Registries Stakeholder Group Statement

Issue: **Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2**

Date statement submitted: **14 April 2020**

Reference url: https://www.icann.org/public-comments/epdp-phase-2-initial-2020-02-07-en

The Registries Stakeholder Group (RySG) welcomes the opportunity to provide feedback on the Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2. The RySG appreciates the willingness of the EPDP Team to allow, due to recent events, anyone who was unable to submit their input on the EPDP Team's Initial Report by the initial deadline of 23 March, to submit comments by 3 May 2020.

EPDP On the Temporary Specification for gTLD Registration Data - Phase 2 - Public Comment Proceeding Input Form

1. **Email address**
2. **Please provide your name:** Samantha Demetriou, RySG Vice Chair, Policy
3. **Please provide your affiliation** Registries Stakeholder Group (RySG)
4. **Are you providing input on behalf of another group (e.g., organization, company, government)?** Yes
5. **If yes, please explain:** Comment on behalf of the Registries Stakeholder Group (RySG)

Recommendation #1: Accreditation

Please find a link to the text of Recommendation 1 here:
https://docs.google.com/document/d/1Mq8T1EBcQhbKnCBcVwYtb3qKDIgJcOClu5G0NaNaO50/edit .

7. **Please choose your level of support for Recommendation #1:**

Support Purpose as written
Support Purpose intent with wording change
[✓ Significant change required: changing intent and wording]
Purpose should be deleted
No opinion

8. **If your response requires an edit or deletion of Recommendation #1, please indicate the revised wording and rationale here.**

Change d) to reflect Registrars are the disclosing entity: “d) The decision to authorize and disclose registration data (….) will reside with the Registrar.’

Whereas a Registry may be required to assess a disclosure request in limited circumstances, vis a vis the SSAD, it should not be considered a primary source for disclosure. A process whereby an upheld ICANN compliance action resulting from the non-response or other procedural defect in a registrar’s response may authorize escalation to a Registry operator for their review; however, this has not been adequately defined to date by the team and requires further thought.

It is clear that nothing in this document will prevent a third party from requesting such data directly from the registry (or registrar) (i.e. not via the SSAD), and via a process to be established by the Registry; it must be clear however that where multiple requests are made to both SSAD and Registry/Registrar, this should be considered as an aspect of the relevant review of the request. A Registry/Registrar must be able to query the SSAD for similar requests made to the SSAD, and any attempt of forum shopping or indicators where previous requests have been denied by the SSAD should be considered in any decision

f) is overly prescriptive - there are different ways this functionality can be accomplished; this language unnecessarily restricts the implementation.

g) Change to “Signed Assertions MAY convey (if used) ....” to provide flexibility to the implementor.

I) is not clear: Is this code of conduct applicable to the operator(s) of the SSAD? The accreditation authority? Need to clarify the intent.

u) We assume that the brackets around [cooperate with any audit or information requests as a component of an audit;] is a drafting error but request to confirm that the brackets are not significant.

No discussion in the accreditation recommendation regarding renewal (accreditation for public entities requires renewal “periodically”).

Recommendation #2: Accreditation of governmental entities

Please find a link to the text of Recommendation #2 here:
https://docs.google.com/document/d/1NOTbh3PeQSaDr3O4GKjGjJPHgpB3bVIMTyJvz7pzpsU/edit .

9. **Choose your level of support of Recommendation #2:**

[✓ Support Recommendation as written]
Support Recommendation intent with wording change
Significant change required: changing intent and wording
Recommendation should be deleted
No opinion

10. **If your response requires an edit or deletion of Recommendation #2, please indicate the revised wording and rationale here.**

Recommendation #3: Criteria and Content of Requests

Please find a link to Recommendation #3 here:
https://docs.google.com/document/d/1_w7EJHo4RzPtRis-zKgyJ4GzmY3KvGjk_-o03n7Yuzk/edit .

