

Registrar Stakeholder Group response to RDS WHOIS2 Review Team Final Report

<https://www.icann.org/en/system/files/files/rds-whois2-review-03sep19-en.pdf>

The Registrar Stakeholder Group (RrSG) is pleased to comment on the Registration Directory Service (RDS) WHOIS2 Review Team Final Report. However, as it does not differ in any significant way from the draft report published in September 2018, the extensive comments which the RrSG provided at that time¹ still apply. It is also a given that this report is coming too late following the adoption of GDPR and other data protection laws.

The RrSG would like to highlight it's key remarks from our previous comment:

- Comment (rec 1). The RrSG believes it is appropriate for there to be greater foresight and overview of RDS within ICANN and that this role and the responsibilities be properly assigned.
- The RrSG generally supports this recommendation (rec 1.2), but also suggests that such updates also be provided to the GNSO council to enable it to initiate timely policy development processes where necessary.
- Comment (rec 2). The RrSG believes it is curious that the RDS-WHOIS2 RT has categorized this recommendation as fully implemented given their findings are very similar to that of the first RT. While there is a collection of any number of policies related to WHOIS, and those policies now reside in a more singular space, ICANN Board has NOT created a single WHOIS policy document. At best this recommendation is only partially implemented.
- Support (rec 3.2), however the costs for such outreach should not increase the ICANN budget
- Comment (rec 4). The recommendations are not supported by corresponding data. The reviewed data does not seem to indicate the existence of “systemic issues”.
- Do not support (rec 4.1). Given the advent of numerous privacy laws, the RrSG views this recommendation as creating more risk by trying to place ICANN Compliance into a more investigative mode, digging through data without justification. Compliance action should be targeted at issues raised by reporters. RDS accuracy is an obligation of the registered name holder (RNH). It is not the role of compliance to enforce RNH obligations. This recommendation is not supported by any data that shows that such systemic issues actually exist, so without a problem, no solution is needed.
- Support Depends (rec 4.2). The RrSG would like to understand better how ICANN Compliance would be detecting “patterns of failure”. As ICANN

1

<https://mm.icann.org/pipermail/comments-rds-whois2-review-04sep18/attachments/20181118/9e7c200e/RrSGresponse-RDS-WHOIS2ReviewDraftReport-InputForm-0001.pdf>

Compliance already conducts audits on registrars who have proven to have a track record of non-compliance, it's unclear how this recommendation differs from the current practice and what the RT is envisioning. The current language is very broad and interpretation could easily lead to increased, unnecessary audits of registrars. Given the complexity of the Audit program and the amount of time and effort required for both ICANN and the affected parties, additional Audits outside the Audit program should only be triggered upon discovery of actual evidence of non-compliance, not for fishing-expeditions to detect potential non-compliance.

- Comment (rec 5.9) We remind ICANN that data accuracy is achieved by providing our customers the tools/rights to access, correct and/or update their information and by establishing internal processes and procedures that ensure the data provided by our customers remains accurate and complete. Article 5(1)(d) of the GDPR does *not* require we poll our customers to ensure the data they have provided themselves as part of the underlying transaction was in-fact accurate. Any suggestion to the contrary is a misinterpretation of the GDPR. Furthermore, since the signing of the 2013 RAA, Sections 1(a-d) as well as 1(f) of the of the Whois Accuracy Program Specification have been implemented. Implementation of these five sections has resulted in near perfect address accuracy and contactability rates. As of January 2018, postal address operability is 99% and postal address syntax accuracy is 88% (up from 80% three years earlier). ICANN's own key findings include that "nearly all WHOIS records contained information that could be used to establish immediate contact: In 98 percent of records, at least one email or phone number met all operability requirements of the 2009 RAA."
- Support depends (rec 5.1) From the RrSG's perspective, this recommendation begs the question, to what end? What purpose does this recommendation serve? If a ticket is created because the WHOIS is deemed inaccurate, and then the ticket is closed because the WHOIS changed, is that not the outcome sought? Additionally, the report notes that 81.6% of tickets are closed after the 1st notice due to the registration being cancelled or suspended and it is then inferred that this is because the data was intentionally entered incorrectly, because why else would you not update the info? This conclusion is simply wrong as there are any number of reasons why the data may not be updated. For example, one could purchase a domain with the intent to use it, but then a life change happens, be it a divorce, or family crisis, or change in job, and this change could result in a new address. You then receive a notice asking for the data to be updated, but you had already decided, based on the change in your circumstances, that you were going to allow the domain to drop, so you don't take any action and allow the domain to be suspended/canceled. This is a reasonable sequence of events, and making assumptions that every instance of inaccurate data or unexplained data element is evidence of something nefarious is not supported by any data or facts. The RT seems to draw conclusions from thin air instead of accepting the most reasonable explanation that due to the time lag between the data query in the ARS

program and eventual compliance review the cause is most likely simply the passage of time. The RrSG is of the opinion that recommendations should address actually existing issues that are evidenced by data instead of initiating fishing expeditions. We also note that we consider it highly doubtful that the ARS program can be resumed under the GDPR and other applicable privacy legislation as it requires ICANN accessing and processing non-public personal information for no valid purpose.

