Details of the Proposal

Draft Model to Address the GDPR submitted by Coalition for Online Accountability

This document addresses how the proposed model submitted by the Coalition for Online Accountability entitled "Working Draft GDPR Compliant WHOIS Model" considers the various points and questions articulated by ICANN org in the Guidelines for Proposed Models to Address the General Data Protection Regulation (GDPR).

1. Analysis of how the model accommodates existing contractual obligations while reconciling them with the GDPR, including:

a. A description of the proposed change and how it differs from the current implementation;

For registrations subject to GDPR, the model specifies ten purposes for the collection of data for inclusion in a WHOIS directory and subsequent access and use by third parties (see section 2: Purpose Statement). While some of the data collected would be accessible without substantial change from the status quo (see sections 4.1 and 4.2 regarding non-personal data of registrations by legal persons and natural persons), other data would be subject to greater control by registrants: an opt-out and data substitution procedure for personal data related to legal persons registrations (section 4.1), and a consent procedure for personal data relating to registrations by natural persons (section 4.2). To the extent that natural persons registrants refuse or withdraw consent, the WHOIS Data Access Model provisions in section 5.1 provide a procedure to third parties to seek access to data by identifying themselves, specifying the purposes for which the sought data would be used, and committing to restrict uses of that data to those purposes. The WHOIS Data Access Model also provides for processing of registrant objections to third party access and use of data for particular purposes.

By contrast, the current implementation does not provide for an exhaustive list of permissible third-party uses; makes no provision for substitution of non-personal for personal data; does not provide for registrant withdrawal of consent or objection to uses by third parties; and is based on a structure of anonymous access to WHOIS data containing personal information, with very few restrictions on third party uses.

b. Identification of how the model impacts current ICANN contractual obligations and specification of the contract provision or policy that is impacted by the cited law;

The main impact of the model would be on section 3.3.1 of the 2013 RAA and the REGISTRATION DATA DIRECTORY SERVICE (WHOIS) SPECIFICATION thereto. These provisions require registrars to provide unrestricted public access to WHOIS data. As noted above, under the proposed model, this paradigm would be modified for certain registrations subject to GDPR, particularly those made by registrants who are natural persons. Corresponding modifications would ultimately be needed to the RDDS provisions of the Base Registry Agreement. We have not yet made a comprehensive survey of all contractual obligations or consensus policies that would be affected by the adoption of a WHOIS model compliant with GDPR.

Nevertheless, in constructing the model we have been mindful of and have sought to adhere to ICANN President and CEO Goran Marby's guidance to find "a path forward to ensure compliance with the GDPR while maintaining WHOIS to the greatest extent possible."(see https://www.icann.org/news/blog/data-protection-privacy-activity-recap)

c. Identification of the applicable section(s) of the GDPR;

This model focuses particular attention on ensuring compliance with Article 13(c) and (d) by setting forth fully the various purposes for processing personal data, particularly processing and access by third parties (including governmental and non-governmental entities) based on legitimate interests. [See section 2 – Purpose Statement]. Article 13 requires that data subjects be informed of the various purposes for which their personal data may be used and the legitimate interests that may be triggered for accessing/processing the personal data at the time the data is collected by the controller. Therefore, we believe it is critical that any model for WHOIS that seeks to comply with the GDPR set forth and detail the entire anticipated range of purposes and legitimate interests that may be implicated, including those of third parties that may legitimately seek access to the personal data.

This model also complies with and recognizes the provisions of Articles 3 and 4 in terms of addressing scope and distinguishing between natural persons—proper "data subjects"—versus legal persons/entities. [See section 1 – Scope]

Throughout, this model seeks to comply with the restrictions and safeguards set forth in Chapters II and III of the GDPR concerning Principles and the Rights of the Data Subject.

d. A description of how this change will comply with the applicable law.

Because this model fully sets forth the scope of purposes and various legitimate interests for which personal data is sought to be collected and processed, including processing by third parties, this model complies with the informational requirements set forth in the GDPR, particularly Article 13(1)(c) and (d).

Many of the purposes of this model are derived from the GAC Communique – Abu Dhabi of November 1, 2017 and incorporate the GAC Principles Regarding gTLD WHOIS Services of March 28, 2007. This model recognizes, as does the GAC, that WHOIS data, including personal data that constitutes WHOIS data, serve an array of important purposes and legitimate activities—including those of third parties such as governments and intellectual property rightsowners. Therefore, this model seeks to preserve and protect those important and legitimate purposes and activities to the maximum degree while complying with the requirements of the GDPR.

Because this model does not have a "default" presumption that personal data will be made publicly available, it complies overall with the GDPR. This model incorporates detailed and clear consent procedures, including ensuring that consent is freely given and that obtaining the services from the registrar (e.g., purchasing a domain name) is not conditioned upon consent. [See section 4 – Determining Whether Data Elements May be Made Publicly Available]. This model also incorporates a process for legitimate third-party access in accordance with the GDPR and includes right to object provisions and thus complies with Articles 6 and 21 of the GDPR.

Because this model is still under development, it does not yet address all of the requirements of the GDPR, such as the conditions to transfer personal data to other countries. We are continuing to work on the model and plan to address those other requirements in due course. In such work, we look forward to the input from other stakeholders and working in collaboration with others.

2. Changes to the collection, storage, display, transfer, and retention of data.

The proposed model would have little impact on the collection of data or its storage. It would impact the display of such data to third parties, its transfer to third parties, and retention practices (which would be tied to the list of permitted purposes) where such data constitute "personal data" that are subject to the requirements of the GDPR.

