

02 October 2020

Mr. Roberto Viola
Director General, DG Communications Networks, Content & Technology
European Commission

Ms. Monique Pariat
Director General, DG Migration and Home Affairs
European Commission

Ms. Salla Saastamoinen
Acting Director General, DG Justice and Consumers
European Commission

Dear Mr. Viola, Ms. Pariat, and Ms. Saastamoinen,

I am writing in follow-up to our exchanges about the ongoing reform of ICANN policies concerning registration data for generic top-level domains (gTLDs), in particular our exchanges relating to the development of a system for disclosure of non-public gTLD registration data to parties with legitimate interests, including in relation to the fight against cybercrime.

Since we last consulted with you on this topic, the ICANN community has completed its work on recommendations for a System for Standardized Access/Disclosure (SSAD) for non-public gTLD registration data. It has worked tirelessly to recommend a system for gTLD registration data access that will protect the privacy of registrants' personal data while also meeting the needs of its users in a manner that complies with the General Data Protection Regulation (GDPR). If approved for consideration by the ICANN Board, we anticipate the Board will vote on the recommendations in the coming months.

ICANN and the ICANN community have embarked on an effort to ensure the rights of data subjects are protected without sacrificing the critical efforts of other stakeholders, including public authorities worldwide and in the EU Member States. Public authorities, including the EU Member States, have persistently asked for "a stable, predictable, and workable method for accessing non-public WHOIS data for users with a legitimate interest or other legal basis as provided for in the GDPR, including law enforcement

authorities and other public enforcement authorities, including for cybersecurity purposes.”¹

The European Commission’s, particularly DG CONNECT’s, active participation in the ICANN community’s Expedited Policy Development Process (EPDP) and its support and facilitation of ICANN’s continued dialogue with the European Data Protection Authorities has greatly benefited the community’s work to date. I thank you for your commitment, and also request that you continue to aid this critical effort. We believe that your continued engagement and further dialogue with the Data Protection Authorities is necessary to obtain clarity surrounding the GDPR’s application in this space, to ensure that ICANN can implement a mechanism for access to non-public gTLD registration data that is predictable, transparent, accountable, protects the rights of data subjects, and also meets the needs of parties who have a legitimate interest in accessing gTLD registration data as advised by ICANN’s Governmental Advisory Committee, of which the European Commission and the EU Member States are a part².

In its [minority statement](#) on the SSAD recommendations, the Governmental Advisory Committee noted: “The currently fragmented system for disclosures combined with a relatively uncertain framework to consider and recommend future centralization, may impede the stability and predictability of the SSAD.” Should the ICANN Board approve the SSAD recommendations and direct ICANN org to implement it, the community has recommended that the SSAD should become more centralized in response to increased legal clarity.

Legal clarity could mean the difference between ICANN having a fragmented system that routes most requests for access to non-public registration data from requestors to thousands of individual registries and registrars for a decision, on the one hand, versus ultimately being able to implement a centralized, predictable solution in which decisions about whether or not to disclose non-public registration data in most or all cases could be made consistently, predictably, in a manner that is transparent and accountable to requestors and data subjects alike. We recall that the G7’s High Tech Crime Subgroup, in a [letter](#) to ICANN, emphasized the importance of a unified solution as “a necessity for public safety.”

The ICANN community develops policies for gTLDs within the boundaries of the law. The community policy development process cannot, nor should it be able to, define,

¹ <http://data.consilium.europa.eu/doc/document/ST-13443-2018-INIT/en/pdf>

² GAC Panama Communiqué, see Rationale of GAC Consensus Advice to ICANN Board (Section V.1, p. 7) and [GAC Minority Statement on the Final Report of Phase 2 of the EPDP on gTLD Registration Data](#)

interpret, or change applicable law. The recommendations developed by the ICANN community with respect to the SSAD are therefore greatly impacted by the legal uncertainty and lack of clarity that exists under the GDPR with respect to a number of issues. These issues that relate to the interpretation of the GDPR continue to be intensely debated by those seeking to understand the law’s application. It is widely recognized that further guidance is needed.

