.

[10] Note that including consent could raise additional issues, such as the right to be forgotten, but this option is included as suggested by some community comments.

6. in addition to procedures in the Transfer Policy, domain name transfers between registrars also would be handled by requiring the losing registrar or the registry to provide the gaining registrar access to the non-public WHOIS data for the limited purpose of facilitating the transfer;

7. registrars, as the primary point of contact with registrants, will continue to process requests from registrants to correct and update registration data and other data subjects' requests under the GDPR; and

8. registries, registrars, and ICANN would independently manage and respond to personal data breaches and notify affected data subjects, competent supervisory authorities and each other when a personal data breach occurs.

Changes to these underlying common approaches and assumptions may affect the proposed interim compliance models.

Purpose Description

As stated in the 21 December 2017 Hamilton legal analysis[11], "[a]s a first step, the purposes for processing of personal data within the scope of the Whois services must be determined and formulated in a way that is compliant with the GDPR."

The following interim draft purpose description for WHOIS draws from community work to-date, including the gTLD Registration Dataflow Matrix of User Stories for WHOIS[12], the 2007 GAC Principles Regarding gTLD WHOIS Services[13], the Final Report of the Expert Working Group on gTLD Directory Services[14], among others.

This is a starting point for further community input, and ICANN Org invites comments on this working purpose description.

The purpose of WHOIS:

In support of ICANN's mission to coordinate and ensure the stable and secure operation of the Internet's unique identifier system, maintaining the availability of WHOIS data 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

[11] See Paragraph 2.3.3. at https://www.icann.org/en/system/files/files/gdpr-memorandum-part3-21dec17-en.pdf.

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

[13] https://gacweb.icann.org/download/attachments/28278834/WHOIS_principles.pdf

[14]http://whois.icann.org/sites/default/files/files/ird-expert-wg-final-23sep15-en.pdf

generic top-level domain registration data, as well as consider safeguards for protecting such data."

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

1. Providing appropriate access to accurate, reliable, and uniform registration data;
2. Enabling a reliable mechanism for identifying and contacting the registrant;
3. Providing reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names;
4. 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; and
5. Providing a framework to address appropriate law enforcement needs.

Model 1

Model 1 would apply only to personal data included in the registration data of a natural person where:

A. the registrar and/or registry are established in the European Economic Area (EEA) and process personal data included in registration data;
B. the registrar and/or registry are established outside the EEA and provide services involving the processing of personal data from registrants located in the EEA; or
C. 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.

Under Model 1, unless the registrant otherwise grants permission, registrars and registries would be required to display the following minimum data in public WHOIS:

1. The name of the Registered Name
2. Information about the primary and secondary nameserver(s) for the Registered Name
3. Information about the Registrar
4. The original creation date of the registration
5. The expiration date of the registration
6. The name and postal address of the registrant (i.e. no email or telephone contact information)
7. The email address, telephone number and fax number (where available) of the administrative contact for the Registered Name (i.e. no name and postal address of the contact. Note: This is different from previous versions of the Registrar Accrediation Agreement, which included this contact information.)
8. The email address, telephone number and fax number (where available) of the technical contact for the Registered Name (i.e. no name and postal address of tech contact. Note: This is different from previous versions of the Registrar Accrediation Agreement, which included this contact information.)

A sample of the minimum WHOIS output for Model 1 is included in **Appendix 2**.

Registries and registrars would be required to retain the registration data for two years beyond the life of the domain name registration.

To access registration data not published in the public WHOIS, registries and registrars would respond to requests from third parties on a timely basis. The requestor would be required to submit an application to the registrar or registry stating the specific purpose for accessing the data. The requestor would self-certify that the requested access is necessary for the purposes of the legitimate interests pursued by the requestor, and would self-certify that the data provided would only be used for the limited purpose for which it was requested. The registry or registrar would consider the request, taking into account the required balancing of interests under the GDPR .[15]

Registries and registrars may, but would not be required by ICANN, to provide additional access to non-public WHOIS as long as it complies with GDPR and other applicable laws.

Model 2

Model 2 has two variants on the scope of applicability of the model. Model 2A would apply to personal data included in the registration data without regard to whether the registrant is a natural or legal person where:

(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 provide services 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.

Model 2B would apply to all registrations on a global basis, without regard to location of the registrant, registry, registrar or a processor of the registration data. There are no other variations between Model 2A and 2B.

Under Model 2, unless the registrant otherwise grants permission, registrars and registries would be required to display the following minimum data in public WHOIS:

1. The name of the Registered Name
2. Information about the primary and secondary nameserver(s) for the Registered Name
3. Information about the Registrar
4. The original creation date of the registration

[15] The proposed self-certification and approval process would be similar to the process registries currently use to approve access to Zone File Data in the Centralized Zone Data Service.

