Internet Council of Registrars

2018-03-07

CORE comments on the "Calzone" proposal

CORE Association (CORE) welcomes the opportunity to comment on ICANN's interim model for Whois compliance with the GDPR.

CORE is the Registry Operator for three TLDs, and Backend Registry Operator for additional 17 TLDs, 12 of which located in the EU. Additionally, our wholly-owned subsidiary, COREhub, also located in the EU, is an ICANN-accredited Registrar. In the name of both entities, and many of our customers, we want to submit the following

COMMENTS

1) Collection of Data: We support the current status quo in the interim model, even if we continue to doubt that fields such as Postal Address for the Technical Contact or Fax have any practical use nowadays, and hence, "legitimate purpose" is hard to justify.

2) **Transmission to Registries and Escrow Providers**: We also support the transmission of data in the current terms to Registries, provided Registries include in their RRAs the necessary guarantees and indemnifications. Escrow service, both for Registrars and Registries, is in the clear interest of the Registrants and the whole system's stability, and should therefore be maintained in the current terms, for the whole data set.

3) **Publication of Default Data Set**: In general, we support the defined default data set, given that the model that does not distinguish between natural and legal person Registrants. Our big concern here is operational rather than conceptual: the distinction between the Registrant Name and Organization Name fields has always been confused by registrants. The result is a complete mess that would defeat any useful purpose. There won't be enough time between the approval of this or any model by ICANN, its implementation by Registrars and Registries and the May 25th deadline in order to carry out the multiple necessary rounds of communications to registrants to update their registrations. In this regard we formally ask for a six (6) months of moratorium during which Registrars and Registries could choose not to publish the Organization Name in the default data set.

CORE Internet Council of Registrars (CORE Association)
2, Cours de Rive - CH-1204 Geneva, Switzerland
Phone: +41 22 312 5610 - Fax: +41 22 312 5612 2 - Email: secretariat@corenic.org

ICANN could also consider giving Registries the option to distinguish between natural and legal person Registrants, applying the default data set to natural person ones, and allowing for more data on the corporate ones.

4) **Opt-in to Extended Publication**: We had expressed a preference for an opt-out mechanism for natural person Registrants, but can support the described opt-in for all registrants. We know by experience that this is not easy to implement by Registrars with a long chain of resellers. Again, this measure will need some time beyond May 25th to be universally implemented.

Additionally, while CORE could easily adapt the opt-out mechanism developed for the .cat Whois, we cannot see how Registrars could implement dozens, if not hundreds, of proprietary opt-in extensions. We propose that the opt-in would only be mandatory once an EPP Extension has been standardized.

5) Communication with Registrants: We fully support the substitution of the publication of Registrants' email addresses with anonymized emails or web forms. ICANN should let Registrars (and/or Registries) chose their model, and we have a strong preference for web forms, as anonymized emails published on the Whois will be subject to the same level of massive spam as we witness today. This is precisely one of the main complaints of registrants of any type with the current Whois. We don't only support web forms, but a curated service, in which emails are *not* automatically forwarded to registrants. This set-up, by itself will dramatically reduce spam and most other undesired uses of published emails. This puts some burden on Registrars and Registries, but these parties also have a specific responsibility in a healthy and trusted DNS.

6) **Parties with Access to Full Data Set**: We agree that Escrow Providers, Dispute Resolution Providers and ICANN have legitimate reasons for full access. Regarding Registrars, we request that this is defined as "Registrars accredited and active in that respective TLD". Their claim for full access is basically related to incoming transfers, and they can only perform such transfers for TLDs in their current portfolio.

7) **Accreditation System**: We are afraid that the accreditation procedure, as described, may result in a combination of the worst features of the TMCH and the CZDS. Which is a lot to fear. But we look forward to proactively working with the ICANN community to define a workable model. In any case, we exclude self-certification as an interim, or long term, solution.

8) **Full Access for Certified Third Parties Must Not Be Universal**: One critical point is that a party certified as a legitimate user should not automatically be granted full

access in all TLDs. We have expressed the need for limitations in the case of Registrars, in 6) above. If we take the example of “licensed lawyers representing intellectual property clients, as discussed in your model, we should remind that even the memos prepared by Hamilton law firm expressed concerns that such unrestricted access would be contrary to the GDPR. Even for Law Enforcement authorities, but here we may concede that unrestricted access is justified.

Certainly IP Lawyers, to take that example, may need access to the Zone File in order to perform checks on labels, parts of them, variations thereof, etc. In case they find or suspect specific problems with any number of domains, they have a legitimate interest in being granted full access to only the data related to those domains. Going from, theoretically, a single client with a single trademark in a single jurisdiction to full access to all personal data in all TLDs goes beyond any legitimate purpose, any proportionality measure and is, clearly, contrary to the GDPR. In cases like these, the third parties should file requests for the lists of domains, stating the basis on which their claim is legitimate. We also believe that such requests should be notified to the Registrants in question.

8) **Methods for Accessing Full Data Set**: As said above we don’t believe that a single, universal, unrestricted access right should exist. Therefore the whitelisting of IP addresses seems adequate for certain categories, like IP enforcement or Dispute Resolution Providers, while request-based web forms seem the only way for other cases.

9) **Data Retention**: We support maintaining the existing Waivers, especially as we deem the stated 2 years default in the RRA difficult to justify.

Best regards,

Amadeu Abril i Abril
Chief Policy Advisor
CORE Association