

29 January 2018

[gdpr@icann.org](mailto:gdpr@icann.org)  
[goran.marby@icann.org](mailto:goran.marby@icann.org)

Dear Göran:

The undersigned registries and registrars (“contracted parties”) jointly issue this letter in response to ICANN’s 12 Jan 2018 proposed interim models document.<sup>1</sup> We are pleased to see ICANN take initiative to investigate and propose for discussion potential compliance models for the upcoming EU General Data Protection Regulation (“GDPR”). As you are aware, contracted parties will bear the burden of implementation of and compliance with any model that ICANN deems compliant with the GDPR. In addition, Data Protection Authorities (“DPAs”) will likely monitor contracted parties to ensure compliance with the law. For these reasons we remain eager to find a solution that preserves the security and stability of the Internet and does not force contracted parties to choose between conflicting laws or our contractual obligations with ICANN. We recognize that other stakeholders within the ICANN Community have an interest in continued access to some portion of Registration Data / WHOIS. But if this is to survive, it will require continued work within the Community and leadership by ICANN.

Publication of these models, notwithstanding the calamitous state of its timing, is a positive first step. However, we (1) are not certain of ICANN’s call to action by this publication; (2) worry its multiplicity will lead to continued lengthy discussions on concepts vs. solutions, (3) are discouraged that an industry proposal developed and supported by many contracted parties (e.g., the “Eco Model”) was not discussed or addressed (and perhaps not even considered); (4) have reservations about various elements of each of the proposals, including some of their underlying principles; and (5) continue to be unclear as to the next steps and timing envisioned by ICANN to move towards agreement.

***To be clear, we do not believe any of the models represent anything more than concepts for further discussion. None of the options presented represent an “out-of-the-box” solution to GDPR compliance.*** Despite these concerns, in the interest of time, please find our comments and feedback as to the commonalities, and each of the individual proposed models, below:

### **The Fundamentals**

- All of the proposed models contemplate that “full thick data” be collected by registrars and transferred to registries and escrow agents. What constitutes “full thick data” must be revisited to address basic principles of privacy law (ex: data minimization/purpose limitation) so that only those elements that are necessary to their underlying purpose are collected, and thereafter shared. As addressed in the Eco Model, much of the personal data required in tech and admin contacts was determined to be unnecessary. Any model needs to clearly identify what data elements are being considered, and match

---

<sup>1</sup> <https://www.icann.org/news/blog/data-protection-and-privacy-update-seeking-community-feedback-on-proposed-compliance-models>

these to the underlying purpose. Additionally, perhaps we should discourage the use of “thick” and “thin” as those terms can have varied understanding and limiting meanings.

- As was previously communicated to ICANN by the Hamilton law firm and others within the ICANN community, consent (at least in its current form) is not a practically viable legal ground for processing personal data in an efficient way, given the intended use of the Whois services. In addition, the models require “freely given” consent which is likely not attainable if the service demands consent as noted by the Article 29 Work Party in its letter of 6 December 2017. We also note this section speaks to data elements that are arguably not personal data at all (such that consent would not even be required).
- To the extent the party is a controller of the data at issue, we agree each will be responsible to address data breaches as required by law. However, to the extent ICANN, registries, and registrars are considered joint controllers, more collaboration is necessary to comprehensively define these responsibilities.
- Varied data retention periods are raised in each model and are seemingly arbitrary. We believe data retention requirements should be left to the contracted parties, as they are more familiar with local applicable laws and their own business practices, policies and requirements.

### **Model 1 – Bigger than GDPR and the Issue with Consent**

This model presumes we have a GDPR-exclusive issue. Though it is GDPR’s threat of fines and increased enforcement that has caused the community to take note and urgently react, it’s short-sighted to seek a solution that disregards the (ever-changing) principles of privacy laws elsewhere around the world.

*The Good:* In an ideal world (assuming this becomes a non-GDPR exclusive model), having a Public WHOIS that, upon DPA approval, displays only a few personal data elements (ex: registrant name, address and even email), in addition to non-personal data registration elements (similar to the EU trademark registrar, for example), is seemingly a solution that appeases the concerns of all interested parties (except, perhaps the registrant).

*The Bad:* This model requires that contracted parties continue to publish personal data without proper consent (given its flaws), or other acceptable authority or justification, and without guidance from DPAs or legal advisors as to whether publishing such basic information would be acceptable under some greater, and generally applicable, public interest. Without such assurances, registries and registrars would need to assume significant, and likely untenable, risks.