5. The expiration date of the registration
6. The email address of the administrative contact for the Registered Name (i.e. no name postal address, telephone or fax of the contact)
7. The email address of the technical contact for the Registered Name (i.e. no name postal address, telephone or fax of the contact)

Note for community discussion: This Model would not publish the name of the registrant, whether legal or natural person, unless the registrant opts-in. A sample of the minimum WHOIS output for Model 2 is included in **Appendix 2**.

Registries and registrars would be required to retain the registration data for one year beyond the life of the domain name registration.

In Model 2, registries and registrars would provide access to non-public registration data only for a defined set of third-party requestors certified under a formal accreditation/certification program. Under this approach, certified 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. The user groups eligible for the certification program, and the process for providing access to the non-public WHOIS data would be developed in consultation with the Governmental Advisory Committee (GAC) so that public policy considerations are taken into account.

Registries and registrars may, but would not be required by ICANN, to provide additional access to non-public WHOIS as long as it complies with the GDPR and other applicable laws.

Should a formal accreditation/certification program not be ready in time, the self-certification process described in Model 1 or other interim mechanism would need to be identified while the finalization for a formal accreditation/certification program is put into place. Feedback on what an interim mechanism would be while work towards a formal one is finalized would be appreciated.

Model 3

Model 3 would apply to all registrations on a global basis, without regard to location of the registrant, registry, registrar or a processor of the registration data.

Under Model 3, unless the registrant otherwise grants permission, registrars and registries would be required to display the following minimum data in public WHOIS:

1. The name of the Registered Name
2. Information about the primary and secondary nameserver(s) for the Registered Name
3. Information about the Registrar
4. The original creation date of the registration
5. The expiration date of the registration
6. Do not display any personal data

Note for community discussion: This Model would appear to require a registration-by-registration, field-by-field assessment about whether personal data is included. Additional consideration would be needed about how to implement this. A sample of the minimum WHOIS output for Model 3 is included in **Appendix 2**.

Registries and registrars would be required to retain the registration data for 60 days beyond the life of the domain name registration.

To access registration data not published in the public WHOIS registries and registrars would only grant access to third-party requestors when required by applicable law and subject to due process requirements, such as when the third-party requestor provides a subpoena or any other order from a court or other judicial tribunal of competent jurisdiction for access to non-public WHOIS data.

Next Steps

ICANN Org will continue to refine the potential compliance models based on feedback from the community, including the European data protection authorities, and will publish the interim compliance model in the coming weeks. Feedback on these models is requested by 29 January 2018 and may be sent to gdpr@icann.org. This input will be used to settle on a single model, which ICANN Org intends to publish by 31 January 2018 along with next steps.

Appendices

Appendix 1: Summary Comparison Chart of Proposed Interim GDPR Compliance Models

Appendix 2: Sample WHOIS Output Under Proposed Models

Appendix 1: Summary Comparison Chart of Proposed Interim GDPR Compliance Models

Interim GDPR Compliance Models				
	Model 1	**Model 2**		**Model 3**
		Model 2A	**Model 2B**	
Collection from Registrant to Registrar	Full Thick Data			
Data Transfer from Registrar to Registry	Full transfer of Thick Data			
Data Transfer to Escrow Agents	Full transfer of existing registration data			
Public WHOIS	Display all current Thick Data, except do not display: (1) email and phone number of registrant, and (2) name and postal address of tech and admin contacts	Display only Thin Data + email address for Admin and Tech contacts (do not publish the name or any other data about any registrant)	Display only Thin Data + email address for Tech and Admin contacts (do not publish the name or any other data about any registrant)	Do not display any personal data in any registration
Access to Non-Public WHOIS Data	Self-certification – any 3rd party requestor would identify the specific purpose/need for accessing non-public WHOIS data and self-certify that access is necessary for the purposes of the legitimate interests pursued by the requestor. Upon approval by the registry or registrar, the requestor would agree/certify that it would only use data for the	Formal accreditation – Establish a certification program for certain user groups, such as law enforcement agencies and intellectual property lawyers, and registries and registrars must provide “certified” requestors access to non-public Whois data based on pre-defined criteria and limitations. The	Formal accreditation as described in Model 2A.	Legal due process – third parties would be required to provide a subpoena or any other order from a court or other judicial tribunal of competent jurisdiction to gain access to non-public WHOIS data.

Interim GDPR Compliance Models				
	Model 1	Model 2		Model 3
		Model 2A	Model 2B	
	limited purpose approved. (Note: the approval process could be likened to the process for registries to approve access to 3rd parties for zone file data.) Registries and registrars may provide additional access as long as it complies with the GDPR and other applicable laws.	user groups eligible for the certification program and the process for providing access to be developed in consultation with the GAC so that public policy considerations are taken into account. Registries and registrars may provide additional access as long as it complies with the GDPR and other applicable laws.		
Scope/Applicability of Model	Applies to personal data included in registrations of natural persons where registrant, registry, registrar or processing activities are carried out in the European Economic Area.	Applies to registrations without regard to whether the registrant is a natural or legal person, where the registrant, registry, registrar or a processor are located in the European Economic Area.	Applies to all registrations on a global basis without regard to location of registry, registrar registrant, and processing activities, and without regard to type of registrant. (Note: this option provides a blanket interim solution to provide a single, consistent approach across the board.)	Applies to all registrations on a global basis as described in Model 2B.
Data Retention	Life of registration + 2 years	Life of registration + 1 year	Life of registration + 1 year	Life of registration + 60 days

Appendix 2: Sample Minimum WHOIS Output Under Proposed Models

Unless the registrant otherwise provides consent, the **minimum** WHOIS output for each of the models is shown below. The green highlighted fields represent the registration data that will always be displayed across the three proposed models.