11. **Choose your level of support of Recommendation #3:**

Support Recommendation as written
[✓ Support Recommendation intent with wording change]
Significant change required: changing intent and wording
Recommendation should be deleted
No Opinion

12. **If your response requires an edit or deletion of Recommendation #3, please indicate the revised wording here.**

Criteria is missing an element for the requestor to indicate whether the request is confidential (potentially covered under Request type but the example used there is “Urgent”)

Criteria should not limit Controllers from requiring additional information if necessary to make these decisions, and these criteria should be subject to evolution as Contracted Parties receive and evaluate actual requests.

B – It does not seem clear that all accreditation information is needed for the disclosing entity – just the accreditation status doesn’t seem enough. The SSAD system itself should know about accreditation… the requestor logging in should be enough… the requestor shouldn’t have to enter accreditation info every time.

Doesn’t seem clear that accreditation information will be passed to the disclosing entity… this is a critical component of the SSAD.

Recommendation #4: Third Party Purposes/Justifications

Please find a link to Recommendation #4 here:
https://docs.google.com/document/d/1Xrx96CiQMhMff-dmCQWtomZ_ATISzgqRBSm72z0bzTA/edit?usp=sharing .

13. **Choose your level of support of Recommendation #4:**

Support Recommendation as written
[✓ Support Recommendation intent with wording change]
Significant change required: changing intent and wording
Recommendation should be deleted
No Opinion

14. **If your response requires an edit or deletion of Recommendation #4, please indicate the revised wording and rationale here.**

Third party purpose (iv) in the first bullet seems problematic:
"(iv) Registered name holder consent, contracted to responses to registered name holder's requests exercising their right of access." None of these seem valid third party purposes for requesting data disclosure. Suggest deleting (iv).

We would strongly advise any unnecessary 'procedural' barriers being created (as per iv) in the exercise of any data subject right. Such rights are bestowed by law, and not by the SSAD T&Cs. A data subject will not have to 'apply for disclosure' they will merely make a request to the controller via a direct means. This is not implied by current wording and remains of concern.

Recommendation #5: Acknowledgement of receipt

Please find a link to Recommendation #5 here:
https://docs.google.com/document/d/140U4AsH3so8tSojhdCEUa8I2QkD8OwBXxK9NcIjiCx4/edit? usp=sharing

15. **Choose your level of support of Recommendation #5:**

Support Recommendation as written
[✓ Support Recommendation intent with wording change]
Significant change required: changing intent and wording
Recommendation should be deleted
No opinion

16. **If your response requires an edit or deletion of Recommendation #5, please indicate the revised wording and rationale here.**

Although the concept of the Central Gateway manager being in a position to confirm whether a request is complete or not is welcome, it must be noted that

1) Unless human review is envisaged at the SSAD (which appears not to be the case as per Recommendation 8, fn13), only the form and physical presence of the Rec 3 envisaged elements may be counted. The confirmation of meaningful input will likely only be able to be done by a human review at the Central Gateway, or at the disclosing party;
2) Regardless of a human review or not at the Central Gateway, it needs to be clearer that the decision as to what is actually 'complete' or not, will continue to rest with the disclosing party in the circumstances of the request.

The time from which the SLA runs (recommendation 9) is only referenced in 1 footnote (fn 17) as from the receipt of the disclosure request from the Central Gateway. This is unreasonable, as it presumes a complete request in all escalations, and makes no allowance for error at the central gateway. The process involved here is exceptionally unclear and given the possibility of compliance censure and the effect on SLAs, this must be clarified.

What additional (completeness) checks (if any) does the working group envision the central gateway manager will be (automatically performing) after the form has been submitted (besides form validation).

Note – the ability to amend requests (envisioned here) means this will not be a “fire and forget” system… requests will have state and status. Presumably the requestor would have the ability to login to the (SSAD) and view submitted requests and see their status (implementation note needed?)

Response notes that automated response “SHOULD” contain information about subsequent steps and timeline. Unclear what this means. The working group should clarify what they are expecting – perhaps implementation notes?

