Statement of the Non-Commercial Stakeholders Group on the
Revised ICANN Procedure for Handling WHOIS Conflicts with Privacy Law

Introduction

1. The Non-Commercial Stakeholders Group (NCSG) welcomes the opportunity to comment on the effectiveness of the updated ICANN Procedure for Handling WHOIS Conflicts with Privacy Law ("WHOIS Procedure"), which was recently revised to incorporate an "Alternative Trigger" in addition to the existing mechanism to invoke the procedure. We have carefully considered the new procedure and would like to provide input into the practicality and feasibility of utilising this instrument. In short, we do not consider it to be fit for purpose nor consistent with global trends in data protection. In this comment, we will outline why we believe it is not an adequate solution. We will then offer a pragmatic recommendation that we believe deserves further consideration by ICANN.

2. The NCSG is the most diverse body in the Generic Names Supporting Organisation (GNSO), with individual and organisational members from 128 countries. As a network of individual and organisational end-users and civil society actors representing the interests of non-commercial registrants, we represent a broad cross-section of the global Internet community. Our members are active participants in almost all of the GNSO's Policy Development Processes (PDPs) and some serve in leadership roles within these working groups.

3. Privacy is a fundamental human right recognised in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other regional and international treaties. Privacy underpins human dignity and other rights such as data protection, freedom of association, freedom of expression, speech and opinion. Since the 1970s, over 120 countries have adopted broad laws intended to protect individual privacy. The global trend has been towards adopting comprehensive privacy laws that set a framework for protection. Many of these laws have been based on the models introduced by the Organisation for Economic Cooperation and Development and the Council of Europe. In 1995, cognisant both of the perceived shortcomings of law, and the differences in the level of protection in each of its Member States, the European Union passed a directive which provided its citizens with a wider range of protection, and over time this has come to be seen as the global benchmark for protecting against the abuse of personal information. This piece of legislation has recently been revised and turned into a Regulation, which will be coming into effect next year. This regulation is the more stringent and future-proof General Data Protection Regulation (GDPR). Among privacy professionals, the GDPR is now seen as reflecting a significant step forward in privacy and data protection. There are many in NCSG who echo this view, and consider the GDPR to be a baseline for the protection of personal data which ICANN must meet.

Problems with the New Mechanism

4. The NCSG appreciates the acknowledgement from the ICANN community and organisation that the original WHOIS Procedure was inadequate. We therefore welcome the introduction of an additional avenue through which registrars and registries can reconcile their need to comply with local laws with their need to meet their contractual obligations to ICANN.

5. The Alternative Trigger says that a registry or registrar may present to ICANN a written statement from a government agency:

> *(2) Identifying and analysing the inconsistency agency has found between national law and contractual obligations, citing specific provisions of each; and*
> *(3) Certifying that agency has the legal authority to enforce the national law which it has found to be inconsistent with contractual obligations, and that it has jurisdiction over the contracted party for the purposes of such enforcement.*

We understand that ICANN as an organisation feels a duty to balance the interests of all stakeholder groups, including those of the contracted parties and the broader Internet community, when determining whether or not to grant such a waiver.

6. However, we are of the opinion that the Alternative Trigger remains too difficult a tool to invoke to be useful. This is because:

- **It is not realistic to expect an independent regulator to provide advisory opinions on private contracts.** The European Data Protection Authorities (DPAs) defend their independence fiercely, including setting their own priorities. Advice from European Digital Rights, an association of 35 human rights organisations, many of which work closely with DPAs, leads us to believe several DPAs would be very reluctant to provide such detailed, written advice that would satisfy the requirements that ICANN has proposed. This is because providing such detailed and industry-specific opinions fall outside of the scope of their typical responsibilities and would heavily consume their limited resources. Moreover, several DPAs follow the line that they will only provide guidance on issues that have not yet been resolved clearly in other ways. In light of the Lindqvist jurisprudence (ECJ Case C-101/01), ICANN's requirements regarding WHOIS data are in clear contravention of existing European data protection rules.

- In addition, where there is a change in law, the relevant government agency may not be able to provide an opinion on it until such time as the law has becomes effective. This would therefore provide the registry/registrar with no advance notice to enable them to come into compliance with the law without breaching their contract with ICANN.