One such issue that would benefit from further clarification is the GDPR’s concept of controllership, including whether an entity acts as an independent or as a joint controller. In the ICANN context, an understanding of this issue is critical for the implementation of the SSAD in a uniform manner and its further evolution toward more centralization with regard to disclosing data.

The SSAD recommended by the ICANN community envisions that a central gateway (operated by ICANN org) would route accredited requests for disclosure to the appropriate registrar or registry, which would determine whether to grant or deny that request. When policy criteria for centralized disclosure are met (so-called “centralized decision-making”), the central gateway would forward the access request to the appropriate registry or registrar, with an instruction to disclose the requested data. Initially, the decision-making on most requests will not be centralized, but will be routed to the registry or registrar for evaluation and response.³ Over time centralized decision-making is expected to develop, including the further automation of functions, to ensure the uniform and efficient handling of requests.

Whether the SSAD can be further developed to enable greater centralization critically depends on whether legal clarity and certainty can be achieved with regard to the applicability of the GDPR’s controllership provisions. The decision whether or not to disclose will continue to remain with the registrars and registries as individual parties that weigh requests against their own standards, unless further clarity and certainty can be obtained about the impact centralized decision-making will have on the controllership for the processing activities in relation to the disclosure decision. It will be critical to determine whether the central gateway will be solely controlling in case of “centralized decision-making” and whether registries and registrars can be relieved from their controller roles in this regard.

³ At launch, it was recommended that only four “use cases” should be centralized: Requests from Law Enforcement in local or otherwise applicable jurisdictions with either a confirmed GDPR 6(1)e lawful basis or processing is to be carried out under a GDPR, Article 2 exemption; The investigation of an infringement of the data protection legislation allegedly committed by ICANN/Contracted Parties affecting the registrant; Request for city field only, to evaluate whether to pursue a claim or for statistical purposes; No personal data on registration record that has been previously disclosed by the Contracted Party. See EPDP Phase 2 Final Report, Section 9.4, at <https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf>.

I am grateful for your support to gain greater clarity regarding the application of the GDPR's controllership provisions in the context of a model for access to non-public registration data. ICANN's paper, "Exploring a Unified Access Model for gTLD Registration Data" (the "UAM Paper"), which you helped submit to the EDPB, was key to moving this conversation forward. The Belgian Data Protection Authority (DPA), which responded to the paper, acknowledged the potential benefits of a centralized model and explicitly recognized that the GDPR does not prohibit the automation of various functions in a disclosure model. However, the Belgian DPA did not provide definitive answers and cautioned that it is not in the position to give a definitive opinion on the question of controllership alone. We noted with great interest the Belgian Authority's representatives' encouragement to the European Commission representatives during the meeting set to discuss ICANN's UAM Paper and progress of the EPDP team's work⁴, to consider submitting these questions to the EDPB under article 64(2) of the GDPR which provides that, "*the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion.*" Given that, in addition, the newly published EDPB "Guidelines 07/2020 on the concepts of controller and processor in the GDPR" (the "Guidelines") do not contain more definitive guidance applicable to the special circumstances of the SSAD, we firmly believe that an outreach by the European Commission to the EDPB under article 64(2) of the GDPR would immensely help clarify the application of the GDPR controllership provisions on the matter at hand and in turn result in a more predictable and stable access/disclosure system.

As the Guidelines note in paragraph 70, "*there can be situations where various actors successively process the same personal data in a chain of operations, each of these actors having an independent purpose and independent means in their part of the chain. In the absence of joint participation in the determination of the purposes and means of the same processing operation or set of operations, joint controllership has to be excluded and the various actors must be regarded as successive independent controllers*". It will be critically important for the further development of the SSAD in a way that allows for centralized decision-making to understand if and to what extent the actors involved in the SSAD will be able to maintain their roles as successive independent controllers. A more specific allocation of controller roles taking into account that it is possible that independent controllers successively process the same personal data in a chain of operations would also allow for a determination that in case of centralized decision making, as described in the foregoing, the relevant registry or registrar is no longer responsible as a controller for the decision made by the central gateway whether to disclose the non-public gTLD registration data. Or, in other words,

⁴ <https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority>

that the central gateway will have to be regarded as the sole controller for the disclosure of this data.

