From: "Amadeu Abril i Abril (CORE)"
Date: Monday, January 29, 2018 at 13:51
To: "gdpr@icann.org"
Subject: [Ext] Comments from CORE on the 3 propsoed Models.

Dear ICANN GDPR Team,

CORE Association (CORE) welcomes the opportunity to comment on the document "Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union´s General Data Protection Regulation".

While CORE is a Registry Operator located in Switzerland, it provides Backend Registry Operator and Policy Advisory services for a dozen TLDs with seat in the EU, where most of the members of the Association are also located. CORE was also one of the original ICANN Accredited registrars until it transferred its accreditation to its wholly-owned subsidiary COREhub in January 2014, and also serves as one of the ICANN-appointed Emergency Backend Registry Operators (EBERO). In all these capacities, but specially as BERO for EU-based TLDs having negotiated with ICANN and their DPAs a compliant Whois service, CORE wants to submit the following

COMMENTS

A) General Comments.

1. Need to keep current validated models. We wish to stress once again that while the GDPR amends the scope and implementation of Data Protection Legislation, its substantive rules and, specially, principles remain unaltered from previous (still current) EU legislation. In this regard is therefore imperative that no interim mesure interferes with implementations agreed in the past wth (and/or mandated by) national DPAs. And such previously agreed systems should be the basis for future models, at very least, in the same jurisdictions.

2. Goal is compliance, not status quo. While we feel that the goal of keeping (some sort of) a public Whois directory bears some merit, we must remind that the goal of this exercise is to make such service compatible with Data Protection

legislation and the itnterests of registrants, both completely overlooked all these years. Having as a goal to "change as little as possible" leads to less than useful results, and some confusing choices in the models you submit for review.

3**. Support for tiered access.** CORE has long supported a tiered-access model. While all aspects (collection; transfer; publication; access; retention of all personal data) are relevant from the legal point of view, we would lie stressing that the publication of personal contact data in a public, and easily accessible and harvestable, service is the main complaint from users. Choices leading, for any reason, to the excessive publication of such contact data are not sustainable, even if they were legal (but they are not, either).

4. Opt-out for (individual) registrants. In CORE's view the starting point for a meaningful solution consists in allowing individual registrants the choice to opt-out from publication of personal data (with the corollary of mechanisms to handle contact and disclosure requests). The experience of both .cat and a number of ccTLDs show that this system is not only approved by DPAs and supported by users, registrants or not, but also perfectly manageable by Registries and Registrars.

B) Commonalities across all models.

1. Some data fields are not needed at all. CORE generally supports the assumptions made in this part of your document, with some caveats. For instance, some data fields seem perfectly irrelevant or outdated (Fax in 21st Century? Who has ever used the physical address of the TechContact?). A (small) number of data fields could hence be excluded from the whole process.

2 Support for thick Registry model. We feel that this is not the place to restate the whole debate on thick/thin Registry models, but we want to express our strong support for a solution that ensures that the basic data set collected by the Registrar is transferred to the Registry (and to Escrow).

3. Data retention. The different lenghts for post-contractual data retention in the three models seem inconsistent with the data set collected and processed/transferred. Differences in publication do not seem to justify difference in retention periods. And any period of time will need to be justified

according to the GDPr criteria. In general we cannot see any justification for periods of 2 or 1 year, whle six months may be needed (specially at registrar level) for transfer disputes, chargeback controls and other compliance purposes. In addition, certain data fields may require some different periods in different jurisdictions for tax or accounting purposes. But a general periods of 1 year and beyond seem nearly impossible to justify.

4. Differences in scope. Same as in 5 above, we fail to see the connection between the different data models and the personal/geographic scope of those models. This should be discussed as a separate topic, not tied concrete data sets.

5. Access: Contact is not Disclosure. All 3 models seem to assume that access to Registrants by third parties **must go** through some level of disclosure to the relevant data to such third parties. This is misleading. Experience show that there is sometimes a legitimate purpose for contacting a registrant, but this can be handled by a Registry-level Contact Form, ie. This procedure, equivalent to some sort of role address contact or proxy service by the Registry alliviates the need for disclosure in many cases. This has been implemented by some Registries using a tiered-access model, both gTLD and ccTLDs.

C) Model 1

1**. Opt-in/Opt-out.** We support an opt-out model, based on our discussions with DPAs and expperinces with Registries. Both are acceptable, though.

2. Natural-person registrants. We support the specific approach for natural-person registrants, with some conditions. Above all, publishing the contact data for AdminContact and TechContact completely defeats the purpose as they are identical to the Registrant in the vast majority of cases. No real need for third parties to contact such roles, when they are, by default, the very Registrant. As it is described in the current document, we cannot support Model 1 at all.

3. Name of Registrant. In our experience DPAs have not been completely consistent with regard to the publication of the Registrant name when it is an individual. In an interim model we would firmly support a model that does not publish it.

4**. Registrant address**. CORE believes that the jurisdiction (ie, City and Country) of Registrant should be published in order to facilitate a a number of third-party enforcement considrations, but not the physical address (personal data without doubt, and with no specific purpose here).

6. Changes needed to Corporate Registrant Data. We believe that the historical confusion between Registrant Name and Organization Name should be solved and only publish the Registrant Name, ie, the legal entity's one. We are not sure this can be achieved in any meaningful timeframe, though. Also, phone and email have proven to be a source of real problems and complaints to DPAs, specially for small businesses. The abuse of such direct contact data has been increased by the pport implementation of the CZDS.

In summary, we could support a modified version of Model 1 in which neither the Registrant name for natural-person registrnts nor email and phones for any registrant would be published by default.

D) Model 2

1. Publication of contact details. As explained above, this is an absolute no-go for, at very least, domains registered by individuals for non-commercial uses, and probably well beyond that case.

2. Centralized accreditation. CORE is convicnced that such an accreditation process is unfeasible in the short timeframe we have to conform to GDPR. In addition, the really bad experience of the CZDS shows that such a model will require serious thought. Finally, we are convinced that categories such as Intellectual Property Lawyers or even Law Enforcement are legitimate parties that may request concrete data sets, but probably not gain full and unrestricted access to all data from all registrants through a general accreditation process.

E). Model 3

1. Unworkable. "Do not display any personal data" is a well-intentioned goal, but makes the model unworkable (inthe short term) unless Registries/Registrars may select data types for both natural and corporate registrants. Which goes back to the previous models.

2. Due process requirements. Subpena/court orders seems an excessive requirement for all and any access to any data.

F) Conclusion

CORE supports a tiered-access model, based in opt-out (or opt-in) of at least natural-person registrants. No contact details (including, possibly, the Registrant name) should be published without consent. For legal-entity registrants some data fields should not be published. Registries should establish and manage a contact form and both Registries and Registrars should handle disclosure requests according to requests specifying the purpose and legitimacy. No centralized accreditation mechanism seems realistic in any short period of time.

As a second best, a non-publication system similar toa refined Model 3 would be preferable as an interim solution.

In all cases, the scope, access and retention should be discussed on its own merits and not tied to a concrete model above.

CORE will submit its own model for discussion.

Best regards,

Amadeu Abril i Abril
Chief Policy Advisor
CORE Association