Frequently Asked Questions (FAQs) for the Registration Data Request Service (RDRS) Naming Services portal (NSp) for Registrars

Version 1.1

ICANN
7 November 2023

TABLE OF CONTENTS

General

Please refer to the RDRS Requestor FAQs for these questions and answers.

Click here to access the RDRS NSp User Guide for Registrars.

Access

How do I access the RDRS portal?

Participating registrars will access the RDRS via the Naming Services portal (NSp).

How do I enable email encryption and PGP usage?

From the Registrar 'Persona' in the NSp, you can navigate to your Registrar Group settings (where you currently maintain Invoice Delivery and Group Invoicing preferences) by clicking on the Registrar Group name on the home screen. From there, in the top right corner, you can click on 'Update Account'. You will be presented with a screen where you can select 'PGP Enabled' and enter the PGP Key in order to receive encrypted emails for all RDRS requests submitted for IANAs in your group. While you may enter the PGP Key information during the registrar's early onboarding, the actual encrypted email functionality will be made available at the time of the launch in November 2023.

Can I add additional NSp users to respond to requests via the RDRS portal?

Yes, additional NSp users can be added. If you would like to add a user that is limited to only see RDRS requests, the Registrar Primary Contact should contact ICANN Global Support at globalsupport@icann.org with the request and provide the first name, last name/surname, an email address, and phone number of the person to be added to the NSp.

Using the NSp RDRS Portal

How do I use the bulk processing feature?

Registrars will be able to select multiple requests from their Pending list view and click the Bulk Update button to enable in-line editing on each request. From the Bulk Update screen, you will see some details of the request (domain subject, requested date, request category, priority, data requested, etc.) and are able to update the Response Date and outcome of the request (Approve/Deny/Data Publicly Available/etc.) including Denial Reason and Explanation as applicable. Don't forget to click Bulk Update afterwards to save your changes.

What are the advantages of setting up the PGP key?

By setting up the PGP key, registrars are able to receive the nonpublic registration data request in its entirety, including attachments, via an encrypted email. This will allow registrars to only login to the NSp periodically to report the outcome of requests.

How do I opt out of RDRS if I no longer wish to use it?

The RDRS allows a simple step to opt out of the system. You can simply uncheck the 'RDRS Enabled' box under your IANA Details. Note: You need to be in the Registrar Persona (top left corner) to access this setting). Once you opt out of the RDRS, requestors are no longer able to submit any data disclosure request for domains under your management and will be encouraged to contact you directly outside of the RDRS.

Registrars are still required to respond to any requests that were submitted in the RDRS prior to the opt out date per the applicable provisions under the Temporary Specification and/or gTLD Registration Data Policy. Additionally, please mark the disclosure outcome in the RDRS.

Will I receive an individual notification email for all my registrars?

No, for ease of use, RDRS users will receive a single Daily Activity Notification and Pending Request Summary emails that aggregate all RDRS requests for all registrars that belong to your registrar group.

Responding to Requests

How do I see the request details?

Once you have opted-in to the RDRS, registrar NSp users will start to see data disclosure requests in a list view in the RDRS persona in the NSp. You can click each request to see the request details.

Who determines whether the requested data should be disclosed to the requestor?

Registrars are solely responsible for assessing the request and making the decision of whether to disclose the requested nonpublic registration data.

How do I disclose the requested data to the requestor?

The RDRS does not support data disclosure. If you determine that the requested data can be disclosed, you should contact the requestor via the contact information provided in the request form and proceed with the disclosure per your chosen method.

Do I need to do anything in the RDRS after the determination is made?

Yes. After you have reviewed and responded to a request that was made through the RDRS, you should mark the request with the appropriate outcome in the RDRS to complete the request. This step is particularly important as the purpose of the service is to collect accurate usage data.

What do the various disclosure outcomes mean?

The available outcomes for data requests are:

- Approved: All requested data was disclosed to the requestor.
- Partially approved: Only some of the requested data was disclosed to the requestor.
- Denied: All requested data was not disclosed to the requestor.
- Data publicly available: Registrar found the requested data is publicly available.
- Canceled: Data request was canceled before the disclosure decision was made.

For more detailed information, please refer to the RDRS NSp User Guide for Registrars.

What if I need more information or clarification from the requestor?

If you need to communicate with and seek additional information or clarification from the requestor to appropriately respond to a request, that communication must occur outside of the RDRS using the contact information the requestor provided in the request.

What happens once I mark the disclosure outcome in the RDRS?

Once you mark a disclosure outcome in the RDRS, the system notifies the requestor and the request remains visible to both you and the requestor.

Who can see the full request data aside from registrars and requestors?

With data security governance in mind, the RDRS will provide access to limited ICANN staff who have legitimate reasons, such as system operations and maintenance, customer support, and complaint investigations.

How will I be notified of new requests and keep track of pending requests?

You will receive the following email notifications pertaining to new, pending, and canceled requests and will be asked to login to the NSp to mark their decisions and resolve such requests:

- **Daily Activity Notification:** will include any new or recently canceled requests from the previous day.
- **Pending Request Summary**: will include all pending requests submitted more than 30 days prior.

How can I correct an error made logging a disclosure decision in the RDRS?

If you believe you have made an error logging the decision in the RDRS, or if a requestor has flagged a discrepancy with you after logging a decision, you can reach out to ICANN Global Support for options.

Compliance-Specific Questions

Can I require all requests to come through the RDRS rather than accepting some directly?

Neither the Temporary Specification nor EPDP Phase 1 specifically prohibits registrars from establishing a mechanism and process for submitting disclosure requests that directs requestors to submit requests through the RDRS. For example, you may choose to use the RDRS as your primary way to receive nonpublic data requests by including the RDRS URL on your webpage that explains how to make disclosure requests. However, when establishing processes, you must consider applicable law and regulations, as well as any additional requirements set forth in future policies beyond those that pertain to methods of intake.

Will ICANN Contractual Compliance use the RDRS as a part of its enforcement work?

ICANN Contractual Compliance will have visibility to requests made in the RDRS as a means of validating complaints that are submitted by requestors. However, ICANN Contractual Compliance does not intend to access requests as a means of proactive monitoring or enforcement.

If registrar participation in the RDRS isn't required, how does the RDRS impact current contractual requirements?

All requests submitted through the RDRS will be subject to the applicable disclosure requirements under the Temporary Specification and/or gTLD Registration Data Policy for registrars that have opted into the service. In other words, if a requestor submits a request via the service, the participating registrar must review the request considering the current requirements. For example: providing reasonable access, balancing the parties' interests (if applicable), responding to the request, adherence to response time requirements, etc.

However, opting into the RDRS, accepting responses via the service, and logging of responses in the service alone will not demonstrate compliance with the Temporary Specification or future EPDP Phase 1 requirements. For example:

- Opting in does not demonstrate that a registrar has reviewed each response and balanced the parties' interests, if required.
- Logging a response does not demonstrate that the response was sent to the requestor and/or included the necessary information.

Will registrars be expected to respond to UDRP/URS provider verification requests, including domain name lock requests, made via the RDRS?

Registrars participating in the RDRS are obligated to review and respond to all disclosure requests. UDRP and URS providers will be able to use the RDRS for investigative or research purposes. ICANN org is advising UDRP and URS providers to continue to contact registrars directly with official UDRP and URS verification requests and domain name lock requests.