February 27, 2018

By Electronic-Mail

Akram Atallah
President, Global Domains Division
Internet Corporation for Assigned Names and Numbers

John Jeffrey
General Counsel and Secretary
Internet Corporation for Assigned Names and Numbers

Re: GDPR Discussion Group Additional Feedback on ICANN's "Cookbook"

Dear Akram and John:

We appreciate the recent efforts of ICANN staff to engage with the community to share ICANN's vision of a potential interim GDPR compliance model (the "Model"). As requested by ICANN during its 26 February call with representatives of the GDPR Discussion Group, our feedback is provided below. This feedback is based on the Model as it has been presented to us, and is provided with the expectation it will be carefully assessed and considered by ICANN as it continues its ongoing discussions and further refines the Model. Of course, as such refinement progresses, and conversations progress, there may be other areas for further adjustment.

During our February 26th call, we reiterated our support for high-level decision points that ICANN described as being contained in the Model. In particular, we support the following elements of the Model that ICANN has articulated:

(1) short of DPA approval, contracted parties are not required to publish email addresses as part of a publicly available minimum WHOIS data set;

(2) neither the registrant name, nor the registrant street or zip-code, shall be available via public WHOIS;

(3) contracted parties are not required to publish different sets of WHOIS data based upon a self-identified distinction (by the registrant) between natural and legal persons; and

(4) contracted parties may apply the Model globally, as opposed to segmenting the WHOIS based upon where a registrant self-identifies as being located.

Though we have yet to see the full text of the Model, the inclusion of these fundamental elements represents a positive and constructive step towards an implementable model, and we are appreciative of the collaboration efforts it represents. Nonetheless, we are concerned that there remain many unanswered questions. We hope ICANN will take these concerns into account - and specifically address each - prior to publishing its final version of the Model.

1. Legal Basis for Every Processing Activity and Every Data Element

ICANN's proposed Model contemplates that all WHOIS personal data currently collected and processed by registrars be transferred to, and subsequently processed by, the registry, two sets of escrow agents, and (in the case of failure) ICANN/the EBERO provider. As recently suggested by the European Commission, and as was previously highlighted by Hamilton in its memos, any compliance model must necessarily examine with specificity how each individual processing activity by every data processor/controller in the ecosystem is necessary to achieve the identified purpose and on what legal basis such processing activity occurs.

We urge ICANN to ensure that its Model explain how the collection, transfer and processing of all data elements by both registries and registrars as currently required by ICANN's contracts and policies is envisioned to be compatible with the principles of purpose limitation and data minimization, and on what legal basis each processing activity occurs. In this regard, we note that ICANN, the GAC and the European Commission have highlighted that providing access to (an appropriate amount of) WHOIS data serves the public interest. If "processing necessary for the performance of a task carried out in the public interest" pursuant to Art. 6(1) (e) of the GDPR is set forth as a legal basis supporting the interim GDPR compliance model, we urge ICANN to explain in detail how the public interest legal basis supports each identified processing activity for each data element by each data processor/controller.

2. Collection of Data

We request that ICANN continue to consider the necessity of requiring the collection of Admin-C, Tech-C and Billing-C data for all registrations. In practical terms, registrars do not use WHOIS data to determine whom to invoice. Rather, they set up accounts, invoice, and otherwise communicate with the account holder (and not admin, tech or billing-C). Further, research by market leaders has shown that in more than 90% of cases, the data of the aforementioned contacts is identical to the registrant data. Hence, there is little to no additional intelligence to be found in those data elements. We ask that ICANN consider the possibility of making the requirement to collect Admin-C, Tech-C and Billing-C data optional for registrars, rather than uniformly required based on the principle of data minimization. As an example, we ask that ICANN note that a representative of the .DE ccTLD registry, DENIC, recently announced publicly at the DomainPulse conference in Munich that DENIC will no longer collect Admin-C, Tech-C and Zone-C data.

Given that the GDPR requires data subjects to be informed about how their data is processed, contracted parties have concerns about the ability to provide such information to contacts other than the registrant, who might not be part of the contractual relationship with the registrar. As a consequence, obtaining data of third-party Admin-C, Tech-C or Billing-C bears additional compliance risks. In the alternative, we request that ICANN specifically identify the legitimate interest(s) served by the continued collection of these three contacts as requested in #1 above.