Recommendation #6: Contracted Party Authorization

Please find a link to Recommendation #6 here:
https://docs.google.com/document/d/1-iiPCpZMdpYmhPLzqbHHbG7NvfKt80-AbjPPj-isHnM/edit?usp=sharing .

17. **Choose your level of support of Recommendation #6:**

Support Recommendation as written
Support Recommendation intent with wording change
[✓ Significant change required: changing intent and wording]
Recommendation should be deleted
No opinion

18. **If your response requires an edit or deletion of Recommendation #6, please indicate the revised wording and rationale here.**

Point 1: “automated review is not explicitly prohibited where it is both legally and technically permissible” needs to change to “technically and commercially feasible and legally permissible” for consistency. This is what the EPDP team agreed on as a group and it is used inconsistently throughout the document.

Point 4: “nor can refusal to disclose be solely based on the fact that the request is founded on alleged intellectual property infringement in content on a website associated with the domain name”.
While we understand the concern behind point 4, we are of the opinion that in some instances “the fact that the request is founded on alleged intellectual property infringement in content on a website associated with the domain name” is a legitimate basis to refuse disclosure. The current wording goes too far in limiting the registry operator’s discretion.

Inconsistent use of “Contracted Party” and “Authorization Provider” here as the decision maker.

Recommendation #6 is incomplete and doesn’t capture the full spectrum of decision making. There are potentially other legal bases under which Contracted Parties may disclose data. They need to be reflected in this section.

Recommendation #6 envisions that the disclosing entity may request additional information from the requestor. How does the working group envision that this will be accomplished? How will this impact SLA calculations?

How is the contracted party expected to communicate to the requesting entity – either providing the data, or the rejection notice with rational.

Recommendation #7: Authorization for automated disclosure requests

Please find a link for Recommendation #7 here:
https://docs.google.com/document/d/11BSAUqIUOWJmZOSTaQIW0QZncnywljKJPWUtCTtnCHY/edit .

19. **Choose your level of support of Recommendation #7:**

Support Recommendation as written
Support Recommendation intent with wording change
[✓ Significant change required: changing intent and wording]
Recommendation should be deleted
No opinion

20. **If your response requires an edit or deletion of Recommendation #7, please indicate the revised wording and rationale here.**

It is unclear what the title of this recommendation means; it seems to overlap and is confusing with Recommendation #16 (automation).

A fourth requirement should be added:
“4. The Central Gateway Manager MUST forward all requests, including specifically requests that are designated automated, to the authoritative source for the data to be fulfilled. The Central Gateway Manager MUST NOT maintain a record of request-response pairs such that a response could be re-used as a response to a future query.”

The text of Recommendation #7 needs to clarify that the two use cases in the “Implementation Guidance” are provided as examples and are not mandatory. There is no MUST automate language in this report, rather it is SHOULD where technically and commercially feasible AND legally permissible. The Contracted Parties are in the best position to determine whether automation for the data of their customers is technically/commercially feasible and legally permissible (we note that no actual legal analysis has yet confirmed that what people feel can be automated is actually legally automatable). Therefore, any automation use cases, including these two, should be opt-in - for Contracted Parties.

Moreover, it is impossible to agree to these two use cases as mandatory while any of the details of how automation will occur haven’t been worked out. How will jurisdictional issues be handled? How will the system not just say yes but say no? These are complex questions and those details are vital to any decisions about handing over control about decision making of our customers data.

This is not ruling out automation. Many Contracted Parties will want to automate many, most, or all of these requests. But that should be a decision that Contracted Parties get to make based on their own evaluation of the risk.

The wording “Over time, based on experience gained and/or further legal guidance, the Mechanism for the evolution of SSAD is expected to provide further guidance on which types of disclosure requests can be fully automated” is again presupposing a one-way path towards greater automation. We must be open to the possibility that experience may require us to move in the opposite direction as well.

Section 1 – what “criteria” established in these policy recommendations does this refer to? What is to be confirmed in the implementation phase?

