

To the attention of Mr. Göran Marby
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers
(ICANN)

Please contact+

T: 32 (0)2 274 48 00

F: +32 (0)2 274 48 35

E-mail: contact@apd-gba.be

By e-mail: goran.marby@icann.org

Cc: info@dataprotection.ie; edpb@edpb.europa.eu

Your reference	Our reference	Enclosure(s)	Date
	SA2/DOS-2018-03638		

Re: Information regarding ICANN Contractual Compliance Data Processing Activities and the European Union's General Data Protection Regulation (GDPR)

Sir,

I refer to your letter of 6 December 2018 regarding ICANN's Contractual Compliance Data Processing Activities, which you have addressed both to myself and my colleague, Helen Dixon, in her capacity as Data Protection Commissioner of the Irish Data Protection Commission.

In my letter of 26 September 2018 regarding the activities of ICANN's Brussels branch office, I have explained why the Belgian Data Protection Authority shall be competent to act as "lead supervisory authority" for any cross-border processing of personal data carried out by ICANN, including, as the case may be, processing of personal data in the context of WHOIS. Indeed, pursuant to article 56(1) of the GDPR, the supervisory authority of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor. In your letter of 9 August 2018, you indicate that ICANN has only a single regional office on EU territory, namely in Brussels.

Article 56(6) of the GDPR provides that the lead supervisory authority shall be the *sole interlocutor* of the controller or processor for the cross-border processing carried out by that controller or processor. While ICANN remains free to address correspondence to more than one supervisory authority as regards its data



processing activities, the principle of the sole interlocutor entails that it may not always receive a relevant response from an authority other than the lead supervisory authority.

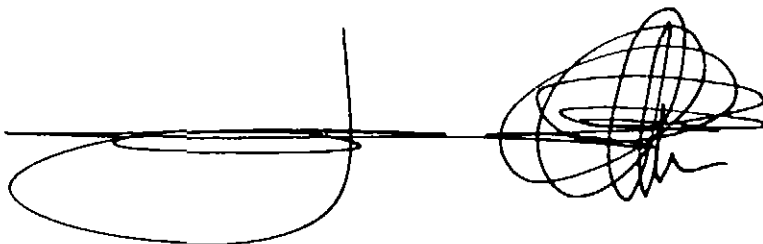
As regards the substance of your letter: you take the view that data transfer safeguards shall not be required in cases where the GDPR is directly applicable to the recipient of the data, even if the recipient is located in a third country.

In this regard, it should be noted that article 44 and following of the GDPR do not stipulate that appropriate safeguards shall no longer be necessary in case where the GDPR is directly applicable to the recipient of the data. Article 46(1) GDPR instead refers to the obligation of the controller or processor to provide appropriate safeguards in case of (any) transfer to a third country or international organization in the absence of an "adequacy decision" pursuant to article 45(3). The only derogations to this general principle are enumerated in article 49 GDPR.

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, such as in the context of an enforcement proceeding. Any decisions concerning cross-border processing shall be subject to the cooperation and consistency mechanism of provided by Chapter VII of the GDPR.

Finally, I wish to note that the GDPR places responsibility for compliance with the provisions of the GDPR upon the (joint) controller(s). It does not provide for a system of prior consultation, except in the case of article 36. It also does not foresee the possibility of prior approval, except in the cases mentioned by articles 40 (codes of conduct) and 47 (binding corporate rules).

Yours faithfully,

A handwritten signature in black ink, consisting of a large, stylized 'W' followed by a series of overlapping loops and a final flourish.

Willem Debeuckelaere
President



6 December 2018

Mr Willem Debeuckelaere, President
Autorité de la protection des données
Rue de la Presse 35
1000 Brussels, Belgium
email: contact@apd-gba.be

Ms. Helen Dixon, Data Protection Commissioner
Data Protection Commission
21 Fitzwilliam Square Dublin 2
D02 RD28, Ireland
email: info@dataprotection.ie

Re: Information regarding ICANN Contractual Compliance Data Processing Activities and the European Union's General Data Protection Regulation (GDPR)

Dear Ms. Dixon and Mr. Debeuckelaere:

I wanted to take this opportunity to share some information with you about ICANN org's data processing activities of our Contractual Compliance department in the course of enforcing ICANN org's agreements with gTLD registries and registrars. ICANN org has received questions from the community about whether these activities are in compliance with the GDPR. Recently, we sent a letter to the ICANN Registrars Stakeholder Group to provide information on this topic and thought this information also may also be of interest to you.

Purpose and Legal Basis for Contractual Compliance Processing Activities

ICANN Contractual Compliance requests registration data to investigate complaints and verify compliance on the legal ground of legitimate interests of ICANN org itself and the parties concerned (Art. 6 para. 1 (f) GDPR). ICANN org is currently working on publishing an overview of its data processing activities related to its contractual compliance function. This overview will set out in more detail the circumstances under which ICANN org requests access to registration data, the legal grounds for such access, and the safeguards implemented due to the direct applicability of the GDPR to ICANN org with respect to such processing.

