

ANNEX 1

Date: 23 January 2018

Subject Invitation for comments on [Proposed Interim Models](#) for Compliance with ICANN Agreements and Policies in Relation to European Union's General Data Protection Regulation (published 12 January 2018):

Comments by the Bureau of the Committee of Convention 108

Against the background expressed in the letter, the Bureau of the Committee of Convention 108 is offering the following preliminary comments on the proposed interim models:

General comments

- The GDPR (fully applicable as of 25 May 2018) is only one amongst several legal instruments addressing the universal human right to privacy (Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights). Data protection legislations adopted by countries located on all continents contain similar provisions to those of our Data Protection Convention (also known as "Convention 108). Convention 108", 37 years old this year is the only binding legal instrument at international level and already served for a number of countries as source of inspiration, imposes legal requirements which should be complied with by any controller subject to the law of a particular country. Some of those requirements which have been laid down since 1981 with Convention 108, include the right to correction of data, right to erasure under certain conditions, the principles of proportionality, of purpose limitation, of lawfulness of the processing (legal basis), etc. The solutions to be developed need to be global.
- The limited publication of WHOIS data can serve the legitimate interests of the controller and it should be added that it could also serve important public interests. The publication however has to serve a specific and predefined purpose and has to be necessary and proportionate to the fulfilment of this purpose.
- In this sense, for example, bullet 1 on page 6 should specify to whom "legitimate" (not "appropriate") "access to accurate, reliable and uniform registration data" is to be provided.
- For non-public WHOIS data, the models propose different layered access solutions. The legal, technical and practical issues related to these solutions would need to be evaluated.

Comments on models proposed

- **Option 2B** would seem to be the most appropriate solution in striking the right balance between different concurring interests and ensuring the adequate guarantees to meet the most stringent privacy requirements.

- The second preferred option would consist in a mixed model encompassing elements presented in Option 1 and in Option 2B, maintaining the distinction between natural and legal persons and adjusting the publicly displayed information according to that distinction. The publication scheme proposed in Option 2 could be applied if the domain name is registered by a natural person, to the exception of admin phone, admin phone ext, admin fax, admin fax ext, tech phone ext, tech fax ext which would be displayed. For legal persons, the publication scheme proposed in Option 1 would be applied. Caution is called concerning the possibility given to Registries and Registrars, under Option 2 to provide additional access to non-public WHOIS data “as long as it complies with the GDPR and other applicable law” as this could lead to discrepancies and uncertainties in the implementation of this possibility.
- On the Chapter “Commonalities Across All Models” on page 4, the suggestion that “[...] all personal data currently included in Thick registration data” can be collected, should only be understood as an ad-hoc, interim solution. To define exactly which data set is needed for the purpose of the processing, a proper analysis and a complete Privacy Impact Assessment would seem to be a prior necessary step and a mention of this in the text would be welcome.
- On points 1, 2, 3, 4 of the same Chapter stating that the data processing can have as legal basis the “[...] performance of the contract and the legitimate interests pursued by the controller or by a third party”, the reference to the legitimate interests of a third party as legal basis for the processing should be questioned as a controller always processes personal data for its own predefined and specific purposes and does not usually process personal data for the legitimate interests of an unspecified third party.
- As to point 1 in the Chapter “The purpose of WHOIS” on page 6, it is recommended to specify to whom it would be desirable to provide “[...] appropriate access to accurate, reliable and uniform registration data”.
- In Point 5 of the same Chapter, the word “legitimate” should replace “appropriate” to qualify the law enforcement needs as it better reflects the conditions set forth by applicable legislation for law enforcement access.
- As to the retention period foreseen for Model 1 and 2, providing an explanation as to why two or one year would be necessary instead of 60 days, as proposed for Model 3, would be recommended.
- For the accreditation of legitimate requestors a centralised model with accreditation by ICANN is preferred and a single access point model should be developed as soon as possible. The “enforcement solution” proposed in Model 2 where “registries and registrars must provide ‘certified’ requestors access to non-public WHOIS data based on pre-defined criteria and limitations” is more likely to meet law enforcement needs while respecting data protection requirements.