Using the RDRS Effectively

Tips for Requestors

Best practices for requests to
ICANN's Registration Data Request Service (RDRS)
for non-public gTLD registration data

ASSOCIATION OF THE INTERNET INDUSTRY

The Registration Data Request Service (RDRS)

ICANN's **Registration Data Request Service (RDRS)** processes requests for access to non-public registration data related to generic Top Level Domains (gTLDs). It is a service for participating ICANN-accredited registrars and requestors. Non-public data can include information such as a contact name, home or email address, and telephone number associated with a domain under a gTLD.

This is a pilot service developed by ICANN and **launched in November 2023** that will run for two years. The pilot project is intended to gather data on the volume of requests for the disclosure of previously published gTLD registration data, which will inform the ICANN Board's decision about building a more comprehensive system. As of mid-April 2024, there were already over 3,500 total requestors and 86 participating registrars.

The RDRS currently covers 57% of all gTLD domains. It does not include ccTLD registration data. Participation is voluntary but strongly encouraged.

There are many benefits for registrars: a centralised platform, one standardised form, and requests can be managed through the existing Naming Services portal (NSp).

As it is a pilot service and is being continuously developed, it is not always straightforward to use. Frequently requested features, such as an API, are being considered but are not yet available. Registrars have to balance the rights of the requestor against the rights of the data subject, and there is no guarantee that you will receive the information you are asking for. However, there are a few things that requestors can keep in mind when using the RDRS to maximise the chances of their request being successful.

Prudence Malinki of MarkMonitor, a requestor, and Sarah Wyld of Tucows, from a registrar's perspective, made several recommendations based on their experience using the RDRS.

Getting your request right

The main reason requests are denied is that they are incomplete. So, first and foremost, explain why you need the data and support your request with salient evidence and correct and coherent information.

- **Justify why your need for the data 'outweighs the data subject's right to privacy'.**
- **If the registrar requests additional information, provide it promptly so they can make their decision without further delay.**
- **Do your research and make sure the data is not already publicly available.**
- **Make sure you identify yourself correctly when submitting your request. It is perfectly acceptable for a domain investor to use the system for research purposes; however, they should identify themselves accordingly.**

Requests are most likely to be successful if they include the following:

- **A clear explanation of who the requestor is and their connection to the domain name being requested.**
- **A succinct description of why the requestor needs the information or some indication of why the issue at hand would be furthered by having the domain owner's personal data.**
- **Details of how the data will be processed, including how the data will be used, how the data will be protected, and when the data will be deleted once the task has been completed.**
- **An attachment with further relevant information can be uploaded if your text is too long for the text box provided.**

The 'expedited' option and emergencies

The 'expedited' option is at the registrar's discretion. There is no guarantee that your request will be expedited. This option should only be used for genuine reasons, and standard requests that misuse it are often rejected.

- An example of a request that should be expedited is a ransomware attack with a deadline for ransom payment.

When expediting your request, you should specify the nature of the emergency. Registrars can and should need to be contacted directly in emergencies that present a threat to someone's life, in addition to submitting a request through the RDRS.

Attach any relevant subpoenas or court orders as PDFs when submitting your request. Make sure you include any deadlines associated with the court order and identify yourself correctly in the "Request Category".

The reason for choosing the 'expedited' option must be valid. While the requestor may be very concerned that a 'famous trademark' is affected and may want to illustrate its importance in detail, this does not necessarily mean the registrar will see this as a reason to expedite a request. Limit the information you provide to what's necessary for the disclosing side to make a legal assessment of your request.

LEA & UDRP

If you are using the RDRS as a law enforcement agency (LEA), stress and repeat this throughout your application, beyond just choosing the 'Law Enforcement' requestor category. Do NOT select the LEA category if you are not a member of a law enforcement agency.

The RDRS is not mandatory for preparing and filing a Uniform Domain Name Dispute Resolution Policy (UDRP) complaint, even though it is one of the requestor categories in the RDRS.

Upcoming developments

As of May 2024, requestor contact details are still optional in the application. As these are required by the registrars, this will soon become a mandatory entry. You can ensure your requests are processed promptly by providing your contact details in the fields which are currently optional.

The RDRS is a pilot project and does not currently cover all TLDs nor any ccTLDs. The system clearly indicates in the application process which TLDs are currently excluded (e.g., .mil, .int, .arpa, .gov, .edu, ccTLDs). As more registrars join the platform, more TLDs will be added to the RDRS.

A recording of the webinar "RDRS – How to access WHOIS data today" is available.

For more resources on how to use RDRS, visit the RDRS page on ICANN.org. If you are looking for publicly available non-personal registration data, use ICANN's lookup tool at https://lookup.icann.org.

1. Explain your request and provide all relevant details

- Clearly articulate why you need the data, providing evidence and relevant details.
- Justify why your need for the data surpasses the privacy rights of the data subject.

2. Include all essential information

- Identify yourself and your connection to the domain name.
- Offer a concise rationale for needing the information and how it relates to the issue at hand.
- Outline data processing details: usage, protection measures, and deletion timeline post-completion.
- Attach PDFs with additional information, if necessary.

3. Utilize the 'expedited' option wisely

- Understand that expedited processing is at the registrar's discretion and should only be used for genuine emergencies.
- In emergencies, direct contact with registrars is advised, in addition to RDRS requests.

4. Attach relevant legal documents for expedited requests

- Include relevant subpoenas or court orders as PDFs, specifying any associated deadlines.

5. Limit the information you provide to relevant details

- Provide only necessary information for the registrar to legally assess the request, even in cases involving famous trademarks.

6. Law Enforcement Agency (LEA) requests

- If requesting as an LEA, emphasise this status throughout the application.

Remember, the success of your request heavily depends on the quality and completeness of the information that you provide to the registrar via the RDRS. These best practices aim to improve the likelihood of obtaining the necessary non-public gTLD registration data.

eco
ASSOCIATION OF THE INTERNET INDUSTRY

eco – Association of the Internet Industry
Lichtstrasse 43h, D-50825 Cologne, Germany
phone +49 (0) 221 / 70 00 48 – 0
fax +49 (0) 221 / 70 00 48 – 111
info@eco.de
international.eco.de