Jan 29th, 2018

Dear Göran,

This comment is submitted by eco Association of the Internet Industry, an association with more than 1000 members from more than 60 countries. More than 150 of these members work in the domain industry. eco has developed the eco GDPR Domain Industry Playbook, which has been submitted to ICANN as a community proposal. The submission of the Playbook has been supported by numerous registries and registrars. The list of these companies is available at https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en as well as the full proposal.

We have reviewed your document titled „Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union´s General Data Protection Regulation" which you have made publically available at https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf

We do not believe that any of the models as presented in this document is compliant with GDPR requirements. We would like to comment on all three models you have presented in the document.

I. Misleading Presentation of the Models

ICANN's announcement post published at the link above includes the following:

> "These models reflect discussions from across the community and with data protection authorities, legal analyses and the proposed models we have received to date."

This statement suggests to the reader that the models have been based on legal analysis and feedback from data protection authorities, i.e. the reader must believe that choosing all models offered are compliant with the requirements established by the GDPR. Yet, ICANN has confirmed during a webinar held by the IPC and BC that e.g. the legal memos by Hamilton have not been used as a basis for the models.

Also, the models do not reflect the community models that ICANN has received. The eco GDPR Domain Industry Playbook, a comprehensive legal analysis and data model, is not reflected in the ICANN proposals. It is unfortunate that ICANN did not do the extensive work by the community justice by offering those models the same visibility and attention as their own models.

We consider such communication misleading.

II. No comprehensive legal assessment possible

Generally, we believe that the models presented are based on the idea of maintaining the status quo as much as possible. From our point of view the way to achieve compliance with GDPR should rather be reviewing the data flow between contracted parties and evaluate whether such data flow can be based on legal ground compliant with GDPR. When reviewing the data flows all basic principles such as data minimization and purpose limitation must be considered, which does not seem to be the case in these models to the depth that is needed to achieve a compliant model.

The models offered by ICANN can only be characterized as rough sketches, but not as models that allow for a legal analysis, let alone implementation.

III. Focus on disclosure only

All models focus on disclosure of data, i.e. the Whois part. None of the models assesses other processing of data, although such analysis is required to establish compliance. What can be transferred to escrow agents, to the EBERO? What are the roles and responsibilities of the parties involved, including ICANN? According to the transparency and information requirements according to the GDPR, the data subject needs to be provided with information on the roles and responsibilities. Absent a discussion and conclusion on who is the (joint) data controller or the data processor, no model can be adopted or operationalized.

IV. Data minimization

The most striking point appears to be that collection of all data elements that ICANN currently requires to be collected remains unaltered without any further review or explanation.

The basic principle of data minimization requires restricting all data processes to the minimum which also applies within the individual legal basis for justifying the process itself. Therefore, the principle also needs to be considered when discussing the legal basis of performance of contract with regard to the transfer and processes of data to and by the registry.

This principle seems not to be fully appreciated by the models as they are presented in this document as it is simply stated that the full transfer of data to the registry is necessary for the performance of the contract.

V. Transfer of data from registrars to registries

One of the commonalities across all models is that registrars may transfer all data to registries.

While it is possible to achieve this, it is necessary to base such transfer on legal grounds. The “Purpose description” of this document is not sufficient for that.

Rather, such transfers can either be based on performance of a contract (Art. 6 I b GDPR) where the registry performs e.g. the validation of eligibility requirements. Additionally, our legal assessment further specified in the eco GDPR Domain Industry Playbook offers a non-exhaustive list of existing legitimate interests that registries are free to assert and document to lawfully obtain data from the registrars.

VI. Purpose description

It is stated that it would be desirable to have a WHOIS system for the purposes named in the document. None of the purposes named requires having a Thick WHOIS at the registries at least not without further explanation; in particular it seems all the purposes named could be managed at registrar levels. Therefore, we see the requirement to further elaborate on the purposes described in the document in particular regarding the question why this purpose can (only or better) be fulfilled by the registry rather than the registrar as only this would justify the transfer of all data to the registry.

VII. Commentary and questions on the models

1. <u>Model 1</u>

a) Only applicable to registration data of natural persons

Model 1 states to be only applicable for data from natural persons registering a domain name. However, registration of a domain name by legal persons can still contain personal data of natural persons. This not only applies to possible contact details for Admin- and Tech-C; also the domain name itself can contain references to natural persons which fall into the applicability of the GDPR. This is particularly true for company names which consist of the natural person´s name behind the company and smaller companies consisting only of maybe one person.

Recital 14 does not say anything different as it only concerns legal person's rights; in the above examples, the legal interests of the natural person are concerned to which GDPR fully applies.