### **Model 2(B) – Complexity, Cost and Time**

Model 2A contains the same problem as Model 1 with regard to its scope of applicability, and as such is not specifically addressed. Model 2B removes the applicability limitations, and contemplates publication of few very data elements publically. This is obviously a preferred outcome by contracted parties absent assurances that publication of personal data will be deemed acceptable. However, a workable ‘certification program,’ which in and of itself is fraught with complications and not necessarily worth pursuing absent DPA approval, is a longer term solution and not implementable in advance of the looming deadlines. An alternative would need to be adopted as an interim solution.

*The Good:* (1) Contemplates opt-ins for registrants, which given the default of no published data, could represent valid consent. (2) No personal data is published (excepting for potential tech/admin email contacts). (3) Applicable to all registrations and all parties worldwide.

*The Bad:* (1) Developing a workable certification program that has buy-in from the Community and DPAs is a long-term task. It must be done in a way that provides access on an objective and consistent basis so that it does not administratively overwhelm registries and registrars (and perhaps should include a central clearinghouse of some sorts, ex: TMCH). (2) Consent remains a very weak mechanism for reasons mentioned above. This model also contemplates opt-ins for registrants, and where there are opt-ins, there must be the right to opt-out, which requires significant development efforts for contracted parties, not to mention the development needed to record and track consent, and withdrawal thereof, on a registrant-by-registrant basis.

### **Model 3 – A Stopgap Option**

Model 3 is the safest model for contracted parties, and is closest to the Eco Model, because publication is limited. Because of its conservative approach, this model makes the most sense as an interim solution, while the Community works to develop consensus policies on RDS, and DPAs have a chance to issue further guidance.

*The Good:* Works as a short-term interim solution pending certain adjustments (e.g., “display unless”).

*The Bad:* (1) Though it would provide the broadest possible short-term protection to contracted parties, unlike the Eco Model, it does not sufficiently contemplate concessions that would also satisfy other stakeholders interested in preserving the status quo of WHOIS. (2) The concept of “display unless field includes personal data” is operationally unworkable. Absent fool-proof ability to screen and determine what is PII vs what is not, displaying any of these fields would unnecessarily risk exposure of personal data of registrants and other contacts.

### **Conclusion**

All proposed models represent a positive step, but all share critical flaws and are several months (at least) beyond the deadline for refinement and improvement. Many contracted parties, representing the bulk of gTLD domains under management and in conjunction with their internal and external legal resources, contributed to the Eco Model and supported its submission to ICANN. While we recognize it is also not a one size fits all model, we believe it to be the best path forward for working as a Community towards GDPR compliance, while addressing the needs of other stakeholders. We encourage ICANN to read and consider the comments submitted by the drafters of the Eco Model in response to ICANN’s proposed models. Those comments provide sound legal analysis that can be useful in consideration of the ICANN proposals and help inform our discussions as we move forward.

As indicated earlier, the near simultaneous publication of these models and the submission of the Eco Model fosters a concern that the latter model was not considered by ICANN in the development of its proposed models.

We recognize and respect the needs of non-contracted parties in the ICANN Community. We are not opposed to examining long-term solutions meant to serve community goals and preserve the

stability and security of the Internet through the existing RDS PDP WG process, but we must ultimately act in the manner most prudent to our ongoing business operations. There can be no doubt that contracted parties, and ICANN the organization, share the costs and risks associated with GDPR compliance. With this in mind, we ask that you join us in further exploring the Eco Model both as an interim and long-term solution for GDPR compliance – including identifying and resolving its remaining deficiencies as we continue as a Community to work on a more permanent solution.

Respectfully,

**1&1**

**Akamai**

**Astutium Ltd**

**Blacknight Solutions**

**Brandma.co**

**DNS Africa**

**Dominion Registries**

**Donuts Inc.**

**Endurance**

**GoDaddy**

**NetEarth One**

**Netistar**

**Nic.br**

**Nominet**

**Nordreg AB**

**Public Interest Registry**

**Realtime Register B.V.**

**SafeBrands**

**Tucows**

**United Domains**

Cc: [akram.atallah@icann.org](mailto:akram.atallah@icann.org)  
[cyrus.namazi@icann.org](mailto:cyrus.namazi@icann.org)  
[russ.weinstein@icann.org](mailto:russ.weinstein@icann.org)