

## **RySG & RrSG Comment on the August 20, 2018 “Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data – For Discussion”**

The Registries Stakeholder Group and Registrar Stakeholder Group (RySG and RrSG, respectively; hereafter the Contracted Parties) have reviewed the August 20, 2018 “Draft Framework for a Possible Unified Access Model for Continued Access to Full WHOIS Data – For Discussion” (the “**Draft Framework**”), and submit the following brief and initial comments. These comments are offered assuming a legally appropriate and acceptable avenue forward for third party access is determined. As the Draft Framework continues to develop, we will likewise provide additional inputs and/or concerns as well.

1. Allocating Liability/Risk. The Draft Framework anticipates ‘Eligible User Groups’ will determine which individuals may be given access to data (under certain ‘Terms of Use’). In other words, access to 3<sup>rd</sup> parties would be determined/granted by a 3<sup>rd</sup> party, yet Contracted Parties, which are and remain ultimately liable for the processing/handling of the data, have limited oversight and control. We will not support any scenario under which we would be required to absorb the full weight of legal and financial liability (claims, damages, actions or regulatory/administrative inquiry) arising from a user’s access to or use of nonpublic WHOIS data. Authenticating Bodies must bear responsibility for granting access to and use of data by individuals that they authenticate, and must be capable of bearing the financial impact of any such liability. Ultimately, we believe proper allocation of liability/risk can be largely accomplished by way of a thoughtfully drafted set of terms of access/use. Given the direct impact these terms will have on the Contracted Parties, we anticipate and expect to be allowed to provide substantial input to this end, and we look forward to working with ICANN in this regard.

2. The Devil is in the Details. Any framework for access (a term undefined and used inconsistently throughout the UAM) must also include careful consideration and meaningful discussion of at least scope of access and technical implementations/flows. For example, there is a vast difference between (1) storing data and issuing credentials from a single central location, and (2) storing data and issuing credentials at each source (every registry and registrar). These considerations do not exist in a vacuum. Though we assume some middle ground will be defined, until that occurs, it is nearly impossible for legal and contractual nuances to be ironed out, let alone the technical challenges we will face.

Similarly, though it is presumed that the Draft Framework will be binding upon Registries and Registrars, it is not clear what the intended mechanism will be to accomplish this (e.g., through the ePDP, a new PDP, or proposed contractual amendment). It is important that ICANN clearly articulate the process by which it intends to make the eventual UAM binding upon Contracted Parties.

3. EDPB Efforts. It is unclear from the Draft Framework text what questions ICANN org is specifically posing to the EDPB. The Draft Framework mentions further discussion and consideration is required on a number of points, but does not seek explicit feedback on those questions. Is ICANN org seeking the EDPB’s opinions on those open issues? Some clarity on what type and form of response ICANN org is hoping to receive would be helpful. As a starting

point, we believe ICANN org needs to seek guidance on the fundamental question of whether entire groups of 'Eligible Users' can lawfully access personal data based on a uniform legitimate interest. The Draft Framework takes this concept as a given. However, it also assumes that all Eligible Users would have "global access" to registration data, which would seemingly make it very difficult to ensure that users, in all instances, do in fact access and use the data in accordance with that interest, and not in a manner that may violate the data subjects' rights under the GDPR.