March 27, 2018

Göran Marby
CEO & President
Internet Corporation for Assigned Names and Numbers (ICANN)

Re: Suggested Procedural Improvements for ICANN's Interim GDPR Compliance Model

Dear Mr. Marby,

We welcome the opportunity to provide feedback on the "Cookbook" model for GDPR compliance (released 8 March 2018).[1] We regret, however, that the ongoing process to develop an interim compliance model has fallen well below the standards for accountability, transparency, and multistakeholder inclusion adhered to in ICANN's standardized Policy Development Processes. Despite the threat of an impending deadline looming large over conversations, it is of utmost importance that ICANN safeguard the openness, inclusiveness, and integrity of its processes to ensure the continued success and legitimacy of the multistakeholder model of governance.

ARTICLE 19 is an international nonprofit organization that has been defending and promoting of freedom of expression and freedom of information around the world since 1987. In recent years, ARTICLE 19 has become an active member in the ICANN community and has consistently worked towards ensuring respect for human rights, particularly freedom of expression and privacy. We believe that human rights considerations should factor into formalized and ad-hoc policy development processes alike, particularly in light of ICANN's Human Rights Core Value to respect internationally recognized human rights as required by applicable law.

We are concerned that poorly defined procedures in the "Cookbook" interim model miss the mark for useful transparency and do not incorporate sufficient checks against abuse. One notable procedural shortcoming has been the disproportionate influence afforded to certain stakeholder groups as the tiered-access model develops. While deferring to the Governmental Advisory Committee might be appropriate for the identification of law enforcement agencies, ICANN should not rely disproportionately on certain stakeholders while excluding others, particularly those representing end-users. Such asymmetrical stakeholder involvement in determining the standards for accreditation—a fundamental component of the tiered access model—both tarnishes the multistakeholder model and trivializes the stakes of communities beyond law enforcement and the IP constituency.

Judging by the "Cookbook" model, the accreditation process for determining third-party access to non-public WHOIS data has yet to materialize, as the relevant section of the document only vaguely

[1] https://www.icann.org/en/system/files/files/gdpr-compliance-interim-model-08mar18-en.pdf

references “pre-defined criteria and limitations” and the possibility of a “WHOIS data access code of conduct.”[2] Highlighting the lack of procedural checks and safeguards envisioned at this stage of the model’s development, we have formulated several suggestions on how elements of oversight and due process can be incorporated into ICANN’s tiered-access interim WHOIS model.

Suggested Improvements

CRITERIA FOR ACCREDITATION

In privacy terms, the tiered access model is a vast improvement over the current WHOIS database. An accreditation program must be developed for this model to come to fruition, and we recognize the merit of the GAC playing a role in this process. However, the approach of consulting exclusively with the GAC and relevant EU data protection authorities to determine the user groups and other entities eligible for accreditation, then bringing in “designated expert groups” to facilitate the selection of accredited parties should be reversed to add legitimacy and expertise to the process. We suggest:

- **Subject experts from within and potentially beyond the ICANN community be involved in developing the criteria**, limitations, and/or code of conduct that will define the accreditation process(es), not consulted ex post facto. One could envision a high-level expert committee being formed for such a purpose.
- **Individual governments and any other consulting actors make their recommendations publically available**, and the criteria for any entity’s acceptance onto any list be made publically available for scrutiny. If multiple lists are created relating to enforcement of laws, distinguishing between the severity of offenses (parsing serious/indictable/violent crimes) rather than strictly by entity could be useful.

TRANSPARENCY

Widely used among Internet and telecommunication companies, transparency reporting (disclosing statistics related to requests for user data) is a best practice that could easily be incorporated into the tiered-access model to promote accountability amongst accredited entities. We suggest:

- **Records of data requests from accredited law enforcement agencies list be kept by jurisdiction**, with the presiding government held accountable for the legitimacy of requests made.
- **Mandatory transparency reports for all requests be published on a bi-annual basis to allow for oversight by the community**, including information on requesting entity, justification for request, and non-public data fields requested. Any entity—law enforcement or otherwise—flagged as making illegitimate requests should be subjected to the same review process, fines, and potential de-certification.