Further guidance on the mechanisms available under the GDPR for international data transfers would also be beneficial for structuring the data transfers relevant for gTLD data processing in general and for the SSAD in particular. We note with interest the European Commission's [24 June 2020 report](#) on the application of the GDPR, in which the European Commission said that it will “provide standard contractual clauses both for international transfers and the controller/processor-relationship.”⁵

In light of the 16 July 2020 decision in *Schrems II*, there is a particular need for updated EU Standard Contractual Clauses to address the risks identified by the Court of Justice of the European Union (CJEU) with respect to access by public authorities to the data transferred. In context of the *Schrems II decision*, it would also be useful if the European Commission could align with the European Data Protection Board so that the Board would issue further guidance on how the adequacy assessment required by *Schrems II* for international transfers shall be conducted as well as the supplementary measures that data exporters and data importers might have to implement, if the result of the adequacy assessment is that the country of the data importer does not provide an essentially equivalent level of protection. It would also be helpful if the Board would detail its guidance on derogations under Art. 49 GDPR for specific transfer situations, including reconsidering whether its narrow interpretation of these derogations should be upheld taking into account the more relevant role that these derogations will have to play for international data transfers in the future.

This information is critical for many entities who need to transfer data across borders, including within the ICANN ecosystem. In particular, the SSAD critically depends on whether certainty can be achieved with respect to the transfer mechanisms available for transfers of registration data within the SSAD (in particular from a registrar or registry to ICANN org as the contemplated central gateway under the SSAD) and outside of the SSAD to non-EEA third parties requesting access to registration data subject to the GDPR transfer restrictions. This information affects the ICANN community's ability to develop more streamlined solutions for the disclosure of non-public registration data within the SSAD. As emphasized in the foregoing, a more streamlined access solution would benefit both third parties seeking access to non-public gTLD registration data, including law enforcement authorities and intellectual property holders, and data subjects through increased transparency and predictability.

⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN>, page 16

A further issue that would benefit from greater clarity is the GDPR's principle of data accuracy. The data accuracy principle has been widely understood as a general obligation of the data controller to take reasonable steps to ensure the factual correctness of personal data. The right of data subjects to request from the data controller the rectification or erasure of inaccurate personal data concerning them supplements this obligation. However, there is a level of uncertainty surrounding potential liability related to the inaccuracy of personal data that is being processed.

The GAC's minority statement on the SSAD recommendations noted that the accuracy of registration data is an essential requirement of the GDPR, and that "[d]isclosure of inaccurate data would defeat the purpose of the SSAD and risk violating data protection rules." Thus, there could be a risk that a requestor of non-public registration data, such as a law enforcement authority, could even lodge a complaint with a Data Protection Authority against a data controller.

In the ICANN context, the potential impact of this liability on the evolution of registration data access cannot be ignored. For example, in the SSAD context, it is unclear whether non-compliance with the data accuracy obligation will result in liability only vis-à-vis data subjects, or even toward third parties relying on the accuracy of the data disclosed (such as requestors for non-public registration data).

It would therefore be very useful if the European Commission could clarify - or if it could align with the European Data Protection Board, and if the latter could further clarify - whether it believes that the GDPR creates a potential liability for contracted parties to third parties with respect to the accuracy of gTLD registration data disclosed in response to an access request.

ICANN will continue to take all available measures within its remit to maintain globally uniformly accessible registration data recognizing the public interest served by access to domain name registration data for third parties with legitimate purposes and continues to remain willing to assume greater responsibility with respect to disclosure of registration data to help serve the public interest if the liability impacts of this are clear under the applicable law, including the GDPR. We appreciate the support and partnership from the European Commission and we thank you in advance for your willingness to provide further context with respect to the issues raised in the foregoing and any other initiative the European Commission is expected to work on going forward that might be relevant to the ongoing work within ICANN.

We look forward to continuing to work with you, the ICANN community, the Data Protection Authorities, and interested stakeholders to obtain greater legal clarity and

certainty with respect to the application of the GDPR, in particular on the aforementioned issues, recognizing that such clarity and certainty will have a critical impact on the evolution of registration data access (including the development and implementation of the SSAD) and keeping in mind that the domain name system is a global public resource that must serve the needs of all its users, including consumers, businesses, registrants, and governments.

Regards,



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