

6 August 2019

RE: 21 June 2019 letter from Mr. Green to Mr. Chalaby

Richard D. Green
Chair, G7 High Tech Crime Subgroup

Dear Mr. Green,

Thank you for your [letter of 21 June 2019](#). We note your concern regarding access to non-public gTLD registration data for public security concerns. ICANN made changes to the publicly available data in the Registration Directory Services, commonly known as WHOIS, in response to the European Union's adoption of the General Data Protection Regulation (GDPR). Several countries around the world are also looking to enact similar legislation. To ensure compliance with the GDPR and possible other future laws, as well as to ensure consistency in the provision of registration data, ICANN is developing a possible Unified Access Model (UAM) for third parties with legitimate purposes to access non-public registration data.

As you may be aware, ICANN recently commissioned a [Technical Study Group for Access to Non-Public Registration Data](#) to explore technical solutions for authenticating, authorizing and providing access to the non-public data for third parties with legitimate interests. The resulting model, [TSG01: Technical Model for Access to Non-Public Registration Data](#), is the basis for the possible UAM we are exploring. This model will serve as an input to Phase 2 of the ICANN community's Expedited Policy Development Process (EPDP), which is focused on a standardized system for access/disclosure in addition to other topics related to registration data policy. Our goal with this work is to provide the EPDP with a legal framework for how such a model may be built. It is up to the EPDP to determine whether and how to make policy recommendations as they relate to any model.

ICANN is exploring this approach in response to [calls from governments](#), as well as from the ICANN community, to determine whether it is workable under the European Union's General Data Protection Regulation. ICANN will seek advice from the European Data Protection Board (EDPB) on whether the model is aligned with the law and previous statements from data protection authorities. For example, the Article 29 Working Party said in a [statement to ICANN in 2018](#), which the EDPB subsequently endorsed, that the WP29 expected "ICANN to develop and implement a model that 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."

In addition, the EDPB also commented on these topics in its [5 July 2018 letter](#) to ICANN org and has encouraged ICANN to move ahead in the development of an access model: "ICANN and the registrars/registries are, as controllers, responsible for ensuring that personal data processed in the context of WHOIS are only disclosed to third parties with a legitimate interest or other lawful basis under the GDPR, also taking into account the other requirements of the GDPR. This implies putting in place an appropriate access model, with appropriate safeguards,

including measures to ensure a sufficient degree of compliance assurance. The responsibility for designing a model that will provide this assurance is in the first instance up to ICANN and the registrars/registries.”

Thank you again for your input on these efforts. Updates on our efforts can be found on this [page](#).

Sincerely,



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