The ICANN GNSO “Business Constituency”

Comment on Proposed Interim Models for Compliance with the European Union’s General Data Protection Regulation (GDPR)

Status: FINAL

Version: 2

29-Jan-2018

Business Constituency Submission

GNSO//CSG//BC

Background

This document is the response of the ICANN Business Constituency (BC), from the perspective of business users and registrants, as defined in our Charter:

The mission of the Business Constituency is to ensure that ICANN policy positions are consistent with the development of an Internet that:

1. promotes end-user confidence because it is a safe place to conduct business
2. is competitive in the supply of registry and registrar and related services
3. is technically stable, secure and reliable.

BC Input

The BC appreciates this opportunity to provide comment on both ICANN's proposed models for compliance with the European Union's General Data Protection Regulation (GDPR) and those submitted by the community[1].

The BC thanks the community for the immense efforts in responding to ICANN's call for Community-Proposed Models for GDPR Compliance and ICANN org for this opportunity to submit comment and continue the robust discussion that started during the January 24th BC and IPC co-sponsored webinar: *Conversation on WHOIS and Compliance with EU's GDPR and ICANN Contracts* (the "Webinar"). The Webinar showcased (with nearly 230 participants) the immense interest in WHOIS among the business community and the community at large.

Our feedback builds upon observations and comments on all proposed models discussed during the Webinar.

General Observations

The BC appreciates ICANN's statements made during the Webinar that ICANN org's goal is to stay as close as possible to (1) the current WHOIS system, and (2) the current thick WHOIS policy -- while finding a solution that complies with GDPR.

As discussed at the Webinar, there are several gaps in the Hamilton analysis which need to be addressed. In several respects, the analysis is potentially biased to favor "over-compliance" in the selection of models, producing a more restricted access model than is necessary to comply with GDPR and taking ICANN org (and others) further from the current WHOIS system and thick WHOIS policy. As ICANN has indicated that the Hamilton analysis serves as a foundational source for its selection of models, the Hamilton analysis must be updated in light of this community input, before it can serve as this foundation.

[1] All models available at ICANN page "Legal Analyses, Proposed Compliance Models, & Community Feedback", at https://www.icann.org/resources/pages/gdpr-legal-analysis-2017-11-17-en

Specific Observations and Comments on ICANN's Models

ICANN's model memo says ICANN org will "continue to refine the potential compliance models based on feedback" -- presumably to address, in part, errors and omissions in Hamilton's legal analysis. During the Webinar, we highlighted open questions on conclusions in critical areas of Hamilton's legal analysis dealing with **Scope** (both Territorial and Natural vs. Legal Person); **Whois Data Accuracy** under GDPR; and **Consent**.

These concerns were drawn directly from the previously submitted *BC Comment on the Hamilton Memo regarding GDPR, as of 15-Jan-2018* and *IPC Comments On Hamilton Legal Analysis*. During the Webinar[2] we noted the possible adverse effects of such errors and omissions in the Hamilton analysis, and our analysis described below of the various models reflect these legal considerations:

Issue	Revision	Notes:
Geographic Scope (Models 1-3):	Revise to be consistent with GDPR Art. 3	Processing must be *in the context of* the registrar and/or registry's establishment to fall within the GDPR, including processing personal data of EU citizens. Without a correction, these models cast a net too wide and apply GDPR where it is not meant to apply. Model 2(b) and 3 unacceptably apply the GDPR's requirements globally, regardless of whether the registrar/registry and its processing falls within the scope of the regulation. Given the limitations of the regulation, these models should be rejected completely as they (1) appear contrary to public policy, and (2) might lead to conflicts of laws in other jurisdictions.
Access (Models 1-3):	Need to distinguish between access by data subjects and by third parties	If the requestor is the data subject, they would not be required to follow these access request requirements. They are entitled to access under the GDPR in most circumstances -- as noted in comments and during the Webinar, the data subject has the right to data accuracy, correction, and rectification under GDPR.
Centralized Credentialing (Models 1-3)	ICANN Org develops a Credential Program which enables for a one-time approval for access for specialized groups; Once approved, credentials are valid for a specified period.	Self-certification should be used until there is a centralized certification program. Requiring registries or registrars to manage credentials or self- certification on a case-by-

[2] Slides from the presentation are attached.

Issue	Revision	Notes:
		case basis is burdensome and introduces costs and unnecessary delays.
Super User Credentials (Models 1-3)	Credentials for "super users" that allow high volume, yet managed and controlled, Whois data access across all registrars and registries so as to support the more powerful search queries that are possible today on commercially available unified Whois data sets. Authenticated and managed access to these features would come with protections against abuse, such as bond and commitment to audits and compliance checks in contract with ICANN Org[3]	Specialized access at an aggregated level should be available rather than one-off look-ups, for search engines, social media platforms, browsers, security professionals, and IP owners and their representatives.
Consent(Models 1-3)	Include provisions to provide informed consent for public display, and provide option to natural persons to have validated data excluded from public, but still included in escrow	Model needs to address the opportunity for data subjects to provide consent to publication of their personal data.
Data Elements – public Registrant Email (Models 1-3)	Registrant e-mail address should also be a public data element. Natural Persons could be offered a forwarding service with a standard email.	Contact is still possible with a standard email that does not include personal information.[4]
Natural Person (Models 2-3)	Information of Legal Persons should be public	Model 1 is the most aligned with GDPR's recognition that legal persons have different privacy implications.
Enhanced Verification (Models 1-3)	Include enhanced validation procedures, such as those done by EU cctlds	The data elements to be maintained in the public database must be accurate and validated, with appropriate corrective processes made available, as required by GDPR;

[3] See the EWG Model and the ICANN Redaction Model for examples of how to prevent abuse

[4] See the EWG Model and ICANN Redaction Model, where standard email are suggested, such as: <domainname.com>@icannredactionservice.org >;

Conclusion

The BC believes that ICANN should move forward with an interim GDPR compliant model based on Model 1, with updates and clarifications detailed below. Model 1 comes the closest to meeting ICANN's objective to "ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible" while striking a balance between issues of privacy, obligations of contracted parties and the needs of those who rely on WHOIS data (3rdparties).

- This model must only apply to data associated with Natural Persons and not extend to data not covered by the GDPR , i.e. Legal Persons
- Registrant Email should be added in the list of publicly available WHOIS data, ensuring that a reliable mechanism exists to both identity and contact the Registrant. This, in addition to the Technical and Administrative email address suggested in Model 1, is an important feature that ensures a globally distributed and decentralized technical infrastructure such as DNS continued to operate in a secure and stable and trustworthy manner.
- With respect to the concept of tiered access, which we support, the BC suggests that any "self-certification" process should be consistent across registries/registrars, ensure quick access when necessary and minimize the burden to contracted parties and 3rd parties alike.
- BC supports a standardized accreditation process as proposed in Model 2, but given the work involved to set such an accreditation system up we suggest that a robust self-certification process (as described above) should be used in the interim.

Model 3 is unworkable and should not be considered since it does not meet the ICANN objective to "maintain the existing WHOIS system to the greatest extent possible."

The BC looks forward to continuing in haste the discussion we began during the Webinar. We trust that you will find our comment useful in selecting or designing an interim model for compliance with GDPR.

--

This comment was drafted by Alex Deacon, Margie Milam, Mary Ellen Callahan, Tim Chen, and David Fares.

It was approved in accord with the BC charter.