Proposed Interim Model for GDPR Compliance-- Summary Description

(The "Calzone Model", 28 February 2018)
Prepared by: ICANN Org

I. Introduction

The Proposed 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[1] to the greatest extent possible, the Proposed Interim Model maintains robust collection of registration data (including registrant, administrative, and technical contact information), but restricts most personal data to layered access via an accreditation program to be developed in consultation with the GAC.

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 means. The Proposed Interim Model would be required to 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 would apply to all registrations, without requiring registrars to differentiate between registrations of legal and natural persons. The model would include data processing agreements between and among ICANN, registries, registrars, and data escrow agents as necessary for compliance with the GDPR.

II. Competing Community Views About Elements of the Proposed Interim Model

Discussions with various parts of the community about the Proposed Interim Model suggest that there are competing views on the requirements of the GDPR and a few key elements in the Proposed Interim Model, namely:

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

1. 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;

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

3. whether or not registries and registrars would be required to continue to provide full public access to WHOIS data prior to the deployment of an accreditation program for layered/tiered access;

4. whether or not registries and registries should be permitted to optionally apply the model on a global basis; and

5. whether or not the model should apply to contact details supplied by registrants who are legal persons.

These competing community views are discussed in additional detail in the following discussion of the elements of the model.

III. Summary Description of Proposed Interim Model

1. Does the model propose layered/tiered access?

The Proposed Interim Model proposes 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.

This key feature of the model is a significant change to the current WHOIS system, and seems have general acceptance by the community.

2. What are the purposes of the collection and publication of WHOIS data?

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 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:

a. providing appropriate access to accurate, reliable, and uniform registration data;

b. enabling a reliable mechanism for identifying and contacting the registrant;

c. providing reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names;

d. 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

e. providing a framework to address appropriate law enforcement needs.

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

Registrars would be required to 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.

As noted above, this is a topic with competing community viewpoints. Some commentators have suggested that ICANN Org continue to consider the necessity of requiring the collection of administrative and technical contact data[2] for all registrations, noting that in more than 90% of the cases, the data included for each contact is identical to the registrant data. The commentators also assert that obtaining data of the non-registrant contacts introduces additional GDPR compliance risk because these contacts may not have a contractual relationship with the registry or registrar. 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. 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.

In addition, some commentators have asserted 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. The current Registrar Accreditation Agreement already includes accuracy requirements such as the validation and verification of some data elements, and the

[2] Note: Also, some registries require billing contact information to be collected. Provisions concerning the collection and use of billing contacts or other optional registry-specific elements would need to be addressed in Registry-Registrar Agreements.

provision of notice to registrants about how to access, and if necessary rectify the data held about them.

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 (http://tools.ietf.org/html/rfc5730), 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.

4. What data must the registrar transfer to the registry?

The registrar would be required to 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.

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

Registries and registrars would be required to continue to transfer the full data set collected from the registrant or transferred to the registry to the data escrow agent. 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.

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

The model does not include any changes from the current data retention requirements. Registrars would continue to be required 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 that have already been tailored to comply with European data protection and retention laws.

7. What is the scope of applicability of the model?

Registries and registrars would be required to apply the model to collection and processing linked to the European Economic Area. Registries and registrars would have the option to apply the model beyond the European Economic Area. Specifically:

a. Registries and registrars would be required to apply the model to personal data included in the registration data of natural and legal persons 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 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 would not be required to, apply the Proposed Interim Model to registrations without regard to location of the registrant, registry, registrar or a processor of the registration data.

As noted above, this is a topic with competing community viewpoints, both on whether or not the model should apply globally and on whether or not it should apply to contact data for legal persons.

Some commentators have raised concerns that permitting the model to be applied on a global basis and 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. 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 to collection and processing linked to the European Economic Area depending upon how an individual registry or registrar has set up its systems. Data processing agreements would lay out the respective responsibilities for compliance with the GDPR between and among ICANN, registries, registrars, and data escrow agents.

Likewise, some commentators have raised concerns that not distinguishing between registrations of legal and natural persons is an over-application of the GDPR. 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.

8. What registration data must be published in public WHOIS?

Registrars must provide registrants with the opportunity to opt-in to publication of full contact details in the public WHOIS. 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:

a. Must the Registrant name be published?

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.

b. Must the Registrant postal address be published?

The registrant's state/province and country would be published, but the address fields that could be used to more specifically identify the registrant would not be included in the public WHOIS. 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. Some commentators have suggested that additional elements of the postal address are necessary in order to establish jurisdiction such as the particular city and/or postal code. Further community discussion could help to ensure the appropriate balance is achieved.

c. Must the Registrant email be published?

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

As noted above, this is a topic with competing community viewpoints. The anonymized email or web form would enable non-accredited users to continue to contact the registrant. However, some commentators have argued that non-accredited users should continue to be allowed to use the registrant's actual email address to identify, and not just contact, the registrant. Other commentators argue that email addresses are information that could be used to identify the registrant and should not be part of the data available to non-accredited users. The Proposed Interim Model strikes a balance between the competing community viewpoints be enabling non-accredited users to contact, but not identify, the registrant. It should be noted that there are concerns regarding the timeline for implementation of anonymized email or web forms.

d. Must the Registrant phone and fax be published?