	ICANN Model 1		**ICANN Model 2**	**ICANN Model 3**
Registrant	**Natural person**	**Legal person**	**Legal and Natural persons**	**Legal and natural persons**
Domain Name	Display	Display	Display	Display
Registry Domain ID	Display	Display	Display	Display
Registrar WHOIS Server	Display	Display	Display	Display
Registrar URL	Display	Display	Display	Display
Updated Date	Display	Display	Display	Display
Creation Date	Display	Display	Display	Display
Registry Expiry Data	Display	Display	Display	Display
Registrar Registration Expiration Date	Display	Display	Display	Display
Registrar	Display	Display	Display	Display
Registrar IANA ID	Display	Display	Display	Display
Registrar Abuse Contact Email	Display	Display	Display	Display
Registrar Abuse Contact Phone	Display	Display	Display	Display
Reseller	Display	Display	Display	Display
Domain Status	Display	Display	Display	Display
Domain Status	Display	Display	Display	Display
Domain Status	Display	Display	Display	Display
Registry Registrant ID	Do not display	Display	Do not display	Do not display
Registrant Name	Display	Display	Do not display	Display unless field includes personal data
Registrant Organization	Display	Display	Do not display	Display unless field includes personal data
Registrant Street	Display	Display	Do not display	Display unless field includes personal data

	ICANN Model 1		ICANN Model 2	ICANN Model 3
Registrant	**Natural person**	**Legal person**	**Legal and Natural persons**	**Legal and natural persons**
Registrant City	Display	Display	Do not display	Display unless field includes personal data
Registrant State/Province	Display	Display	Do not display	Display unless field includes personal data
Registrant Postal Code	Display	Display	Do not display	Display unless field includes personal data
Registrant Country	Display	Display	Do not display	Display unless field includes personal data
Registrant Phone	Do not display	Display	Do not display	Display unless field includes personal data
Registrant Phone Ext	Do not display	Display	Do not display	Display unless field includes personal data
Registrant Fax	Do not display	Display	Do not display	Display unless field includes personal data
Registrant Fax Ext	Do not display	Display	Do not display	Display unless field includes personal data
Registrant Email	Do not display	Display	Do not display	Display unless field includes personal data
Admin Name	Do not display	Display	Do not display	Display unless field includes personal data
Admin Organization	Do not display	Display	Do not display	Display unless field includes personal data
Admin Street	Do not display	Display	Do not display	Display unless field includes personal data
Admin City	Do not display	Display	Do not display	Display unless field includes personal data
Admin State/Province	Do not display	Display	Do not display	Display unless field includes personal data
Admin Postal Code	Do not display	Display	Do not display	Display unless field includes personal data
Admin Country	Do not display	Display	Do not display	Display unless field includes personal data
Admin Phone	Display	Display	Do not display	Display unless field includes personal data
Admin Phone Ext	Display	Display	Do not display	Display unless field includes personal data
Admin Fax	Display	Display	Do not display	Display unless field includes personal data
Admin Fax Ext	Display	Display	Do not display	Display unless field includes personal data
Admin Email	Display	Display	Display	Display unless field includes personal data
Tech Name	Do not display	Display	Do not display	Display unless field includes personal data
Tech Organization	Do not display	Display	Do not display	Display unless field includes personal data
Tech Street	Do not display	Display	Do not display	Display unless field includes personal data
Tech City	Do not display	Display	Do not display	Display unless field includes personal data
Tech State/Province	Do not display	Display	Do not display	Display unless field includes personal data

	ICANN Model 1		ICANN Model 2	ICANN Model 3
Registrant	**Natural person**	**Legal person**	**Legal and Natural persons**	**Legal and natural persons**
Tech Postal Code	Do not display	Display	Do not display	Display unless field includes personal data
Tech Country	Do not display	Display	Do not display	Display unless field includes personal data
Tech Phone	Display	Display	Do not display	Display unless field includes personal data
Tech Phone Ext	Display	Display	Do not display	Display unless field includes personal data
Tech Fax	Display	Display	Do not display	Display unless field includes personal data
Tech Fax Ext	Display	Display	Do not display	Display unless field includes personal data
Tech Email	Display	Display	Display	Display unless field includes personal data
Name Server	Display	Display	Display	Display
Name Server	Display	Display	Display	Display
DNSSEC	Display	Display	Display	Display
DNSSEC	Display	Display	Display	Display