- **Even if it were feasible, it is not clear which documents a registrar or registry must provide the government agency so that they could form a relevant opinion.** In particular, the purpose of the WHOIS registry has not yet been defined in policy, a problem which the Article 29 Working Party has pointed out to ICANN on several occasions. **Purpose is the starting point for data protection analysis.**

- **Data protection authorities have broad remits and are not experts in ICANN policy.** ICANN is the data processor here; it is therefore inappropriate to shift the responsibility of complying with privacy and data protection to a government agency.

- **Our members have worked for and alongside data protection authorities, and know from personal experience that data protection authorities are already over burdened.**

- **Some registries or registrars may understandably be reluctant to attract the attention of a regulator who has the power to impose substantial fines.** It seems to us unlikely that a business would write to a government agency or a judicial body saying they suspect their operations are not compliant with local laws.

- **Privacy and data protection laws vary by jurisdiction, not by business.** In the event it is determined that the Alternative Trigger is suitable and appropriate, should it be activated by one registry or registrar in a jurisdiction, we believe that it should apply to all registries and registrars in that jurisdiction even without them invoking it. This is because all businesses subject to an ICANN contract within the one jurisdiction are subject to the same laws. In this case, post-GDPR, the European Economic Area can, for most intents and purposes, be considered a single jurisdiction. It therefore follows that for registries and registrars operating in the European Economic Area a single independent analysis of the applicable law should suffice to provide evidence of a conflict with national law.

- **Not all countries with data protection laws have contactable data protection authorities.** For instance, in South Africa, the country adopted a data protection law in 2006 but did not staff the relevant agency until 2008. How would a registrar/registry in South Africa have been able to invoke the Alternative Trigger if there was no body considered authoritative enough by ICANN to provide evidence of a conflict with national law and their contractual obligations to ICANN? In addition, one may make a good faith effort to contact a government agency requesting such advice, but may not hear back and there is no way of compelling a response.

- **This procedure would disproportionately hurt smaller registries and registrars.** Particularly in developing regions of the world, where registries and registrars have considerably less resources, the burden of imposing the Alternative Trigger could be significant, especially given that the legislative landscape for privacy is changing quickly. For example all registries and registrars in most of Africa have to comply with their national implementation of the African Union Convention on Cyber Security and Personal Data, which is in the process of being implemented across members of the African Union. It would make more sense to have ICANN fund independent analysis of its contracts vis-a-vis the aforementioned international law, since this is bound to affect a lot of registries and registrars in a developing region.

- Regardless of the mechanism used, be it the original trigger or the alternative one or future mechanisms, **we do support the Consultation Step "in which all interested parties can review the written statement submitted in the Notification Step and to comment on all aspects of it".** Comments from the community have an important role to play in ICANN's decision-making processes. We would like to see guidelines and a procedure developed so that we can better understand how ICANN Staff analyse the comments which are received. Section 2.5 of the Procedure states that, "ICANN would also consult with the GAC representative (if any) from the country in question" on the comments which are received. We would like to better understand what this would entail. Would the GAC representative, for instance, have a veto over the community comments received? We respectfully suggest that not all GAC representatives are data protection experts and may not be best positioned to speak on these matters.

Recommendation

7. Rather than further revise the existing trigger or create another alternative trigger, we believe there is a much easier solution. We insist that organisation-wide **ICANN implement the global best known practice in data protection and comply in good faith with the European Union's GDPR.** We note that our colleagues in the At-Large community have made this same suggestion to ICANN. As they note in their comment:

> *"It is not unusual for ICANN to implement best practice that goes beyond current applicable local laws: Trademark protection in the DNS clearly goes beyond anything that can be ensured on the basis of national laws alone... Accordingly, we have no hesitation to formally request that ICANN implement global best practice in the matter of the protection of personal data."*

This can be done through a privacy policy based on a combination of the GDPR, the OECD Guidelines, and the Council of Europe's Revised Convention 108. Alternatively, ICANN could develop binding corporate rules, as provided for in the GDPR. We recommend that ICANN also implement a practice of subjecting policies and contracts impacting personal information to a privacy impact assessment (PIA).

Conclusion

8. We are grateful for this opportunity to share our views and trust you will find our recommendation helpful. As you move forward with your work, we ask that you please keep the NCSG updated on your progress. Given the recent establishment of a new task force that is focused on determining how ICANN and the Registrars and Registries must comply with the GDPR, may we suggest that further development of the "WHOIS Conflicts with Law procedure", as discussed by the GNSO when it approved the new trigger mechanism, be put on hold pending further developments. Thank you.