Part of section 1 and all of section 2 are redundant and repetitive with Rec #5 (acknowledgement of receipt)

Section 3 is redundant and does not fit in this requirement.

Section 3, EPDP Phase 2 Recommendations #8-9

Recommendation #8: Response Requirements

Please find a link to Recommendation #8 here:
https://docs.google.com/document/d/1U6iEnJzxls_824MsBzgW1tk7Qa2W6eY72B3QkdMu2Uk/edit? usp=sharing .

22. **Choose your level of support of Recommendation #8:**

Support recommendation as written
Support intent of recommendation with edits
[✓ Intent and wording of this recommendation requires amendment]
Delete recommendation
No opinion

23. **Do you recommend a change to the wording of Recommendation 8? If so, please indicate proposed edits and rationale here.**

Section a) is redundant with other Recommendations including #5. This needs to be cleaned up to address potential inconsistencies and confusion in implementation.

Section b) also overlaps with other recommendations.

Section c) - We will require significant transparency about how the Central Gateway is making this recommendation in order to determine whether we can rely on it. It is unclear at this point how the Central Gateway will be able to reliably make these recommendations since they do not possess the underlying data being requested.

Section d) is about SLAs and overlaps with Rec #9. It should be removed from this section and covered in Rec 9 – SLAs

Section e) - Response back to the Central Gateway regarding denials will necessarily need to be lightweight. We cannot communicate details about our evaluation that could be considered personal data in their own right. And if we can't really go into detail, what purpose does this notification serve qualitatively (i.e. beyond us saying "we agree" or "we disagree"). This process needs to be lightweight in order to not unnecessarily encumber Contracted Parties who are processing requests.

Additionally, re e), the detail as to how 'public data' may be obtained seems to be not in keeping with the actual expectations of a controller. It is not the responsibility of the controller to educate a requester as to location of publicly accessible data. If data is publicly available, then making it an expectation that the controller must somehow be a repository of publicly available sources is simply unrealistic. Should the controller be aware of a publicly available resource, and is denying specifically for that reason, they should be encouraged to provide this detail, as it will help prevent further delay in an otherwise invalid query; however, making this mandatory is simply not acceptable. It is not the job of the controller to carry out investigations on behalf of a disclosing party. It should also be noted that a failure (repeated or otherwise) of a requester to not consider publicly available sources should at a minimum be considered in future balancing tests, and where repeated, this should be fed back to the Central Gateway. Such conduct should be considered a serious abuse of the process, as it demonstrates a lack of care and contradicts the expectations of the terms of use as per Recommendation 1.

Sections f) and h) cover urgent requests. This does not seem out of place in the response requirements recommendation and should be moved to its own dedicated recommendation to avoid confusion.

Section g) - note that the way this provision is drafted, all parties essentially get one freebie in terms of submitting non-urgent requests marked urgent. Is that what we intend from a practical perspective?

"If the Contracted Party determines that the disclosure would be in violation of applicable law or result in inconsistency with these policy recommendations, the Contracted Party MUST document the rationale and communicate this information to the requestor and ICANN Compliance (if requested)". We make the same note as above regarding the level of detail we can provide without disclosing any personal or personally identifiable data. Contracted parties are likely able to provide more detail to ICANN (if joint-controller) than a third-party requester so perhaps these two should not be equated.

The second to last paragraph should either be moved to implementation guidance or the "contracted parties" section. It is out of place as a stand-alone paragraph.

The last paragraph doesn't seem to belong in a response requirements section – what does the working group expect ICANN compliance to do with complaints about disclosure requests? ICANN compliance is not a competent authority to "judge" disclosure request decisions.

"If a requestor is of the view that its request was denied erroneously . . ."
It needs to be emphasized that ICANN Compliance's role is in reviewing a party's procedural compliance with the requirements of this policy, not substantive evaluation (or re-evaluation) of balancing tests or

disclosure decisions that a Contracted Party has performed.

Implementation guidance a) and b) are both redundant and covered multiple times in other places. This duplication needs to be addressed to avoid inconsistencies and confusion.

