Paris, 26 March 2018

Afnic comment on Proposed Interim Model for GDPR Compliance

Afnic is the registry operator for top-level domains corresponding to the national territory of France (.fr, .re, .pm, .yt, .wf, .tf) and the backend registry operator for 14 new generic Top Level Domains. Afnic is a member of CCNSO, Centr, and APTLD.

In 2006, Afnic has implemented for .fr domain names a personal data protection process according to which the personal data of the individual registrants are not disclosed in the WHOIS.

That is the reason why we welcome the opportunity to share our views on the proposed interim model in particular with regard to our long term experience regarding personal data protection.

1- Distinction between natural and legal persons

First of all, we would like to share our concern with the potential approach proposing not to distinguish between registrations of legal and natural persons. As many commentators have already pointed out, we believe that this is indeed an over-application of the GDPR.

Despite the fact that GDPR does not protect data pertaining to legal persons, we would like to remind ICANN that in its letter dated 11 December 2017, WP29 states the following:

*"WP29 wishes to stress that the unlimited publication of **personal data of individual domain name holders** raises serious concerns regarding the lawfulness of such practice under the current European Data Protection directive (95/46/EC), especially regarding the necessity to have a legitimate purpose and a legal ground for such processing".*

It appears very clearly that only personal data of individual domain name holders are requested to be protected and undisclosed in the WHOIS.

Not distinguishing between legal and natural person is a misinterpretation of European DPA's explicit recommendations on the new legal framework.

2- Who can access non-public Whois data, and by what method?

The proposed interim model provides that "*registries and registrars would provide access to non-public registration data only for a defined set of third-party requestors certified under a formal accreditation program.*"

Despite the fact that this accreditation program might require time to be set up, we remain sceptical with regard to its complexity and more importantly, its legal basis.
Personal data is by essence protected by a confidentiality principle. It is the reason why we stress the importance of a case-by-case approach rather than an automated and bulk approach.

One disclosure model described below could allow legitimate access to personal data by third parties, while protecting the rights of the registrants:

- For law enforcement agencies, access to this confidential data shall be based on legal grounds providing precisely the type of data requested and the entity allowed to accessing this data. The analysis of the legal ground should be carried out further to case-by-case verifications, prior to each request of data disclosure.

- Regarding other third parties, the balance needs to be established between the third parties interests and the interests or fundamental rights and freedoms of the registrant.

For that purpose, Afnic has set up in 2006 a procedure granting a right of access to third parties with a legally protected interest in a domain name. Upon disclosure request, AFNIC carries out a case-by-case analysis of these requests, based in particular on the applicants' previous rights (trademarks, previous distinctive sign, surname etc.). The requestor would self-certify that the data provided would only be used for the limited purpose for which it was requested.

Based on our experience, we have some concerns regarding an automated mechanism providing access to personal data, even if built on an accreditation program.

If this accreditation program relies on the signature by the requesting third party of a licence contract in order to access the full Thick WHOIS data for an unlimited period of time, with no case-by-case prior checks, this will not be sufficient with regard to the protection principle.

Afnic has assessed the risks related to personal data disclosure under .fr (harassment, identity theft, spamming etc.) and in order to take these risks into account, AFNIC requires, for every data disclosure request, the signature by the applicant of a commitment with regard to the provided data.

An unlimited automated access to the full Thick WHOIS is not satisfactory with regard to the protection principle neither in terms of materiality nor in terms of duration.

Such unlimited automated access, even to accredited requestors, would ultimately go back to make all personal data in the WHOIS available to the general public.

Finally, we would like to point out that registries, registrars and ICANN will be evaluated on the transparency of their processes and on the clear information given to their users.

GDPR refers to each one's own responsibility. What will matter is the appropriate balance between the protection of individuals and other legitimate interests.

Marianne GEORGELIN
Head of Legal & Policy

Association Française pour le Nommage Internet en Coopération, Immeuble Le Stephenson, 1 rue Stephenson, 78180 Montigny-le-Bretonneux (France)
Tél. : +33 (0)1 39 30 83 00 | Fax : +33 (0)1 39 30 83 01 | Siret : 414 757 567 00030 | APE : 6311Z - TVA N° FR 72 414 757 567
www.afnic.fr | contact@afnic.fr | twitter : @afnic I facebook : facebook.com/afnic.fr