6 December 2018

RE: Your Letter of 26 September 2018

Mr. Graeme Bunton
Chair, Registrar Stakeholder Group

Dear Graeme,

Thank you very much for your letter of 26 September 2018. We appreciate your willingness to work with ICANN as partners to resolve specific GDPR compliance related questions, and hope that these answers will help continue our dialogue on these important issues.

Question 1: (On what grounds does ICANN believe it can lawfully gain access to personal data entrusted by the registrants to their registrars?)

The legal basis for processing personal data by ICANN org, and for that matter the Contracted Parties, will depend on the personal data, and the nature and purpose of processing. The Registrar Stakeholder Group should specify the specific cases of access to registration data for which they would like to obtain further information on the applicable legal grounds.

ICANN org assumes that this question relates to registration personal data processing related to ICANN Contractual Compliance requests. 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 recently published an overview of its data processing activities related to its contractual compliance function for the Expedited Policy Development Process (EPDP) Team. This overview 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. Direct applicability of GDPR to ICANN org is discussed in more detail in the answer to Question 3 below.

Additional transfer mechanisms, such as the Standard Contractual Clauses, are not needed in order to safeguard the transfer of registration data from registrars in the European Economic Area to ICANN Contractual Compliance, as this type of activity is subject to direct applicability of the GDPR, as discussed in more detail in the answers to Question 3 below.

Question 2: (How does ICANN plan to provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the GDPR requirements and ensure the protection of the rights of the data subjects?)

ICANN org has undertaken various efforts to ensure that its 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 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 org.

- 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.

Question 3: (How does ICANN intend to ensure that processing of personal data that is subject to the GDPR will not be transferred outside the European Economic Area ("EEA")?)

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 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 (which means 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

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

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 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 registrars to ICANN org and within the ICANN org. ICANN org will have to implement, however, appropriate technical and organizational measures pursuant to GDPR requirements, as described in the answer to Question 2, in order to safeguard such data processing activities.

Question 4: (How is personal data protected by the GDPR that was collected by ICANN before May 25 being treated? For example, is personal data collected in the course of processing compliance complaints prior to May 25 or contained in compliance complaints that were received before May 25 still being retained by ICANN? If so, under what legal basis?)

As the GDPR has in principle not changed the meaning and scope of the legal basis of processing necessary for the purposes of legitimate interests pursued by the controller or by a third party which will usually apply to compliance related processing activities, ICANN org could continue to process personal data collected for such purposes prior to GDPR becoming applicable on 25 May 2018; assuming, of course, any other requirements of GDPR are met in this regard.

To ensure that ICANN org is implementing all appropriate safeguards including providing adequate information about its processing activities related to the WHOIS Accuracy Reporting System, ICANN org has ceased to process WHOIS data collected prior to 25 May 2018 through the WHOIS ARS.

Additionally, ICANN org recognizes that the retention of personal data related to its various processing activities, including the WHOIS ARS, must be compliant with Articles 5(e) and Article

[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 fulfil 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] Lokke 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."

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.

Question 5: (When will ICANN update the terms of service applicable to requestors of personal data?)

The Terms of Service (ToS) (https://www.icann.org/privacy/tos) govern the use of the ICANN website and are not the correct place for providing information about ICANN's compliance-related data processing activities. Such information would rather be provided in ICANN's privacy policy (https://www.icann.org/privacy/policy).

While ICANN's privacy policy refers to compliance audits as one of the purposes of processing, ICANN org has initiated a review to ensure that the policy includes the level of information about ICANN's compliance-related data processing activities as required under Art. 13 and 14 GDPR.

As a controller of the registrant personal data, however, registrars themselves are also responsible to inform individuals about the processing of their personal data, including for purposes of compliance (*see* Arts. 13 and 14 GDPR and section 3.7.7.4 of the Registrar Accreditation Agreement (RAA) <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#3.7.7.4> as modified by section 7.1 of the Temporary Specification for gTLD Registration Data <https://www.icann.org/resources/pages/gtld-registration-data-specs-en>.

We hope the above answers are helpful in understanding ICANN Contractual Compliance access to registration data and look forward to continuing our dialogue on how to ensure GDPR compliance of ICANN's compliance-related data processing activities.

Best regards,

Cyrus K. Namazi
Vice-President
Global Domains Division