Applicability of GDPR and International Transfers of Personal Data

The GDPR directly applies to ICANN Contractual Compliance processing activities. Depending on the role of the Brussels office of ICANN in the context of these activities, direct applicability of

the GDPR either follows from Art. 3 para. 1 GDPR or under the principle of extra-territorial application of the GDPR enshrined in Art. 3 para. 2 (a) GDPR, the “establishment” and the “targeting” criteria as outlined in the recently published draft guidelines by the European Data Protection Board.¹ In either case the GDPR applies to ICANN Contractual Compliance processing without regard to the location outside the EEA where the processing takes place.

Pursuant to Art. 44 GDPR transfer safeguards, such as Standard Contractual Clauses, are required only with regard to transfers to data recipients located in third countries (i.e. countries outside of the EEA), or in case of international organizations as the data recipients, where such importers are not subject to direct application of the GDPR. If data recipients in third countries are already in the direct scope of applicability of the GDPR, such transfer safeguards will not be required. If the GDPR directly applies, the level of data protection required under the GDPR is ensured.²

Because of the direct applicability of the GDPR to ICANN org, no transfer safeguards with registries or registrars are needed, including for any transfers of personal data in response to compliance requests handled by ICANN compliance team members in Los Angeles, Istanbul and Singapore or elsewhere in the world.³ This includes both, transfers from registries and registrars to ICANN and within the ICANN org. ICANN org will have to implement, however, appropriate technical and organizational measures pursuant to GDPR requirements (which are described below) in order to safeguard such data processing activities.

Safeguards for Data Processing Activities

ICANN org has undertaken various efforts to ensure ICANN org’s processing activities are in compliance with GDPR. An overview of ICANN org’s activities with respect to GDPR is available on ICANN’s website at <https://www.icann.org/news/blog/data-protection-privacy-update-icann-s-gdpr-efforts-with-temporary-specification-now-in-effect>.

Taking into account the direct applicability of the GDPR to ICANN org, ICANN org also maintains appropriate physical, procedural, administrative, organizational and technical security

¹ EDPB Draft Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation – adopted on 16 November 2018

² Art. 29 Working Party (WP) Working Document, Transfers of personal data to third countries, Applying Articles 25 and 26 of the EU data protection directive, 24 July, 1998, clarifies the reason for using contractual safeguards such as Standard Contractual Clauses for transfers of data outside of the EEA: “In the context of third country transfers, therefore, the contract is a means by which adequate safeguards can be provided by the data controller when transferring data outside of the Community (and thus outside the protection provided by the directive, and indeed by the general framework of Community law) to a third country where the general level of protection is not adequate. For a contractual provision to fulfill this function, it must satisfactorily compensate for the absence of a general level of adequate protection, by including the essential elements of protection which are missing in any given particular situation.” The Art. 29 WP makes a point that such contractual safeguards are only needed with regard to transfers outside of the EEA where the protection provided by the EU Data Protection Directive does not apply. As the principles for international data transfers have not changed under the GDPR, this rationale remains applicable.

³ Loïck Moerel, “GDPR conundrums: Data transfer” (<https://iapp.org/news/a/gdpr-conundrums-data-transfer/>) confirms this view for U.S. controllers within direct applicability of the GDPR: “If the original data processing by the U.S. controller is governed by the GDPR, the full scope of protection already applies to the controller []. Here, imposing additional requirements by the processor onto the original controller is not useful and the transfer rules therefore do not add any value. Also, the transfer rules should simply not apply.”

measures intended to prevent loss, misuse, unauthorized access, disclosure, or modification of personal data under our control, including the following measures:

- **Identification and Monitoring of users with access to personal data** – ICANN org has a system of access controls in place for users with access to personal data. This includes proper access controls and restricted access to personal data. Only authorized users may gain access to personal data on an “as-needed” basis.
- **Assessment of security controls** – ICANN org has a documented process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing in place. This involves manual assurance through audits, assurance reviews, penetration testing and red-team activities, as well as consolidated and integrated security products, so that fewer point products need to be managed and reported on.
- **Safeguards Requirement on Processors** – ICANN org has a documented process for imposing data processing requirements, in line with Art. 28 GDPR, on data processors who process personal data on behalf of ICANN.
- **Data Subject Rights** – ICANN org has a documented process for processing data subject rights requests with respect to any personal data from gTLD registrations it processes.

Data Retention

ICANN org recognizes that the retention of personal data related to the above activities must be compliant with Articles 5(e) and Article 17 of the GDPR, among other related obligations affecting retention of personal data. To address personal data deletion requirements under the GDPR, ICANN org has developed and implemented a data deletion program consisting of policies and procedures for the destruction of personal data relating to EU data subjects, including deletion upon a data subject's request under the GDPR.



We hope you find this information to be helpful in understanding ICANN Contractual Compliance's data processing activities. We are happy to provide additional information as needed on the steps ICANN org is taking to ensure its Contractual Compliance-related data processing activities are in compliance with the GDPR.

Best regards,

A handwritten signature in black ink, appearing to read "Göran Marby".

Göran Marby
President and Chief Executive Officer
Internet Corporation for Assigned Names and Numbers (ICANN)

cc. Dr. Andrea Jelinek, Chair
Rue Wiertz 60, B-1047 Brussels, Belgium
Email: edpb@edpb.europa.eu