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

e. Must the Admin and Tech contact names be published?

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

f. Must the Admin and Tech contact postal addresses be published?

The Admin and Tech contact postal address would not be required to be published in public WHOIS.

g. Must the Admin and Tech contact phone and fax be published?

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

h. Must the Admin and Tech contact email be published?

Similar to the registrant email field, the public WHOIS would include anonymized email addresses or a web form from which messages could be forwarded to the Admin and Tech contact email addresses. This solution is proposed to balance the need to have a method to contact the registrant to resolve issues with a registration with the potential privacy concerns with publishing email addresses.

A sample of the minimum WHOIS output fields is included in **Attachment 1**.

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

To access registration data not published in the public WHOIS, 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 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. 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.

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

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 interim” solution, however this would raise a number of questions that would need to be

addressed to comply with the GDPR. This will be a continued topic for discussion in the coming weeks.

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 a data processing agreement between and among ICANN, registries, and registrars.

Additional details about the proposed accreditation program for continued access to full Thick WHOIS data are included in **Attachment 2**.

Additionally, **Attachment 3** provides a high-level diagram of a potential process for providing access to full WHOIS data. As shown in the diagram, law enforcement agencies (and other governmental authorities) and private third parties would make a request the applicable certification body for access to full Thick WHOIS data. Users accredited by the relevant certification body would be recorded in a central clearinghouse, which would make the database of accredited users to registries and registrars. Accredited users would have query-based access to full Thick WHOIS data.

10. What is the legal basis for the Proposed Interim Model?

The legal justification for collection, use, and publication of the WHOIS data will be based on legitimate interests of the controllers, data subjects, and third parties, which will be discussed on a detailed basis in an analysis that will accompany the final version of the model.

As referenced in feedback from the Article 29 Working Party, "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".[3] This feedback suggests that legitimate interest could be used as the basis for a limited public WHOIS.

Also, the Hamilton legal analysis finds that, "... it should be possible to base such processing on legitimate interest as legal ground in accordance with Article 6.1(f) GDPR as long as the processing is limited to what is necessary, given the purpose."[4]

The community comments and the legal analysis suggest that the justification for collection, use, and publication of the WHOIS data can be based on lawful grounds set forth in Article 6 GDPR, including legitimate interests of the parties involved. As mentioned above, these lawful grounds will be detailed in an analysis accompanying the final model. This analysis will take into consideration that the WHOIS service is provided pursuing various public interests, as confirmed by the European Commission, which may constitute relevant legitimate interests pursuant to Art. 6 (1) (f) GDPR.

---

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

[4] Paragraph 2.4.3, https://www.icann.org/en/system/files/files/gdpr-memorandum-part2-18dec17-en.pdf

With respect to access to WHOIS data, the detailed legal analysis accompanying the final model will address a layered data access model for the Registration Data Directory Service on the legal basis of Art. 6 GDPR, and particularly how these legal bases correspond to each type of processing activity, purpose, and personal data element. A layered approach takes into consideration varying personal data elements in WHOIS data, limited open publication of certain data elements, and access by contracting parties and third parties to certain personal data elements, in each case tied to a defined purpose for which the data elements will be used, in order to ensure a legitimate basis for such processing as required under Art. 6 GDPR.

The detailed legal analysis will also address the accreditation program under which third parties requesting access to certain WHOIS data can be certified in order to ensure that (1) the personal data processing is consistent with the processing principles under Art. 5 GDPR, (2) the personal data are processed on a legal basis in accordance with Article 6 GDPR, and (3) adequate safeguards enforceable through a code of conduct and consistent with Article 32 GDPR have been employed.

IV. Next Steps

As noted in ICANN Org's 28 February 2018 Blog providing an update on our data protection/privacy activities, the community's feedback is requested on the Proposed Interim Model, preferably prior to ICANN61, where we will continue this conversation on the direction we are taking toward interim compliance with the GDPR.

Attachment 1 -- Sample of Minimum WHOIS Output Fields

WHOIS Data Fields	ICANN Proposed Interim 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
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 2 -- Accreditation Program for Continued Access to Full WHOIS Data

This document identifies a possible approach for an accreditation program to allow continued access to full WHOIS data for accredited users with a legitimate interest. In summary, the approach could provide access to public law enforcement and other governmental authorities recognized by governments, and to private third parties abiding by codes of conduct to be developed in consultation with the ICANN Governmental Advisory Committee (GAC). The document is intended as a starting place for further discussion on how to approach the following questions:

1. **Who would be eligible for continued access to full WHOIS data?**

   A defined set of groups with a legitimate interest, and certified under a formal accreditation program, would be eligible to continue to have access to full WHOIS data. A limited set of registration data would be available to the public as outlined in the proposed models for GDPR compliance being discussed by the community. Registrars would continue to follow their current practice of providing third-party bulk access to the limited set of registration data that would be available to the public.

