22 October 2018

Cherine Chalaby, Chairman of the Board
Göran Marby, President and CEO
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536, USA

Dear Cherine and Göran:

We understand, from various blog postings, webinars, and public meetings, that ICANN has begun to explore whether, by playing a more direct role in providing access to redacted domain name registration data to third parties, it could reduce potential Contracted Party (CP) liability under data protection laws including the General Data Protection Regulation (GDPR). Specifically, we understand that ICANN is exploring (among other things) the extent to which a system with the following high-level characteristics might comply with applicable law and effectively make ICANN the sole data controller (or otherwise effectively accept legal responsibility) for the provision of access to personal data contained in domain name registration data by parties with a legitimate and proportionate interest for such access:

1. ICANN would adopt a policy (e.g., in the form of a Code of Conduct or Binding Corporate Rules) developed through ICANN multistakeholder processes such as the ongoing ePDP (following completion of the Gating Questions in the ePDP Charter), governing (a) who would have access to personal data in WHOIS records; (b) the purposes for which such access would be permitted; (c) jurisdictional concerns/controls; and (d) the safeguards applicable to such access.
2. ICANN would verify and credential prospective registration data users with legitimate and proportionate interests in registration data consistent with the qualifications, requirements, and safeguards of the policy/code/rules.
3. ICANN would maintain a central registration data access request portal for receipt of data requests from credentialed users.
4. Upon receipt of a properly verified access request, ICANN would arrange for responsive data to be made available to the relevant third party for specified uses consistent with applicable data protection laws, including GDPR, and the policy/code/rules, through a mechanism to be determined.

We agree that the provision of third-party access to information about registered names and nameservers, consistent with applicable law and the ICANN Mission, is an ICANN objective, and we agree that establishing ICANN as the sole data controller for a centralized access portal operating under community-developed and GDPR compliant policies might result in a more predictable and uniform experience for those with legitimate and proportionate interests in use of registration data. Although, as discussed below, more information is needed to evaluate this concept fully, we believe it is worth exploring. We also believe that it is possible for ICANN to conduct such exploration in parallel with the ongoing ePDP, and without usurping the community's policy development authority.

At present, each individual registry and registrar must apply GDPR's balancing test on a case by case basis, taking relevant local data protection guidance (which may or may not be directly on point) and its own circumstances into account. The results are inevitably inconsistent, based on differences in judgment, location, and risk tolerance. Absent detailed and proscriptive guidance from the European Data Protection Board (EDPB), which does not appear to be forthcoming, such inconsistency is to be expected where data protection principles must be applied in a complex, global joint-controller environment.

It goes without saying that much more detail is required to understand whether and how a system in which ICANN could serve as the sole data controller for third party access would work consistent with GDPR and other data protection laws. Among other things, this is dependent upon the substance of the policy/code/rules governing such access, elements of which are under discussion in the ePDP. Further work must also be done to identify potential mechanisms for receiving and processing data access queries and responses including, in particular, where the underlying data used for this purpose is retained, how it is distributed, etc. Contractual changes may or may not be needed to ensure the effectiveness of this approach. Nonetheless, exploring the legal viability of variations on a "hub and spoke" approach for third party access subject to the GDPR and community developed policy makes sense at this time. It would be extremely useful to know whether and under what circumstances a system like this could have the legal effect of establishing ICANN as the sole data controller for access through a centralized system and effectively shifting potential liability with respect to that activity from Contracted Parties to ICANN. In closing, we also call on ICANN to issue a more detailed explanation and analysis of the approach being contemplated, which we believe is essential to enable meaningful dialogue with data protection authorities in order to understand its legal viability.

Sincerely,

Graeme Bunton, on behalf of the Registrars Stakeholder Group

Paul Diaz, on behalf of the Registry Stakeholder Group