Implementation guidance c) use of “typically” here is confusing.

Implementation guidance d) should be moved to “urgent requests” (see above)

Recommendation #9: Determining Variable SLAs for response times for SSAD

Please find a link to Recommendation #9 here:
https://docs.google.com/document/d/1QwHyvI1SnFgVi8WGGIheCu0-fG76I_SIUFBe-sph-Ew/edit .

24. **Choose your level of support of Recommendation #9:**

Support recommendation as written
[✓ Support intent of recommendation with edits]
Intent and wording of this recommendation requires amendment
Delete recommendation
No opinion

25. **Do you recommend a change to Recommendation 9? If so, please indicate proposed edits and rationale here.**

Priority and SLAs are commingled in this Recommendation; they should be separated to avoid confusion.

The working group needs to address the concern regarding SLA percentages as applied to parties with a low volume of requests (particularly for urgent requests which by definition should be low in volume).

As a principle the working group should be creating a framework for SLAs that provide ICANN compliance with tools to combat bad actors but do not constrain ICANN compliance into taking action against parties making legitimate attempts to comply with the policy.

The concept of when the SLA calculations actually run from is also severely lacking in specificity and detail. We note that this recommendation suggests that timelines run from ‘the receipt of the disclosure request from the Central Gateway’ (see fn 17); however, this does not account for the fact that there are severe doubts as to the ability of the Central Gateway Manager to complete, in an automated manner, any such meaningful assessment of the completeness of a request. As we have also noted, the determination as to what constitutes a “complete” submission, must lie with the Controller in making that decision, not an automated review. At a minimum the time must run from when the controller deems the request to be full and complete in the circumstances of that request.

We also note that the concept of ‘urgent’ requests, currently indicated to be at the choice of the requester’, is not determinative. We further note that there is no room for meaningfully incorporating such extraordinary circumstances into the SLA.

We would like to remind that any requester may request disclosure from a data controller. The Registries have partaken in phase II in good faith, heeding the concerns of the community with regards to enhancing predictability and making the process more streamlined for all. We must remind that unless specifically provided for in the laws of a specific jurisdiction, the disclosure of such data to third parties is not a legal obligation of the controller. Noting both these facts, the imposition of SLAs seem almost punitive in nature, and although we appreciate that the intention is to ensure that requests do not go unanswered, this could be achieved by less invasive means than SLAs.

We also advise caution as it seems reasonable to assume that the expectation of “speedy” disclosure encourages quantity over quality. he timelines being imposed on the CPs / controllers, enforced by the SLAs, are considerably tighter than even those which are afforded to the Data Subject themselves in the exercise of their legal rights. Such a concept is anathema to ‘Privacy by Default’ and ‘Privacy by Design’; we must ensure that our policy does not create incompatibilities with the law, and where new obligations are being imposed on controllers, that such obligations do not hinder or promote a culture of prioritizing created contractual obligations, by design, over the actual legislative / legal obligations as data controllers. Any policy recommended must not create enhanced legal risk for the contracted parties, whilst also ensuring that the rights of the data subject remains at its core.

How does the working group expect that changes in priority will be reported to the central gateway manager and requestor?

The “what happens if the priority needs to be shifted” section includes information that has nothing to do with changes to priority. This section needs to be reorganized for clarity. It contains information (for example: “if the contracted party determines it is unable to disclose the nonpublic data; the contracted party SHALL provide a rationale to the requestor and the Central Gateway Manager”) that does not belong in this recommendation and is duplicative with other recommendations.

A paragraph on page 33 mentions a “small team” recommendation. This should be addressed, but also seems to deal with reporting requirements and not SLAs.

Registries do not agree that response targets for fully automated responses are to be developed during the implementation phase.

The last paragraph has nothing to do with SLAs and isn’t appropriate here. It should be deleted as it’s already covered in other recommendations.