REGISTRANT NOTIFICATION

At present, provisions for notice to registrants indicate only the purposes for data use and how data subjects may access or rectify their personal information. This is a missed opportunity for including a built-in, bottom-up procedural check. We suggest:

[2] Section 7.2.9: “Who can access non-public WHOIS data, and by what method?”

- **Provisions for notice be amended to the effect that registrants are informed whenever access to their non-public data is requested by any actor**, unless there are express legal reasons invoked by the requestor for such notifications not to occur.
- **Registrants be provided an option to flag and contest illegitimate access** to their personal information as an ongoing procedural check for the accreditation program.

DE-ACCREDITATION

Just as personnel security clearances are subject to periodic review and can be denied or revoked for cause, the accreditation process granting access to non-public WHOIS data should be neither guaranteed nor irrevocable. We suggest:

- **A process for de-accrediting entities when illegitimate use of data occurs be incorporated.** In order to determine the legitimacy of requests that have been flagged as potential abuses, an independent review process would have to be established.
- **Costs associated with such a review process could be offset by revenue generated through an accreditation fee scheme, as well as through fines** leveraged against accredited entities for instances of illegitimate use of personal data.

IMPACT ASSESSMENT

The GDPR interim compliance model is being assembled quickly and under pressure, raising the likelihood of unforeseen outcomes and unintended consequences. Just as ICANN the organization is currently undergoing a human rights impact assessment to evaluate its compliance with ICANN's Human Rights Core Value, similar tools exist in the realm of privacy and data protection. We suggest:

- **Privacy Impact Assessments be carried out on the final GDPR interim compliance model** to ensure compliance, evaluate protection mechanisms, and assess risks and effects, particularly for "downstream" stakeholders. Assessment(s) should be carried out by an independent third-party on a semi-annual basis throughout the life of the interim model.

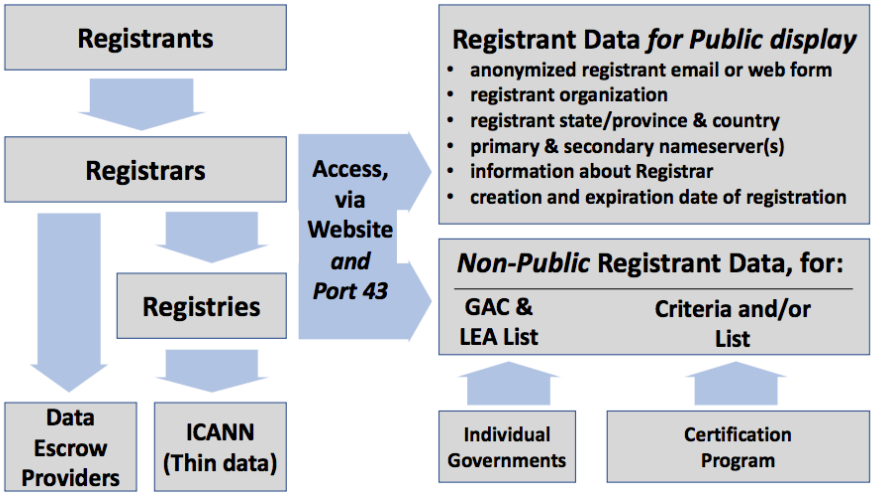
Please feel free to contact us should you wish to further discuss any of the proposed solutions set forth in this document. Thank you for your consideration.

Sincerely,

Collin Kurre and Vidushi Marda
Digital Programme
ARTICLE 19

ANNEX

Originally proposed process chart:



(from Cross-Community Session: GDPR & WHOIS Compliance Models Part 1)

Updated process chart with ARTICLE 19 suggestions: