From: "Taylor, David"
Date: Wednesday, January 10, 2018 at 18:49
To: "gdpr@icann.org" <gdpr@icann.org>
Subject: [Ext] Hogan Lovells comments on the 3rd Hamilton Memorandum re GDPR

Dear Goran

Further to your request in your blog for comments / feedback and suggestions about the layered access approach described in Part 3 of the Hamilton legal analysis please see below some specific comments on that from Hogan Lovells.

Hogan Lovells is one of the leading privacy and cybersecurity law firms in the world, we are involved in an ever-expanding array of matters at the cutting edge of legal, policy, and technical work. In 2015, we won the first ever Chambers Privacy and Data Security Team of the Year award. In 2017, we were awarded this honor once again. We counsel tech-sector titans in Silicon Valley and major financial services corporations in New York. The auto industry turned to us to help them develop "connected car privacy principles." We recently handled one of the largest retail data breaches. One of the largest health insurer data breaches. And one of the largest hospital data breaches — all within a few months of one another. We are also heavily involved in the Internet and Domain Names.

Our Global Domain Name and Internet Governance Practice has advised clients in this area for 20 years offering a unique, comprehensive and centralized online brand protection service called Anchovy. Hogan Lovells also specializes in all aspects of the ICANN new generic Top Level Domain (gTLD) process. We have been involved in the ICANN process for many years (since the fourth ICANN Meeting in Los Angeles, 1999), and as an example provided comments on every version of the new gTLD Applicant Guide Book. Hogan Lovells is also an accredited ICANN registrar. So we understand domain names.

With regard to the 3rd Hamilton memo* we have the following specific comments:

2.7.10

Quote: "*In light of the above reasoning, our opinion is that it will not be practically feasible to fulfill the purposes listed under this section 2.7 through a layered access model, as such a model would require the registrars to perform an assessment of interests in accordance with Article 6.1(f) GDPR on an individual case-by-case basis each time a request for access is made.*"

Comment: If the layered access model is based on the "automatically qualified parties" having adhered to a Code of Conduct, or binding policy, such model could be feasible. The GDPR does not require an assessment on an "individual case-by-case basis", since the "purpose of specifying the application" of the GDPR with regard to the "legitimate interests pursued by controllers in specific contexts" is explicitly listed as an example for the content of a Code of Conduct (Art. 40(2)(b) GDPR).

2.7.4
Quote: "*our assessment is that access to the e-mail addresses of registrants which are natural persons is not necessary for the purposes listed in 2.7.1(i) - (v) above and that such e-mail addresses therefore should not be made publicly available through the Whois services*"

Comment: The basis for such assessment is not clear. One missing element for instance is what the data subject "can reasonably expect" (recital 47 GDPR), and whether the WHOIS practice during the last decades influences such expectation. We also miss an analysis of the current use of email addresses for the discussed WHOIS access purposes (eg. IP infringements, business owner identification). We do not see how an email address, in particular one that is chosen by random or used only for this specific purpose, raises more privacy concerns than a name or a postal address.

2.1.1
Quote: "*we concluded that consent is not a practically viable legal ground for processing personal data*"

Comment: This might be true if consent were taken as the ONLY legal ground, but not if consent is one of several options, and freely given. Updating the consent procedures could make consent a viable option for ICANN here.

3.4.2.
Quote: *"Where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller shall consult the applicable DPA."*

Comment: Whereas this accurately reflects Article 36(1) GDPR, it is a risky approach to undertake a DPIA, and to come to the conclusion that there is an "absence of measures ... to mitigate the risk". The DPIA should preferably come to the conclusion that the WHOIS procedure provides for sufficient measures to mitigate all risks. As a consequence, a DPA can still be asked for informal comments on the DPIA, but not in the framework of the regulated prior consultation in accordance with Article 36(1) GDPR.

* https://www.icann.org/en/system/files/files/gdpr-memorandum-part3-21dec17-en.pdf[icann.org]

Respectfully submitted

Stefan Schuppert, Partner Hogan Lovells
David Taylor, Partner Hogan Lovells