3. Who will be impacted by the change and how (for example: registrants, users of WHOIS data, other contracted parties).

Registrants of registrations falling within the scope of the proposed model would be asked to identify themselves as legal or natural persons. If legal persons, to the extent that they provide WHOIS data containing personal data, they would be given the possibility to opt out of inclusion of this data in the publicly available WHOIS database, by substituting non-personal data. If natural persons, if they choose not to consent to public access to their personal data, such data would be excluded from the publicly accessible database. Such registrants would also have the power to withdraw consent, and to object to access by third parties under the section 5.1 WHOIS Data Access Model.

Users of WHOIS data would be impacted primarily in terms of access to personal data of natural persons registrants subject to GDPR who have not consented (or have withdrawn consent) to publicly access their personal data. In such cases, users wishing to access such data would have to identify themselves to the registrar or its agent, specify the purposes for which they will use the data sought, and commit to restrict their uses accordingly.

Registrars would need to implement systems to enable registrants to self-identify as legal or natural persons; modify their processes for obtaining consent to meet GDPR standards and to provide for withdrawal of consent; create (or participate in) a facility for processing data requests under section 5.1; and implement processes for dealing with registrant objections to access and use for particular purposes, including processes for working with requesting parties to determine whether such objections should be overridden in accordance with GDPR Article 21.

4. Interoperability between registry operators and registrars.

We have not yet addressed this interoperability issue in our model. Again, our model is a "work in progress" and we intend to continue developing it and hope to collaborate with others in so doing.

5. How users with a legitimate need for data will request and obtain data if it is no longer available in public WHOIS.

This model contemplates that third parties may access personal data that is not publicly available only for legitimate purposes as set forth in section 2 – Purpose Statement and on the basis of a self-certification process as set forth in section 5 – WHOIS Data Access Model. In proposing a simple and straightforward self-certification model, this model seeks to minimize the burden on registrars as well as third parties. It also seeks to facilitate the legitimate purposes and interests articulated by the GAC and to comply with the GDPR while maintaining WHOIS to the greatest extent possible.

6. Whether data handling will be uniform or if there will be variation based on things such as "natural person" vs. an organization, physical address of a point of contact, location of the registry operator or registrar, etc.

This model contemplates making distinctions in the handling of data based on the Scope (Article 3) and Definitions (Article 4) of the GDPR. Section 1 – Scope sets forth territorial/nationality distinctions as set forth in the GDPR and states that this particular model for WHOIS only applies to the processing of personal data that falls within the scope of the GDPR as set forth in Article 3 of the GDPR. Similarly, this model draws distinctions between natural persons and legal persons in accordance with the GDPR such as in section 4 – Determining Whether Data Elements May Be Made Publicly Available.

7. Whether this model has been reviewed by a data protection authority. If so, indicate which data protection authority, when, and any details of their response.

This model has not yet been reviewed by a data protection authority.

8. High-level description of any changes to other agreements beyond the Registry Agreement and Registrar Accreditation Agreement (for example: Registry-Registrar Agreement, Data Escrow Agreement, Registration Agreement, Registrar Reseller Agreement, Privacy Policies, etc.).

We believe changes to ICANN agreements will be required by adoption of a model to comply with the GDPR, but we think it is premature to try to detail those changes until a model appears likely to be settled upon for implementation.

9. If applicable, how this differs from other models and whether you endorse any other model. If you endorse another model, please identify whether you endorse the entire model or specific sections.

We are not aware of any other models that have been submitted to ICANN via this process. We have reviewed at a high—but not yet detailed—level the v.061 draft eco GDPR Domain Industry Playbook ("eco model"). We would like to express our appreciation to eco for making its draft model available for review and for organizing the recent meeting in Brussels on December 11 to explain and discuss the model.

Our model is similar to the eco model in that it provides registrants the ability to shield their personal data from public availability. Like the eco model, our model also provides third parties that demonstrate a legitimate interest the ability to access non-publicly available personal data. In terms of conceptual frameworks, we think our model and the eco model are compatible insofar as they both adopt a tiered access approach. Where our model differs from the eco model is that the eco model seems to treat all data as falling within the scope of and subject to the requirements of the GDPR. Furthermore, the eco model does not appear to draw distinctions between natural persons and legal persons in terms of treatment of data. In contrast, our model seeks to maintain as much public accessibility of WHOIS data as possible and, therefore, focuses on the scope and type of data covered by the GDPR as set forth in Articles 3 and 4 of the GDPR. In so doing, our model seeks to ensure compliance with the GDPR while maintaining current WHOIS to the greatest extent possible.

Understandably, the eco model focuses on the uses of data by registrars in their contractual/business relationship with registrants. Our model does not focus on those purposes, but we believe any final model will have to address the purposes of the registrar (likely data controller) as well as the purposes of third-parties in accessing and processing the data. While the eco model does address third party access and legitimate interests, we believe it does so in an overly narrow fashion to the detriment of legitimate interests. In addition, we believe our proposals for access provide a more efficient way of balancing the rights of data subjects with the legitimate interest in accessing data. For example, the eco model will require new infrastructure (in the form of a certification body). We think a self-certification process, as we have proposed, will be easier for all parties to implement and one that does not involve such a drastic departure from the existing WHOIS system.

We appreciate that the eco model acknowledges that "certain patterns at the registered domains must be received for a successful mitigation of abuse" and that under certain circumstances unless data of all registrants from various registrars is made available "sustainable recognition of patterns [of abuse] would be impossible." Indeed, we have incorporated that principle in Purpose number 8 of our model's Statement of Purposes in section 2.

We look forward to working with eco and others to attempt to reconcile the various proposed models in a manner that not only complies with the GDPR but also properly balances the interests and needs of all parties.