Comments on proposed interim (whois) model for GDPR compliance by DNS Belgium

DNS Belgium is the registry operator for the .be ccTLD and 2 new gTLD's: .vlaanderen and .brussels.

DNS Belgium has noted the recent blog post by ICANN President and CEO Göran Marby and would like to share it views concerning the proposed interim model for GDPR compliance. We have 3 concerns that we would like to share: differentiation between "private" and "corporate" registrants in whois, non-compliance of bulk access to whois with GDPR and potential issues with data transfer (e.g. escrow) to non EU jurisdictions.

DNS Belgium has substantial experience with regard to the legislative framework concerning the processing of personal data as it is an organization based in the EU and is already subject to data privacy laws on both European and Belgian level. As a consequence, DNS Belgium has modified its public whois for .be over a decade ago with the explicit aim to protect the privacy of .be domain name holders.

Distinction between registrations of legal and natural persons

At the same time, DNS Belgium is convinced of the overall relevance and importance of a public available whois and the purposes it serves. Therefore, we share ICANN's view "*to identify the appropriate balance for a path forward to ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible*".

This being said, we also share the following concern that was mentioned in the article:

"Some commentators have raised concerns that permitting the model to be applied on a global basis and not distinguishing between registrations of legal and natural persons is an over- application of the GDPR and not consistent with ICANN Org's stated objective to maintain the existing WHOIS system to the greatest extent possible."

While we understand that not all registry operators have opted to differentiate between registrations of natural persons and those of legal persons, we are disappointed that the lack of such differentiation has been considered as the only viable option for creating a new whois model. The fact remains that many registry operators have solutions in place to differentiate between "private" and "corporate" registrations and would be able to work with a model that displays more relevant data through whois and yet remain in line with the GDPR principles.

DNS Belgium suggests considering a more layered model that would allow a registry operator to make the decision whether or not contact data of "corporate" domain name holders would be available through whois. Registry operators that feel they cannot reasonably differentiate between "private" and "corporate" registrations could then opt for the currently proposed model while registry operators that are of the opinion that they can make such a differentiation could apply a slightly different version of that model (one that allows to publish registrant data for "corporate" registrations). This would certainly assist those registries to maintain closer to the existing whois model.

Access to full whois vs. privacy by design/default

With respect to layered access to whois data, DNS Belgium would like to share a number of serious concerns.

We feel that the proposed way forward is highly problematic in a number of areas as we will explain in detail below.

The overall approach of granting certain groups access to full whois data under an accreditation program is in conflict with the principles of privacy by design/privacy by default as listed in art. 25.2 of the GDPR. The purposes of whois do not require full or "bulk" access to the data. A "case by case" access could be sufficient to meet the needs of the groups seeking access to whois and would preserve the principles of art. 25.2 of GDPR at the same time.

The proposed mechanism for whois data access under an accreditation program seems also problematic in terms of timing & operability. We fear that the different stakeholders will not be able to reach a full decision on this by 25 May 2018. Even in the case of a full decision by that date, this doesn't mean that registry operators and registrars will be able to implement this in a timely fashion. There is also a serious concern about the determination which entities will be accredited or not. We fear that neither the GAC, neither a working group representing the ICANN community possess the legitimacy to determine under which conditions access to private data would be tolerable from a GDPR perspective. Such determination would better be left to the relevant DPA's or the successor of the ART29 WG. On top of that, such accreditation program would heavily depend on the level of scrutiny of the applications. A mechanism such as currently used for those who seek to access the zone file of gTLD's would clearly not be sufficient.

Transfer of data to jurisdictions that have a lesser degree of privacy protection than EU

Lastly, DNS Belgium also wishes to share a concern regarding the transfer of data (or access to that data) for escrow providers and ICANN itself. While we understand the need for escrow services and ICANN to have access to the data, we must emphasize that a transfer from that data to countries/territories that do not guarantee the same level of protection as in the EU is not possible without having certain safeguards in place. In order to make this a viable solution, ICANN would first need to consider putting such safeguards in place.

DNS Belgium welcomes the opportunity to provide feedback on the proposed interim model for GDPR compliance and hopes that its comments are useful to amend the proposed model.