The differentiation between natural and legal persons´ data for compliance with GDPR is not manageable without high administrative effort if at all possible. Therefore, a model should apply equally to data from natural and legal persons.

b) **Why is the publication of registrant data, Admin and Tech-C in a public WHOIS system necessary for the performance of the contract or based on legitimate interests?**

For the registration of a domain name it is not necessary to publish name and address of the registrant or the contact details of an Admin or Tech-C in a publically available WHOIS system. Art. 6 I b) GDPR cannot justify such disclosure of personal data.

Also, Art. 6 I f) does not seem right to justify such disclosure. This would require a legitimate interest by the registrar that override the data subject´s rights.
Making available the registrant name and address to the broad public is a very intense intrusion into the data subject´s rights and needs careful evaluation when arguing with legitimate interest. The purposes stated in the purpose description of the document do not seem to allow such interpretation of overriding interests by the registrar.

c) Why not use role contacts?

For the purpose of providing a possibility for third parties to contact the registrant, Admin-C or Tech-C for a certain domain name, a less intrusive measure would at least be to publish only role contacts rather than actual contact details of natural persons.
Therefore, even in case the disclosure of contact data is evaluated necessary for the performance of contract (which is highly doubted) or can be based on legitimate interest in general, we see no reason why the disclosure of role contact details not containing personal data, cannot achieve the same purpose while limiting the intrusion in the data subject´s rights.

d) What legitimate basis has the retention of data for 2 years according to this model? Would this apply to all data equally? What purpose does the retention of the e.g. phone number have?

It is stated that all data shall be retained for 2 years after the termination of the domain name registration.

Generally, GDPR requires deleting all data as soon as the purpose of collection has been fulfilled unless there is retentions obligation or further justification for the retention in place.

It is not stated for what purpose the data is retained; therefore, it cannot be reviewed whether the purpose is actually sufficient for such a long period of retention to be compliant with the GDPR.

2. <u>Model 2</u>

a) <u>Disclosure</u>

The model indicates that no personal data is disclosed without consent from the data subject and suggests the implementation of a certification procedure.

Please note that the ECO model has already provided an example for the implementation of such a certification and access model.

Valid consent may of course be the basis for disclosure of data in a public WHOIS system.

b) <u>One year retention?</u>

Please see above III d).

3. <u>Model 3</u>

a) <u>Permission by data subject</u>

In the description it is only stated that no further personal data is displayed without consent from the data subject. In Appendix 2 it is then stated that most data is displayed unless it contains personal information.

It is unclear how this process shall be implemented. We assume that any data fields shall be displayed if they do not contain any personal information. In case they do contain such information, they shall only be displayed with consent from the data subject.

It can be quite difficult to determine whether information is personal according to GDPR or not. This can only be determined with certainty on a case to case basis taking all other information provided and possibly displayed into account.

This can cause lot of administrative effort for registrars trying to determine what can be and cannot be published in the WHOIS system. A streamlined system where the data to be published is clearly defined for all contracted parties is preferable.

b) <u>Retention of data</u>

The retention period of 60 days is not explained and therefore cannot be reviewed for compliance with GDPR requirements.

c) <u>Disclosure</u>

The limitation of access to WHOIS data for third parties providing a subpoena or any similar court order seems too strict.

There are many reasonable interests by third parties who could justify the disclosure of registrant data based on legitimate interest or even for performance of contract,

e.g. UDRP and URS procedures. In many cases it would be unreasonable and unacceptable to require third parties to achieve a court order to obtain information on the registrant of a domain name. For example, reviewing whether a trademark infringement occurs on a website, it can often require reviewing who is owner of said domain name to evaluate whether this owner has any own rights in the mark in question. It would be a too high of a barrier to require a court order just to have the possibility to review whether an infringement is given or not.

VIII. Action required

We urge ICANN to

- enter into discussions with the contracted parties to settle on a mutually acceptable model to avoid the risk of being sanctioned and not take a decision unilaterally;
- acknowledge that ICANN cannot take a decision on its own on a model;
- continue the dialogue with the Art. 29 WP and other appropriate bodies together with the contracted parties;
- set the record straight about the misleading announcement of the models; and
- provide a robust legal rationale for the models published as well as any other models that ICANN may publish in future for GDPR compliance.

Respectfully submitted,

Thomas Rickert
Director Names & Numbers
eco Internet Industry Association

The following companies and organizations have asked to be listed as supporters of these comments:

- 1&1
- Akamai
- Astutium
- Blacknight
- Brandma.co
- DNS Africa
- Dominion Registries
- Donuts

- Internet Infrastructure Coalition (i2Coalition)
- GoDaddy
- NetEarth One
- Netistrar
- Nordreg
- Public Interest Registry
- Realtime Register
- regiodot GmbH & Co. KG (.ruhr)
- SafeBrands
- Tucows
- Wolf-Ulrich Knoben, DE-CIX, ISPCP constituency member