Dear Contracted Party,

As we indicated on 21 November 2024, conformance with the Registration Data Access Protocol (RDAP) specifications (both the RFCs and the ICANN gTLD RDAP Profile) is still very low among the contracted parties and jeopardizes a coherent ICANN Registration Data Directory Service (RDDS). Please reference the 21 November email for further details of the issues.

The functionality of RDDS for internet users is a critical responsibility of ICANN and its contracted parties. As such, ICANN is requesting you prioritize the following aspects of your RDAP service to ensure general usability ahead of the 28 January 2025 "WHOIS Sunset Date". ICANN's Contractual Compliance team is prioritizing these aspects of the RDAP service as part of ICANN's RDAP enforcement efforts.

It is recommended that you test for the following set of requirements to ensure that your RDAP service may be considered generally usable (not to be confused with fully compliant):

1. HEADERS: Your RDAP service MUST return an "access-control-allow-origin" (CORS) header. The gTLD RDAP profile (per the Technical Implementation Guide, section 1.13 of the 2019 version, section 1.14 of the 2024 version, respectively), requires the servers to always return an "access-control-allow-origin" header, but it has been discovered that some RDAP services only return this header when the request has an "origin" header. An absent or misconfigured "access-control-allow-origin" header will prevent RDAP clients running inside of web browsers from accessing an RDAP server. You can test this with the "curl" utility, which is found on most Linux systems and available for MacOS and other operating systems.
2. PARSABILITY: Your RDAP service provides responses that can be parsed and generally recognized as RDAP according to RFC 9083, per Section 1.1.2 of the Registration Data Directory Services (RDDS) Specification of the 2013 Registrar Accreditation Agreement. You can test this with the ICANN RDAP CLI. While this client does flag some conformance issues, it will only return a non-zero exit code if it cannot establish a connection and cannot retrieve RDAP-formatted JSON. As this is a general purpose client, it is as lenient as possible with regard to RFC 9083 conformance.
3. SECURE TRANSPORT: Your RDAP service MUST be provided over HTTPS (e.g., not over HTTP; per the Technical Implementation Guide, section 1.2 of the 2019 version, section 1.4 of the 2024 version, respectively) using TLS 1.3, or TLS 1.2 with the recommended Cipher Suites per RFC 9325, which is the successor of RFC 7525 (per the Technical Implementation Guide, section 1.3 of the 2019 version, section 1.5 of the 2024 version, respectively). The TLS server certificate is valid (e.g., is not expired) and follows the recommendations in RFC 9325. You can test these with SSL Labs or OpenSSL.

Addressing the aspects identified above ahead of 28 January 2025 will help ensure the RDDS system continues to be generally usable for Internet users, but does not address full compliance with RDAP requirements in your Registry Agreement and/or Registrar Accreditation Agreement. Once general usability is addressed, you will need to bring your RDAP service into full compliance with the RDAP requirements detailed in STD 95 and the 2024 gTLD RDAP Profile by 21 August 2025.

If you have any inquiries regarding compliance to the RDAP specifications, please send them to globalsupport@icann.org.

ICANN will monitor the landscape of compliance with RDAP during the first part of January 2025 and will send additional communications with the status of compliance to RDAP.

Regards,
GDS Technical Services
Internet Corporation for Assigned Names and Numbers (ICANN)