3. Retention Requirements

We understand that the proposed Model may have a data retention period the life of the domain registration plus two years. We would like to clarify whether this data retention requirement applies only to registrars, as it does today, or whether ICANN envisions extending a date retention requirement to registries, as well. We are concerned that instituting a data retention requirement for registries would create a new, rather than modify an existing, contractual obligation for registries. We also remained concerned about the sufficiency of any legal justification for such a retention period, and request that ICANN clearly and explicitly set forth the basis for whatever time period requirement is advanced.

4. Publication of Data

We understand that ICANN has not yet decided upon a minimum public data set for the Model. As discussed on the 26 February call, we do not see how publication of a registrant's email address and certain granular details of the registrant address (e.g., zip code, city) comply with the principles of the GDPR.

ICANN has, however, proposed requirements to display an anonymized email address or web contact form in lieu of a registrant or other contact's email address in public WHOIS records. Has ICANN developed any implementation guidelines for contracted parties to review around how to achieve this? This type of undertaking is a complicated task that should be fully discussed and fleshed out before being presented as part of a final solution.

5. Layered Access for Layered Access

ICANN has stated that its intention is to create a "layered" or "tiered" access model for accredited parties to be able to access WHOIS data that is not displayed in public records. The GAC and the European Commission have highlighted the importance of taking into consideration the practical needs for law enforcement authorities' investigations, particularly with respect to high volumes of requests.

We note, however, that while the European Commission has stressed that access to personal data shall be granted subject to applicable national law, the GAC has stated that the denial of access to personal data must not be made based on the origin of the request / requestor. How does ICANN plan to assist the contracted parties in navigating the complicated issue of determining how and whether to disclose EU registrant data via a layered access model in a manner compliant with the GDPR where the requestor is not based in the EU? Will the proposed Model attempt to reconcile these divergent positions?

These jurisdictional matters will be critical to consider when developing an accreditation or credentialing system to support layered access and the contracted parties remain willing to collaborate with ICANN to help sort out these complex questions. We see the GAC and the EC as having a critical role to play since they have articulated requests for an as accessible as possible WHOIS and should therefore be engaged by ICANN with all due haste.

6. Self-Certification

Noting that a layered access model based on accreditation or credentialing will be impossible to create prior to the 25 May 2018 GDPR enforcement deadline, it has been suggested that a self-certification system of accessing non-public registration data could be an option in the short term. We hope ICANN shares our view that self-certification, even as an interim solution, raises a number of serious questions and concerns, including:

- Who will develop and provide a set of uniform requirements, processes and terms for such self-certification that can be utilized by all registries and registrars - if not ICANN, is it expected that contracted parties would develop their own requirements, processes and terms, or adhere to a uniform system? We encourage ICANN to work with the contracted parties to develop these requirements and processes.

- Would ICANN require registries and registrars to verify the information provided by requestors in their self-certifications?

    - If not, how would ICANN envision allocating the risk associated with the potential disclosure of millions of personal data records based on "false" self-certifications?
    - If so, how would ICANN envision such verifications be conducted in a uniform manner without imposing significant costs on contracted parties (particularly when conducting the verifications will necessarily require additional international transfer/processing of personal data)?

- Would ICANN envision that the processing of certification requests be manual - given that some registries and registrars currently process a huge number of WHOIS queries per day, how would contracted parties be expected to handle such a volume of requests?

- Would ICANN require some form of uniform service-level agreement when it comes to responding to self-certification requests?

    - If so, how would the SLAs address the disparate impact that a self-certification mechanism places on larger v. smaller registries and registrars?
    - If not, how would ICANN address non-compliance (e.g., unreasonable delay or inaction on self-certification requests)?

- Would the self-certification mechanism require certification on a request-by-request basis to provide access to only the thick WHOIS information responsive to the specific legitimate interest pursued by the certifier, or would a single self-certification provide access to the entire Thick WHOIS database maintained by the registry/registrar?

    - If the former (access to only those Thick WHOIS records responsive to the proffered legitimate interest) by what mechanism would a registry/registrar determine which records are responsive and in compliance with the purpose limitation/data minimization principles?

- If the latter (access to the entire database) how would this "universal access" be seen to comply with the purpose limitation and data minimization principles required by Art. 5 of the GDPR?

7. Additional Authentication (an alternative to self-cert)

At a bare minimum, we propose and would hope any immediate interim solution would include both:

(1) Validation of the identity and standing of the requesting party by a qualified validator; ***and***

(2) Self-certification for before access to non-public WHOIS is granted.

