

To the attention of Mr Marby
goran.marby@icann.org

E-mail: contact@apd-gba.be

Your reference

Our reference

Enclosure(s)

Date

SA2/DOS-2018-03638

04-12-2019

Re: Unified Access Model for gTLD Registration Data proposal 25 October 2019

Dear Mr. Marby,

I am writing you in response to your letter of 25 October 2019, in which you raise a number of questions concerning a Unified Access Model (UAM) as a centralized system for access to non-public registration data regarding gTLD domain names. Your questions essentially concern the structure of the model proposed by ICANN org, as well as the roles and responsibilities of the parties involved in the disclosure of personal data under GDPR in this context.

1. Structure of the proposed model

In its statement of 25 May 2018, the EDPB reiterated the expectation that ICANN develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data.¹

I understand from your letter and accompanying documents that the proposed UAM is intended to facilitate standardized access and disclosure to non-public registration data. No final determination has yet been made, however, in relation to the parties which may be authenticated and authorized, nor for what data fields they may acquire. Other areas of work include the determination of appropriate safeguards for personal data

¹ https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_en



processed in such a system, such as steps to ensure data accuracy, data security, minimization, logging of requests and mechanisms to verify requestors' identities and legal bases for access to requested data.²

ICANN org is proposing a UAM which would provide a centralized system for access to non-public registration data, as opposed to a decentralized system. In the centralized system, ICANN org would take on the responsibilities associated with the operation of central gateway through which requests for access to non-public registration data would be accepted and processed. Under a decentralized system, in contrast, each Contracted Party would (continue to) be responsible for directly receiving and responding to requests for disclosure. In this context, ICANN org is seeking guidance as to whether or not a centralized unified model would ensure a higher level of protection for natural persons than a decentralized (distributed) system.

As a starting point, I would like to remind you that, in accordance with the principle of accountability, it is the responsibility of the relevant controllers and processors to implement appropriate technical and organizational measures in accordance with articles 24, 25 and 32 GDPR. It is not the role of a supervisory authority to validate or approve the suitability of organizational or technical measures which are being considered by a controller as part of its compliance obligations.

Moreover, on the basis of the information provided, it is not possible to make a determination as to whether or not the proposal for a centralized UAM will deliver a higher level of data protection than a distributed system. The proposed UAM is premised upon the "*assumption that there will be a policy to be developed by ICANN's multistakeholder community that sets forth specific access requirements that can be applied through the UAM*". It is expected that such a policy would describe who gets access to what, and under what conditions, for how long, as well as other relevant safeguards.³ From a data protection perspective, however, such elements will be extremely important when assessing whether the model which is ultimately developed complies with the requirements of the GDPR. Finally, whether or not a centralized model increases or decreases the level of protection enjoyed by natural persons will depend on how the relevant policies and safeguards are applied and administered in practice.

I encourage ICANN org to continue its efforts to design a comprehensive system for access control which takes into account the requirements of security, data minimization and accountability. In this context, I also encourage ICANN org to take note of the draft Guidelines recently issued by the European Data Protection Board on Article 25 Data Protection by Design and By Default.⁴

² ICANN, "Exploring a Unified Access Model for gTLD Registration Data", 25 October 2018, p 20-21, available at <https://www.icann.org/en/system/files/files/unified-access-model-gtld-registration-data-25oct19-en.pdf>.

³ ICANN, "Exploring a Unified Access Model for gTLD Registration Data", 25 October 2018, p 20

⁴ European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and By Default, 13 November 2019, Draft version for public consultation, available at https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

2. Roles and responsibilities

The proposed UAM seeks to centralize responsibilities associated with the disclosure of personal data contained in gTLD registration data and to increase the consistency in responses.

As indicated earlier, ICANN org proposes to take on the responsibilities associated with the operation of a central gateway through which requests for access to non-public registration data would be accepted and processed. In this context, ICANN org is seeking guidance as to whether or not it would be possible to “remove” certain controller-related responsibilities from Contracted parties, in particular in relation to the acts of (a) deciding whether or not to disclose non-public registration data to third parties and (b) disclosing nonpublic registration data to a requestor.

As a starting point, I would like to stress that the concept of “controller” and “joint controller” are autonomous concepts of EU law, which must be interpreted in light of the jurisprudence of the CJEU.⁵ Parties to a processing operation therefore are not free to simply “designate” which party shall be deemed to act as a controller or joint controller, as the case may be. Instead, a factual and case-by-case assessment is necessary to determine the role of the parties involved.

In its letter of 11 December 2017, the Working Party 29 indicated that *“At first glance it would seem that since ICANN and the registries jointly determine the purposes and means of the processing of personal data for the WHOIS directories, ICANN and the registries are joint controllers. This would mean that both ICANN and the registries must ensure that personal data are processed in accordance with the obligations of the European data protection laws”*.⁶

Insofar as ICANN acts as a joint controller, together with the registries and/or registrars, they must act within the boundaries of article 26 GDPR which implies that:

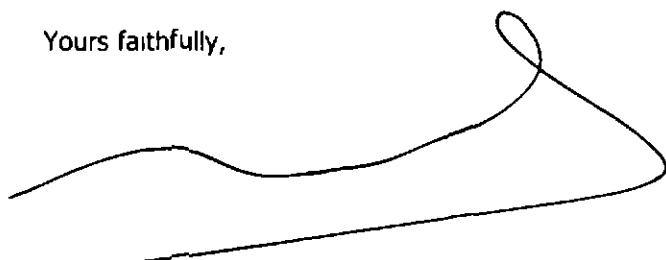
- ICANN together with the registries and/or registrars must determine their respective obligations for compliance with the obligations of the GDPR, in particular as regards the exercising of the rights of the data subject and article 13 and 14 by means of an arrangement. As prescribed by article 26.2 and art.26.3 GDPR, this arrangement must duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects and irrespective of the terms of the arrangement, the data subject would be entitled to exercise his or her rights under the GDPR in respect of and against each of the controllers involved.
- each (joint) controller shall remain accountable for ensuring compliance with data processing operations under its control and cannot abdicate its responsibilities by virtue of a joint arrangement.

⁵ See in particular the Judgment in *Wirtschaftsakademie*, C-210/16, ECLI EU C 2018 388, the Judgment in *Jehovah's Witnesses*, C-25/17, ECLI EU C 2018 551 and the Judgment in *Fashion ID*, C-40/17, ECLI EU:C 2019:629.

⁶ Article 29 Data Protection Working Party, Letter to Dr Cherrine Chalaby and Mr Goran Marby, 11 December 2017, available at www.ec.europa.eu/newsroom/just/document.cfm?doc_id=48839

The analysis contained in this letter has been made on the basis of the information currently available to the Secretariat of the Belgian Data Protection Authority. It does not preempt a later formal decision by the Belgian Data Protection Authority, including in the context of an enforcement proceeding. Any decisions concerning cross-border processing shall be subject to the cooperation and consistency mechanism provided by Chapter VII of the GDPR.

Yours faithfully,

A handwritten signature in black ink, consisting of a long horizontal stroke that curves upwards at the right end, forming a loop.

David Stevens

Secretary General