- Do not support (rec 10.1). The RrSG believes this recommendation seems to overlook that Privacy/Proxy is a SERVICE, same as email, and therefore the underlying customer information is already being verified and validated by the registrar. In essence this is requiring the customer info to be verified/validated twice, which adds no value. The RrSG also rejects the notion of a recommendation dictating contractual language. Contracts are the sole remit of ICANN and the contracted parties.
- Support depends (rec 11.2). At first look it feels to the RrSG like there is more risk associated with this recommendation than any resulting benefit. However, if ICANN org plans to be the sole controller of this common interface and will be responsible/liable for pulling the data to create it (presuming the data is being correctly displayed in the first place (meaning not PII)), and they are comfortable with risk and their ability to comply with applicable laws, then OK. That said, we appreciate the apparent intent of ensuring that the common interface provides both registry and registrar RDS outputs as these may currently differ under the Temp Spec, thereby reducing the potential of confusion with the users of the interface.
- Comment (objective 3). We encourage the use of outside facilitators to draft and conduct surveys to ensure that results or questions are not biased towards the interests of any particular group.
- Comment (rec LE.1). We note that LEA needs in the past often seemed to go beyond the scope of RDS services provided by contracted parties and relied on the use of third party data mining/data scraping services, so surveys may not correctly reflect the effectiveness of RDS services alone.
- Do not support (rec LE.2). The RrSG cautions against including parties who work with LEAs in any survey or attempting to equate the needs of those who work with LEA to the actual needs of LEAs. The expansion of such a survey to third parties that have not been empowered by regulation or statute with legal enforcement or investigatory powers and legal rights is highly dubious as the legitimacy of such parties is not equal to that of LEAs even though they may provide useful services. LEA only have powers within their territory/local jurisdiction and registrars/registries must follow the rules of law within their jurisdiction(s). While some LEAs may have mutual cross agreements between countries, these agreements and authority do not extend to third parties. There are no global LEAs, only local LEAs.
- Comment (objective 5). The RrSG has no issue with these requirements, with the assumption that any update of the contracts will not be extended to anything outside of them. Such requirements should be general, not specific and merely reference best practice legal regulations such as the GDPR. For example, a reference that under the GDPR, contracted parties would already be bound by appropriate requirements would be sufficient as implementations

of applicable laws may vary and ICANN dictating one particular implementation model may be onerous.

- Support (rec CM.1), however, we reject the notion of the RT dictating contractual terms.
- Do not support (rec CM.2) The RrSG views this as very problematic. The ARS studies have shown that the number of grandfathered domains is already decreasing steadily on its own, illustrating that there is no strong need for a complete removal of grandfathering privileges for pre-2013 RAA domain names, which would create significant implementation issues for both registrars and registrants. The terms of the 2013 provisions were negotiated by ICANN and the RrSG under consideration of the realities of the domain business and difficulties in having to reach out to existing customers. The RT also does not demonstrate any reasonable fact-based need for removing the grandfathering rules. If an existing registration that predates the adoption of the 2013 RAA by the sponsoring registrar is not causing any issue, there needs to be a compelling reason to impose sanctions. The presumption that sufficient time has passed since the adoption of the 2013 RAA is erroneous as registrars have been adopting the new RAA over time, not at the time it was introduced by ICANN.
- Support (rec CM.3). The RrSG has doubts, however, that the Inaccuracy Reporting Function will remain viable in their current form under data privacy regulations as such data is no longer publicly accessible. As such, any review or study of this tool may be a misuse of resources.
- Comment (rec CM.4). It is unlikely that the use of a bulk reporting tool referenced in recommendation 4 will be compliant under GDPR or other applicable data protection regimes as bulk access to this data has become impossible/illegal too.
- Comment (bylaws). The RrSG takes no issue with the bylaws being updated, however, it should be ensured that the data safeguards remain part of the revised language.
- The RrSG notes that only a select number of LEAs, ie those that had a direct relationship with the GAC and members of the Review Team, participated in the questionnaire and so the results do not necessarily reflect the views of a full cross-section of national and local LEAs around the world.