RECOMMENDATION 12

The EPDP Team recommends that the current requirements in the Temporary Specification in relation to reasonable access remain in place until work on a system for Standardized Access to Non-Public Registration Data has been completed, noting that the term should be modified to refer to "parameters for responding to lawful disclosure requests." Furthermore, the EPDP Team recommends that criteria around the term "reasonable" are further explored as part of the implementation of these policy recommendations addressing:

- [Practicable]* timelines criteria for responses to be provided by
- Contracted Parties;
- Format by which requests should be made and responses are provided;
- Communication/Instructions around how and where requests should be
- submitted;
- Requirements for what information responses should include (for
- example, auto-acknowledgement of requests and rationale for rejection
- of request);
- Logging of requests.

[*Some concern expressed that timeliness that should not be translated into requirements that are impractical for contracted parties].

Disclaimer: *This overview has been developed to facilitate the EPDP Team's consideration of the concerns expressed and possible updates to the recommendations. However, this does not replace the EPDP Team's obligation to review all input received in full and to indicate if any concerns in this overview have inadvertently been mischaracterized.*

Noted Concerns

Concern	Corresponding PCRT Comment #	Further Discussion Required?
The EPDP Team's work is incomplete until the issue of setting parameters and recommending a process for responding to lawful disclosure requests to redacted data has been resolved. the EPDP Team should now also define and develop simple processes around "reasonable access" and make sure that implementation details of these processes are completed within this EPDP and not delayed until future discussions regarding implementation. "Reasonable access" must be defined in a complete and holistic fashion. In the absence of a definition, every registrar must define their own standard of reasonableness, and this has generally resulted in no access at all.	5, 6, 9, 10, 11, 14, 15, 19 (Coalition for Online Accountability, INTA, BC, Microsoft, IPC, MPAA, Walt Disney Company, MarkMonitor)	Yes/No
It is simply not the case that a party's status is sufficient to be provided with full access to all personal data. Each request for access must include justification and be reviewed individually, understanding the balance between the right of the requestor for access to personal data where appropriate and the natural person's right to privacy. This is a balancing test and will, necessarily, be different in each case.	7 (Tucows)	Yes/No
It it is important to provide a means for multiple queries, particularly when pivoting off fields in an investigation, and reverse Whois, which is critical for cybersecurity investigations. Moreover, there should be a means for expedient access in certain circumstances, such as a global cybersecurity attack. To the extent queries are logged, there should be guidance for how this will work, what would be included in the logs, and permitted uses of the logs.	8 (Europol AGIS)	Yes/No

Premature to be discussing "Access recommendations" until the gating questions have been answered. Repeated efforts by some EPDP Team members to focus on access to, and/or disclosure of, data in the initial phases of the EPDP's work has significantly hampered the group's ability to make progress on the core issues of defining purposes for data collection and the roles and responsibilities of parties. The Charter explicitly states that data access questions are to be addressed in the second phase of the EPDP. Therefore, inclusion of this recommendation, as written, is premature and serves to predetermine the issue to be discussed.	12, 24 (John Poole, RySG)	Yes/No
The criteria provide much needed predictability and clarity around the obligation of "reasonable access" including what the process and expectations for requesting and providing access need to be.	13 (NTIA)	Yes/No
The current "requirements" are so vague as to be unworkable and unenforceable. there do need to be more specific, measurable, enforceable requirements of the kinds contemplated in Rec 12. At minimum, the following are easy to implement immediately: 1) Links and instructions for data requests must be placed on registrar and registry operator web sites 9just like they are required to have abuse links and contacts on home pages per the ICANN contracts.) 2) Contracted party must provide written acknowledgement of receipt of the request, and 3) must return a written response with either the data or the reason for the rejection, within three days.	16 (iThreat Cyber Group)	Yes/No
Timelines should also be made for allowing opt-in by registrants to public WHOIS.	17 (George Kirikos)	Yes/No
It is unclear what the ALTERNATIVE is to continuing to use the current methodology.	18 (ALAC)	Yes/No
This recommendation should be rewritten to make the distinguish between law enforcement requests, private party disclosure requests, and pseudonymized access for research purposes. The legal bases for	20 (GoDaddy)	Yes/No

these three use cases are different. Also, this approach will also be driving by whether ICANN or contracted parties will be required to fulfill disclosure requests. Additionally, it is important to note and emphasize that "reasonableness" does not refer to the ease of access, but rather must take into consideration whether such access is lawful, because nothing is reasonable if it creates legal liability for the Contracted Parties.		
Each registry and registrar should be able to evaluate to whom they may disclose personal data. There are local laws to take into consideration, as well as any data privacy legislation. It would be impossible to have a blanket order to disclose personal data as it would depend on the requestor.	21 (RrSG, Volker Greimann, Michele Neylon)	Yes/No
Replace "Standardized Access to Non-Public Registration Data" with "parameters for requesting lawful disclosure requests," as that more accurately describes the objective. It will simply be insufficient to state a mere category of request for data, e.g., "intellectual property allegation" or "law enforcement need." The requirements of GDPR dictate that prior to revealing the personal and sensitive data of registrants, there is an evaluation that must take place.	23, 26 (Domain Name Rights Coalition, NCSG)	Yes/No
Internet infrastructure providers have a gateway function - there is an imbalance of informational power that must be rectified by transparency and due diligence by the providers. From the viewpoint of a third party with legitimate requests, there should also be the possibility to object to decisions by infrastructure providers not to provide requested information. These decisions are often haphazard and inconsistent with transparency recommendations.	25 (VAP)	Yes/No
The timeline criteria provided by contracted parties may differ from one contracted party to another based on each party's data infrastructure and overall organizational factors. Instead the timeline criteria could be provided by ICANN which could act as a single contact point for access	27 (Sivasubramanian Muthusamy)	Yes/No

requests which it could process in accordance with the policy that it is developing by its multi-stakeholder global process. Even the data access could be granted from ICANN Compliance database / escrow , by privilege levels as determined by the class of requester and the nature of request. Such a process may remarkably reduce the burden on Registries and Registrars and would also considerably ease the processes for the Requester who would otherwise have to request access from multiple Registries and Registrars, each in a different geographic location.		