17 April 2019

Registrar Stakeholder Group's (RrSG) response to the GNSO Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Policy Recommendations for ICANN Board Consideration

The Registrar Stakeholder Group (RrSG) thanks the EPDP Team and supporting ICANN staff for the immense amount of time and effort involved in producing the Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process.

The RrSG generally supports the recommendations contained in the Final Report, but believes it necessary to highlight the following:

WHOIS Data

The RrSG commends the EPDP Team's efforts to move away from "thick" WHOIS, and instead provide a minimum public data set of registration data, and without geographic discrimination (unless a registrar or registry operator opts to differentiate).

The lawfulness of public "thick" WHOIS data mandated under our contracts with ICANN has long been debated without resolution. The Final Report is evidence that, through compromise, a fair and balanced approach to providing registrant data is possible.

It is important to note that several recommendations (EPDP Team Recommendations 6, 12, 13, 14 and 16) put registrars in an authoritative position when it comes to WHOIS data because registries cannot execute these recommendations within their platforms. If registrars are not authoritative, these recommendations cannot be implemented; thus, thick WHOIS is no longer necessary to achieve the documented and agreed-upon purposes for processing personal data.

Phase 2 Issues:

The RrSG welcomes and supports the continued work of the EPDP Phase 2 at a realistic pace, given the complexity of the issues and natural limits to volunteer participation, to determine the criteria and subsequent handling of lawful and legitimate disclosures of

personal data. However, we raise concerns with the following issues which were carried over from Phase 1 to Phase 2 for deliberation:

Legal v. Natural

Natural persons can also be legal persons, and being a legal person does not mean there is no right to privacy; this is not absolute and indeed not black and white.

Although legal persons are not protected under the GDPR, the data provided by a legal person can easily contain or reveal that of a natural person, such as someone working for an organization, which should be protected. And other privacy laws and regulations may treat this topic differently, extending privacy rights to legal persons.

Furthermore, the RrSG is concerned about the feasibility of requiring differentiation between legal and natural persons for the over 150 million legacy registered domain names. Any policy discussion and recommendation need to ensure that the risks for legacy registered name holders are accounted for.

City Field

The registrant City field, while typically not containing personal data itself, can in many cases be used to identify a specific data subject. Thus, this field is considered "identifiable data" under the GDPR and other data privacy regulations. Additionally, publication of the City field brings no additional value to a third party looking at the public data to determine the registrant's jurisdiction or applicability of a specific law, as this can be known from the State/Province and Country fields, which will be publicly available. Since the City field can contain identifiable data and there is no legitimate reason to publish it, it should be afforded full protection as any other piece of personal data would be.

Geographic Differentiation based on geographic location is a flawed concept and should be set aside without further consideration given to how it may be achieved.

The registrar only has the registrant contact data to rely on when determining the presumed location of the data subject, but this does not indeed indicate if there are data privacy laws to be followed, as the data subject may list a country on the domain which is different from where they live or the laws they are protected under. The registrar may be located in a place where the GDPR or another similar data privacy law is in force, so it may need to provide uniform data protection to all the personal data it controls or processes.

Defining the Role of ICANN

As noted on many occasions in Phase 1, the success of Phase 2 and viability of any uniform access/disclosure model is predicated on a clearly-defined role for ICANN Org. Registrars, as contracted parties, must be able to manage the legal and regulatory uncertainties associated with responding to requests for non-public data that have been relayed by ICANN. We look forward to the active participation of ICANN Org in Phase 2 of the ePDP's work.

Finally, as the Board is well aware, all the elements of this Final Report are dependant on each other, and one cannot remove or change one aspect without risking the entire thing falling apart. One change in a definition might have unforeseen consequences for other recommendations (this has been observed many times in several past IRTs). As such, we recommend adopting the Final Report in its entirety.

Sincerely,

Graeme Bunton
Chair, Registrar Stakeholder Group