This would create essentially a two-factor authentication system before a requesting party is allowed in "behind the gate" and allow them to conduct searches of the non-public WHOIS. That party would then be required to abide by terms of service which would prohibit use of data gained in these searches in a manner that is inconsistent with the GDPR. In other words, in addition to the requestor having to provide a self-certification prior to making a request to access to non-public WHOIS, that requestor might also need to be validated by an independent third party, perhaps selected in consultation with its respective constituency (ex: IPC, WIPO??), prior to gaining access behind the "gate." This additional step, while not perfect nor assured to be blessed by any DPA, at least makes layered access more legally-defensible.

What is available?

- Once a credentialed entity or individual has access to the WHOIS, what can it access? Is its access limited to searches for the WHOIS records for particular domain names, or may a requestor have access to the records of all the domain names associated with a given registry or registrar?

- While we understand that some WHOIS users consider the ability to search across an entire database is critical, we are concerned that this kind of access is in tension with both the purpose limitation principle and the data minimization principles required by Art. 5 of the GDPR. We believe that DPA guidance on this point is required. Similarly, what happens if a requestor is found to have abused its access to the non-public WHOIS? It seems to follow that any requestor would have to agree to some terms of service ensuring that it will access, collect, retain and delete any data in the non-public WHOIS in a manner that is consistent with the GDPR.

As noted, while a central credentialing body is desirable for contracted parties and those seeking to make WHOIS requests, having such an entity/organization and the requisite technical development operationalized in the next three months is unlikely. If that is the case, and the Model still contemplates a mechanism for credentialed or gated access, it leaves a substantial void that would need to be filled by an immediate "Interim for the Interim" solution to deal with how we limit access to some appropriate level of degree.

We could not support an immediate interim solution that relies upon a pure "Self-Certification" method, where any party that completes the certification form or questionnaire in full is automatically granted access to nonpublic WHOIS data, unless and until a Data Protection Authority clearly states that self-certification is acceptable for that purpose. Without such an assurance, self-certification on its own is not defensible as it amounts to an "honor system" that can and would be easily gamed by any actor seeking to access the non-public WHOIS (i.e., it serves as no true gate at all).

8. Implementation

Implementation of the Model, as well as compliance with the GDPR itself, may necessitate changes to various contracts. What will the timeline and process be for implementing the Model via contracts (RA, RRA, RAA, Data Escrow Agreement, etc.), especially for those non-WHOIS related items (transfers, escrow, etc.) of GDPR compliance?

- Does ICANN envision Registries and Registrars utilizing existing amendment and WHOIS waiver processes or will ICANN develop a fast track or expedited process considering the expedited timeline of GDPR related implementation actions?

- What will the Contractual Compliance framework be for implementation of the Model by contracted parties (e.g., if contracted parties find through their own evaluation that they are unable to implement the Model as presented, how will compliance handle that)?

9. Public Interest

ICANN, the GAC and the Commission have highlighted that the provision of a WHOIS service is in the public interest and it appears like the existence of a public interest is used as a justification for processing data, particularly the disclosure thereof. It remains unclear, however, what the legal basis for data processing based on the public interest is. Art. 6 I (e) of the GDPR mentions processing necessary for the performance of a task carried out in the public interest, but it applies only to controllers in very limited situations. The processing of data by controllers working on behalf of an official authority for example can be justified if they are vested to carry out the tasks in public interest or in exercise of official authority. The same may apply to ICANN in case ICANN is also vested in exercise of official authority and therefore the ICANN bylaws are derivatives of this task. However, this would require a commitment by ICANN regarding this official task and confirmation from DPAs and/or the Commission regarding such role of ICANN. In such case, ICANN could process data in the public interest, but how is the connection made to registries and registrars?

Alternatively, should Art. 6 I (f) of the GDPR have been considered as the legal basis, would all the public interests mentioned by the GAC and the EC be considered legitimate interests according to the aforementioned clause? If so, would those be considered legitimate third-party interests that per se outweigh the interests of the data subject?

In order to operationalize the requests by the GAC and the EC, the contracted parties would need to understand exactly what legal rationales can be used to process the data.

Conclusion

The questions and requests for clarification detailed in this letter are meant to provide constructive input to ICANN as it moves toward proposing its Model. We hope ICANN gives due considerations to the matters raised herein and continues to collaborate with the contracted parties as it refines the details. We look forward to further discussions on these questions and hearing more about the Model.

Sincerely yours,

Paul Diaz, RySG Chair
Graeme Bunton, RrSG Chair
Thomas Rickert, eco – Association of the Internet Industry

cc: Göran Marby, CEO