# RDS PDP WG Poll on Purpose - 13 December
# Results as of 19 December 18:00 UTC

During the 13 December RDS PDP WG call, we started deliberation on the following charter question/sub-question:

*2. Who should have access to gTLD registration data and why?*
*2.1 Should gTLD registration data be accessible for any purpose or only for specific purposes?*

To seek common ground, we started by focusing on "thin data" as defined by the Thick WHOIS Report ("A thin registry only stores and manages the information associated with the domain name. This set includes data sufficient to identify the sponsoring registrar, status of the registration, creation and expiration dates for each registration, name server data, the last time the record was updated in its Whois data store, and the URL for the registrar's Whois service.") To apply this charter question to "thin data" only, we also discussed: *What is the purpose of "thin data" about gTLD domain names?*

The following poll gives all WG members an opportunity to share opinions about concepts that surfaced during this call. Poll responses received by **19 December 18:00 UTC** have been aggregated below and will be used as input to the next WG call.

**Q1) During the WG call, it was suggested that sub-question 2.1 (above) be teased apart to allow for other possibilities. Which of the following alternative statements (if any) do you agree with?**

| | |
|---|---|
| **18.2%** | a) "Thin data" about gTLD domain names should be accessible for any purpose(s), except for illegitimate purpose(s) expressly prohibited by policy. |
| **40.9%** | b) "Thin data" about gTLD domain names should be accessible for legitimate purpose(s) only, as expressly permitted by policy. |
| **9.1%** | c) "Thin data" about gTLD domain names should be accessible for any purpose(s), without being limited by purpose or taking purpose into consideration. |
| **0.0%** | d) No "thin data" about gTLD domain names should be accessible, period. |
| **20.0%** | e) "Thin data" about gTLD domain names should be accessible to all users anonymously and without any declaration of purpose, with illegitimate uses expressly prohibited. |
| **4.5%** | a) and b) Some thin data elements should be accessible for any purpose(s) except for illegitimate purposes and others should only be accessible for legitimate purposes. |
| **4.5%** | b) and c) Some thin data element should be available for any purpose, but others should only be available for specific purposes as expressly permitted by policy. |
| | Total Responses = 22 |

**Q2) Please elaborate on your answer to poll question Q1 above, sharing your rationale for why purpose should or should not impact policies associated with access to "thin data" about gTLD domain names. The comment box below may be used, for example, to give any assumptions you made when supporting or not supporting a listed Q1 option, or any alternative(s) that you prefer to those listed under Q1.**

| |
|---|
| Thin data about gTLD domain names should be accessible to all users anonymously and without declaration of purpose, with illegitimate uses expressly prohibited by policy. |
| It would be a missed opportunity if, on the basis of the replies to these questions, we would not define a purpose for the collection / use of thin data. The definition of a purpose for the collection / use of thin data would help us to specify the particular data elements, and would help us and others for further iterations of the work, e.g. where it is considered to add new data elements. Therefore, I would argue for defining (a) legitimate purpose(s) for the collection / use of thin data, albeit a rather general / high-level purpose in order to allow for the rather broad use of thin data. When discussing data elements that could be considered as personal data (which I believe are currently not considered as part of thin data), a more specific and explicit purpose would have to be defined. |
| Reliable Whois data is a valuable research tool for troubleshooting DNS issues and broader research into registration patterns. Thin Whois data does not need to include any PII data to be valuable, simply technical data relevant to a donain. |
| Under basic privacy policy principles, people provide data about themselves - and consent to it being public - based on their consent to the uses for which the data will be available - so they should be able to know what those uses are. |
| I agree with Greg's rationale for now. |
| Need to balance transparency with privacy. Thin data typically includes no personally identifiable information, so the balance weighs in favor of having that info be public, and any use of that info permitted except illegal uses |
| We need the policy to follow universal data protection principles. |
| While admittedly still grappling with this question, I am currently thinking that I would choose a) and b) for question 1, i.e., it may be that some thin data should be accessible for any purpose(s) except for illegitimate purposes and some should only be accessible for legitimate purposes. |
| Most of information provided in Thin Data may be used later to launch attacks (social engineering, scam, spam, etc.). Restricting the access to these details will diminish this kind of abuse. |
| "Thin data' about gTLD domain names should be accessible to all users anonymously and without declaration of purpose, with illegitimate uses expressly prohibited by policy." |
| Any sort of data should only ever be available for _legitimate_ purposes |
| I agree with the commentary in email regarding existing Thin Data remaining status quo. 'Thin data' about gTLD domain names should be accessible to all users anonymously and without declaration of purpose, with illegitimate uses expressly prohibited by policy. |
| It is inappropriate, and constitutes the exercise of too much power, for ICANN or a related entity to, on a global scale, deign to tell internet users what an appropriate or inappropriate purpose is, either for thick or thin data. ICANN or a related entity (including this group) cannot possibly foresee every possible purpose for using this data. Moreover, there simply isn't any rationale for not making this available. |
| None of the above. All appear too restrictive. "Thin data' about gTLD domain names should be accessible to all users anonymously and without declaration of purpose, with illegitimate uses expressly prohibited by policy." If this is judged to be identical to option (c), please aggregate this answer with that one. (Note that it's unclear whether (c) will ask for a declaration of purpose or identification of the requester, even if purpose is not taken into consideration.) |
| None of the above. I suggest another option, which is the current status quo with WHOIS, and was discussed in the 13 December call. My suggestion is: "Thin data' about gTLD domain names should be accessible to all users anonymously and without declaration of purpose, with illegitimate uses expressly prohibited by policy." The four options in the poll require users to declare a purpose or identify or authenticate before receiving access. They all assume that purpose DETERMINES whether access will be granted. The use of "accessible" in those four options was sometimes not qualified enough, and creates problems. |
| While each of the specific data items may or may not be important, the general picture of non-personal data that is useful for certain purposes related to name registration is a good one. Rather than try to come up with some "prohibited" uses, the simplest solution is to keep it completely free (both as in speech and as in beer). |

RDS PDP WG Poll on Purpose - 13 December
Results as of 19 December 18:00 UTC

| |
|---|
| It is my opinion that "purpose" needs to be further developed as a key concept.  It seems odd to me to talk about accessibility when we don't know if the data is available because we don't know if we collected it because we don't have a defined purpose for collecting it. |
| I do not agree with any of the statements. I believe that *some* thin data elements (those that are available via the DNS, for example) should be available for any purpose, but other thin data elements should only be available for specific purposes as expressly permitted by policy. This seems to be somewhere in between options b) and c). |
| Despite not being as protected by law as thick data, there seem to be good reasons of also requiring legitimate purposes for thin data as such data is regularly abused by third parties, such as previously discussed on the mailing list. Unless there is an immediate and obvious need for publicity of such data, it seems prudent to protect such data against abuse as well, especially since those parties that should have access to this data (registrant, registrar and registry) will have it by design through various existing reminder policies or by technical design. |
| Total Responses = 19 |