2. **Who would be responsible for determining which categories of entities/user groups are eligible for access to full WHOIS data and for what purpose/legitimate interest?**

   The ICANN Governmental Advisory Committee could identify or facilitate the identification of entities/categories of user groups eligible for the accreditation program so that public policy considerations are appropriately taken into account. The purpose/legitimate interest for providing access to full WHOIS data is the subject of ongoing community discussion, including with the GAC, as part of the proposed interim model.

3. **Would public law enforcement or other governmental authorities have access to full WHOIS data?**

   Individual countries, through the GAC, could provide a list of law enforcement authorities and other governmental authorities who should be certified for continued access to full WHOIS data. Registries and registrars would provide global access to these law enforcement authorities, subject to applicable laws.

4. **Would private third parties have access to full WHOIS data?**

   ICANN Org could work with the GAC to identify specific categories of private third-party user groups eligible for continued access to the full WHOIS data. The categories of user groups could include, for example, certificate authorities and licensed attorneys representing intellectual property rights holders. Additionally, (i) ICANN Org would continue to have access to full WHOIS data to carry out its security and stability mission, and to facilitate compliance activities related to enforcing its contracts and policies, (ii) ICANN accredited registrars would have access to full WHOIS data to facilitate transfers of domain names, (iii) ICANN-approved dispute resolution providers administering the Uniform Domain Name Dispute Resolution Policy and the Uniform Rapid Suspension, for example, would have access to full WHOIS data for continued administration of ICANN dispute resolution processes and policies; and (iv) ICANN-approved data escrow agents would have access to full WHOIS data to facilitate verification of registration data submitted by registries and registrars.

5. **After the GAC determines which categories of user groups would be eligible for access, who would accredit specific entities in the approved categories?**

   With respect to law enforcement authorities, as noted above, it could be up to individual governments to determine which authorities in their jurisdiction should be granted access. This information could be communicated via the GAC.

   With respect to private third parties, the GAC could be consulted on the identification of relevant bodies which have the appropriate level of expertise related to each user group. Also, the GAC could be asked to advise on developing an appropriate code of conduct for those who would have access to the full set of WHOIS data. These bodies could serve as the "certifying bodies" for the relevant user group and could establish criteria to determine whether a specific entity is eligible as part of a category of user group. The certifying body could monitor compliance with the established code of conduct.

6. **Who would maintain the list of accredited entities and/or users? How would it be updated?**

   For transparency, the list of accredited entities and/or users (i.e. law enforcement authorities and private third parties) could be made publicly available in a central repository managed by ICANN or at ICANN's direction. Updates and other changes to

the list of accredited entities and/or users could be managed via the GAC (for law enforcement and other governmental authorities) and via the certifying body (for private third parties).

7. **Would there be any limitations on how the full WHOIS data could be used?**

   Yes, the GAC could assist in developing or advise on developing codes of conduct or principles for codes of conduct for the eligible categories of private third-party user groups. The codes of conduct could establish the appropriate limitations on use of the data, proper procedures for accessing the data, and other safeguards and public policy considerations relating to the responsibilities and practices for the third-party user group.

   In general, the data must be used for the purposes it was provided, and it must not be forwarded to unauthorized third parties.

8. **Once accredited, what technical methods would be used to access to the full WHOIS data?**

   There are a number of technical methods that could be used to provide access to the full WHOIS data, and ICANN Org would work with the technical community to develop secure mechanisms to do so. For example, access to the full data could be achieved by maintaining a whitelist of IP addresses in a central repository. When the WHOIS is queried from an address on the whitelist, the full contact data would be returned.

   Another alternative could be a PIN/token/certificate issued to accredited users to use to query WHOIS databases, either via web-based queries or possibly through the implementation of the Registration Data Access Protocol (RDAP).

9. **Would the identity of those submitting WHOIS queries be known to registrants or other third parties?**

   Pending further policy development, the status quo would be maintained -- the identity of the person/entity submitting a WHOIS query would not be visible to the registrant or other third parties. Depending on the technological solution used to implement accredited access, the IP address of the requester would continue to be visible to the registry and registrar operating the WHOIS service, but no new requirements regarding the identity of the requesting user are proposed.

10. What is the scope of data that would be available to accredited users?

The accreditation program would provide query-based access to current WHOIS data. Some commentators have suggested that additional bulk access and searchability features should be included in the model. In the absence of further policy development, the status quo would be maintained in that additional bulk access, searchable or historical WHOIS data would not be required features.

11. Would there be a central repository of WHOIS data from which access would be granted?

No, registries and registrars would maintain current requirements to operate a WHOIS service available via port 43 and a web-based Directory Service.

Attachment 3 -- Draft High-Level Diagram of a Potential Process for Providing Access to Full Thick WHOIS Data