Public consultation

Facilitating access to registration data for authorised authorities

Summary of contributions

January 2023

www.afnic.fr | contact@afnic.fr

Twitter: @AFNIC | Facebook: afnic.fr

CONTENTS

1. Introduction

The public consultation was held from 12 September to 12 October 2022, online, on our website (**www.afnic.fr**).

We received three contributions in response to this public consultation.

This document presents a summary of these contributions.

2. Reminder of the project

This consultation concerned the plan to give authorised public authorities **direct** access to the registration data of domain name holders under the .fr TLD (and also .re, .pm, .wf, .yt and .tf) in the registry's database by means of the Registration Data Access Protocol (**RDAP**).

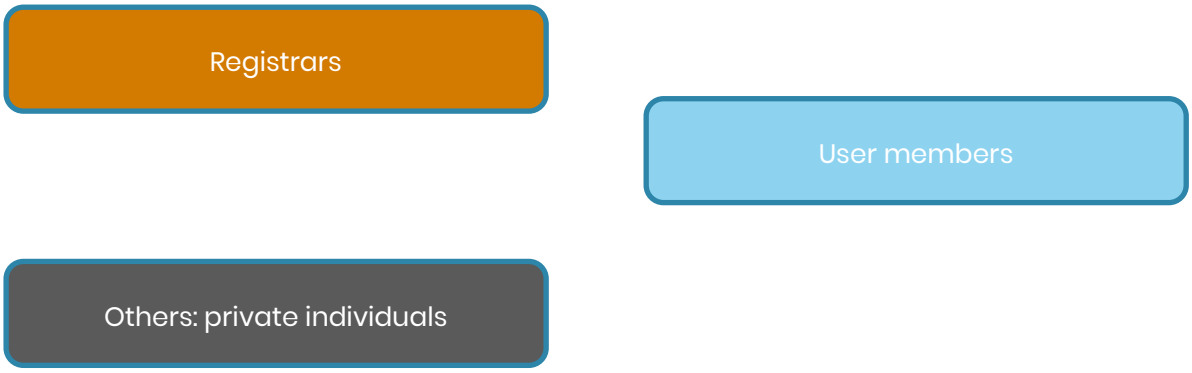
"Authorised public authority" means an authority or body having a **right of communication** based on legislative or regulatory provisions.

The authorities making these requests to Afnic to date are: the **gendarmerie, the police**, the **CNIL** (French Data Protection Agency), the **DGCCRF** (General Directorate for Consumer Affairs, Competition Policy and Fraud Control), **DGFIP** (General Directorate of Public Finance), **Customs** and the **DDPP** (Departmental Directorates for the Protection of Populations).

This project forms part of our overall approach to combating abuse, and more specifically our aim **of facilitating the access of public authorities to registration data in the context of their investigative powers, for the repression of online abuse**.

All the contributions and consultation results gathered over the course of the year 2022, from the public and from the internal bodies of Afnic and the CNIL, will be taken into account when we roll out the project.

3.Categories of respondents



4. Summary of contributions

We received very few responses to this consultation, but the quality of these responses enables us to present a pertinent summary, since the contributors proposed ways of improving the project.

From the comments received, it is evident that the idea in itself is seen as **attractive**, but that there are concerns as to the **security safeguards** in view of the nature of the data concerned (personal data).

- Reaction to the project
- Technical securing of the process
- Contractual framework and monitoring
- Protection of personal data

4.1 Reaction to the project

Opinions / Contributions
The FR domain is by no means exempt from abuse, although the level of abuse is **relatively low** compared with other TLDs.
The project presented by Afnic is a solution allowing **the authorities to react faster to cases of abuse.**
This in turn would **relieve Afnic of the** relatively regular and growing **task of collecting and sending data**.
Afnic's departments are remarkably responsive, but the **authorities' independence** in this precise area could allow them to **act faster** and so bring an end to the abuse.

4.2 Technical securing of the process

Opinions / Contributions
Holders need to be given the assurance that this access will be obtained through a secure channel and within a well-defined framework.
The use of **RDAP** with **nominative access**, **dual authentication**, **traceability** of actions and **limitation** of the number of requests, seems perfectly suited to the project.
Authentication and **verification** must be strict (see if authentications could be cross-checked).

4.3 Contractual framework and monitoring

Opinions / Contributions
Require each agent with access rights to **sign an undertaking of responsibility** reiterating the framework and the limits that cannot be exceeded (requests about domains outside the prerogatives of their administration).
Randomly extract some domain names that have been the subject of requests to make sure that they correspond to the prerogatives of the administration (if necessary, consider requiring evidence of this).
Ranking the authorised agents by number of requests could provide an indicator of possible isolated cases of abuse.
In order to safeguard **freedom of expression,** respect private individual holders' **IT rights and freedoms** and avoid potential abuse on the part of the authorities or their representatives, this new procedure needs to be defined and circumscribed as tightly as possible.

4.4 Protection of personal data

Opinions / Contributions
Clarify the **information** to be given **to holders** on this new access to their data. Add to Afnic's general conditions the fact that authorities may have access to holders' particulars.
Inform holders about how they can **exercise their right of access**
Carefully define the **conditions** on which these authorised third parties may **hold data** (duration / internal distribution), security standards, etc.
Undertakings not to disclose or re-use data, to delete them after a certain time, etc.
Need for a **commitment** on the part of the authority to respect the confidentiality of the data made accessible. The data must not be made **public**.
Will holders be **informed** when authorised third parties consult their data?

5.Conclusion

Although few, these responses confirm that the project **is obviously positive as a way of combating abuse** by allowing the authorities concerned to independently identify holders of domain names in the context of their inquiries.

However, the responses are unanimous on the need for vigilance and for the tight definition and control of this mechanism, reminding us of the existence of risks (which we had already identified) and proposing possible solutions aimed at reducing them.

In this respect, it will be interesting to share on our website or via regularly published reports, **statistics** enabling us to **monitor requests** and **measure the effectiveness** of this tool, particularly by establishing, if possible, a correlation with the volume of online attacks or infringements.