**Revised/Consolidated Questions #2,3 and 4 (BB Proposed Rewrite v.2)**

Paragraphs 17 through 25 of Bird & Bird’s memo data January 25, 2019 discussed the potential risks to Registrars associated with reliance on a Registrant’s (i) self-designation as a legal person and (ii) confirmation that the registration data does not contain personal data.  The memo identified a variety of steps that Registrars could take to mitigate the risk of inadvertent publication of personal data.

For example, the memo suggested Registrars might take certain steps to improve the accuracy of self-designation/attestation such as: providing separate, clear disclosures, including descriptions of the consequences of self-designation as a legal person and asking the registrants to confirm that they are not submitting personal data; testing the clarity/readability of such disclosures; periodic follow up emails to registrants and/or technical contact; and providing a mechanism to change self-designation, or correct or object to publication of personal data.

1.     Assuming that a Registrar takes the mitigation steps identified by Bird & Bird, and based on your experience and applicable precedent, please describe the level of risk, likelihood of enforcement actions, fines, counseling, etc. flowing from subsequent inadvertent publication of personal data contained in the Registration data of a legal person.

2.     Expanding on Question 1, please discuss what level of risks (e.g., enforcement actions, fines, counseling, etc.) a Contracted Party faces with respect to publication of personal data if a confirmation email sent by a Registrar to the Registrant and/or the Registrant’s tech contacts (i) clearly states that the Registrant has self-designated as a legal person and has affirmatively stated that no personal data has been included in its registration data; (ii) explains that based on those two representations all fields in the registration data will be published on the Internet; and (iii) provides an easy-to-use mechanism through which the self-designation can be rescinded and an individual receiving the email can object to publication of their personal data and/or rectify any inaccurate date? Must the Registrar require the registrant’s and/or tech contact’s affirmative response to the confirmation email?  Does the answer differ depending on the medium of the notification (e.g., snail mail v. email)?

3.     Are there additional or alternative mitigation and/or verification steps that a Contracted Party could take to further reduce/eliminate liability associated with inadvertent publication of personal data in connection with reliance on a registrant’s self-designation, e.g. confirming the existence of corporate identifiers (Inc., GmbH, Ltd. Etc.), reviewing account holder data for indicia of legal personhood, etc.? To what degree would each such additional step reduce liability?

4. Would you change or add anything else on your analysis under points 1, 2 and 3 if an additional step is introduced after distinguishing between natural and legal persons, as described in the 2-step approach below? In particular, could you please assess the level of risk (if any) of such approach:

a. Step one, allow self-identification of registrant as either natural and legal person. If natural, then full redaction of data remains in place, if legal go to step 2.

b. Enable registrant to further confirm that its provided data contains only non-personal information.

Step 2, Further distinguishing between data of legal persons which contain personal information and data which contain non-personal information. Publish only non-personal information.

.

Please advise on potential further steps that could be taken on how to safely implement such an approach to minimize liability for wrongful disclosure (if different than the steps described above).

QUESTION # (**Proposed rewrite of Q5 and Q6 (EURid/RIPE-NCC) (BB Proposed Rewrite v.2):**

Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (‘.eu Regulation’) sets out the public policy rules concerning the implementation and functions of the .eu Top Level Domain (TLD) and public policy principles on registration of domain names in the .eu TLD.

Article 16 of the .eu Regulation is entitled ‘Whois database’ and provides:

*‘The purpose of the WHOIS database shall be to provide reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names under the .eu TLD.*

*The WHOIS database shall contain information about the holder of a domain name that is relevant and not excessive in relation to the purpose of the database. In as far as the information is not strictly necessary in relation to the purpose of the database, and if the domain name holder is a natural person, the information that is to be made publicly available shall be subject to the unambiguous consent of the domain name holder. The deliberate submission of inaccurate information, shall constitute grounds for considering the domain name registration to have been in breach of the terms of registration.’*

As from 13 October 2022, the .eu Regulation will be repealed by Regulation 2019/517, which provides under Article 12, entitled WHOIS database:

‘*1. The Registry shall set up and manage, with due diligence, a WHOIS database facility for the purpose of ensuring the security, stability and resilience of the .eu TLD by providing accurate and up-to-date registration information about the domain names under the .eu TLD.*

*2. The WHOIS database shall contain relevant information about the points of contact administering the domain names under the .eu TLD and the holders of the domain names. The information on the WHOIS database shall not be excessive in relation to the purpose of the database. The Registry shall comply with Regulation (EU) 2016/679 of the European Parliament and of the Council.*’

The Whois database is currently administered by EURid, a non-profit designated by the European Commission to manage the .eu registry. In its Whois database, EURid publishes the email addresses of domain name registrants in the .eu TLD (both natural persons and legal entities). EURid distinguishes between natural persons and legal entities by publishing the postal address information of legal entities, whereas this information is not published for natural persons.

Through Article 16 of the .eu Regulation, EURid is able to rely on GDPR Article 6(1)(e), which provides a legal basis for processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. While we understand that this Article 16 public interest basis is not available outside the .eu domain, the existence of this lawful basis for EURid’s processing could be interpreted to suggest that the EU legislature recognized that disclosure of the Registrant data serves a legitimate interest in stability, security, and resilience. Further, in carrying out its mandate under Article 16, EURid has determined that publication of the Registrant’s email “is not excessive in relation to the purpose of the database.”

Similarly, while RIPE-NCC relies on consent to publish personal information about tech/admin contacts, it publishes personal information about resource holders on the grounds that “facilitating coordination between network operators is the one purpose that justifies the publication of personal data in the RIPE-NCC database and that it is clear that the processing of the personal data referring to a resource holder is necessary for the performance of the registry function, which is carried out in the legitimate interest of the RIPE community and the smooth operation of the Internet globally (and is therefore in accordance with article 6.1.f of the GDPR).”

We understand that the public interest basis supplied by Article 16 is not available to Contracted Parties outside of the .eu top level domain. Based on your experience and applicable precedent to what extent if any do:(i) the existence of Article 16 of the EU Regulation; (ii) EURid’s decision to publish Registrant email addresses consistent with Article 16, (iii)RIPE-NCC’s decision to publish the email addresses of resource holders; and (iv) draft language regarding access to registration data in the recently proposed NIS2 Directive create precedent that would reduce Contracted Party risk in connection with publication of a legal person Registrant’s email address, even if it contained personal information? Do these facts affect your answers to Questions 1-3 above? If it does not affect your answers, please explain why.