26. **If you do not agree with the proposed SLA matrix and/or accompanying description, please provide your rationale and proposed alternative language.**

Recommendation #10: Acceptable Use Policy

Please find a link to Recommendation #10 here:
https://docs.google.com/document/d/1JHgbtfvnHezDhEJLkj6KxvGC1bvGu1v7XZA73Z47IMA/edit? usp=sharing .

28. **Choose your level of support of Recommendation #10:**

Support recommendation as written
Support intent of recommendation with edits
Intent and wording of this recommendation requires amendment
Delete recommendation
[✓ No opinion]

29. **If your response requires an edit or deletion of Recommendation #10, please indicate the revised wording and rationale here.**

Recommendation #11: Disclosure Requirement

Please find a link to Recommendation #11 here:
https://docs.google.com/document/d/1r6qgmnI-0ha0mmYqP0Z3drZr3FJsxG-uW9bRC2bJ4Uo/edit?usp=sharing .

30. **Choose your level of support of Recommendation #11:**

Support recommendation as written
Support intent of recommendation with edits
[✓ Intent and wording of this recommendation requires amendment]
Delete recommendation
No opinion

31. **If your response requires an edit or deletion of Recommendation #11, please indicate the revised wording and rationale here.**

Stating that Contracted Parties and SSAD "[w]here required by law, MUST perform a balancing test before processing the data" rules out any automation requiring a 6(1)(f) balancing. On strict reading of this would mean that any automation of a disclosure requiring a balancing test would violate the disclosure requirements and be subject to ICANN Compliance enforcement.

We are missing an element here regarding requirements to notify parties whose data has been disclosed.

f) "Upon a request from a data subject the exact processing activities of their data within SSAD, SHOULD be disclosed as soon as reasonably feasible"
We disagree with this statement. There are legal requirements about the format and timing of responses to requests from data subjects and I want to follow those, not a "reasonably feasible" standard. Therefore, we suggest "SHOULD be disclosed in accordance with applicable law."

g) is merely a redundant restatement of what the law actually states. Additionally, the SSAD and the rules surrounding it, should not even attempt to dictate the manner in which a controller meets their legal obligations. This serves nothing but to greatly increase the liability of that body that is tasked with enforcement of this policy. Section g) should be deleted.

i) It should be noted that there must be a means whereby when a valid Art 17 request is made to a controller, that the Central Gateway must be capable of handling the ‘pass-on’ notification requirements of Art 17 (requirement to provide reasonable notification of an Art 17 request to those persons/entities to whom the data has previously disclosed) are properly taken into account. In general, the RySG advises additional consideration must be given in general with respect to the exercise of all individual data subject rights vis a vis the interaction of the disclosing parties and the SSAD so as to ensure the SSAD continues to be respectful of data subject rights of registrants.

f) and i) somewhat overlap and are inconsistent (should vs. must)

Recommendation #12: Query Policy

Please find a link to Recommendation #12 here:
https://docs.google.com/document/d/1_ng86GC09Ye5ruCBk4vBrXZN7nCyagAanJT9aSDBrGQ/edit? usp=sharing .

32. **Choose your level of support of Recommendation #12:**

Support recommendation as written
[✓ Support intent of recommendation with edits]
Intent and wording of this recommendation requires amendment
Delete recommendation
No opinion

33. **If your response requires an edit or deletion of Recommendation #12, please indicate the revised wording and rationale here.**

We would like to add in the fact that the disclosing parties, who may receive requests outside of the SSAD, must be notified with all details, including identity and details as to the various requests made, as to any such decision relating to access policy violations. The disclosing parties MUST be aware and must be in a position to be able to consider where the SSAD system is being ‘gamed’ by a requester. The controllers should not be placed in a position where they are releasing data to those requestors who have been deemed to have abused/contravened the SSAD process.

Last paragraph of b) is confusing. Working group should revisit and clarify the intent.

c) remove “in whatever form it eventually takes”.

Recommendation #13: Terms of Use

Please find a link to Recommendation #13 here:
https://docs.google.com/document/d/1ou3hY3peDnxgo45FmUBs_cIv4f3qUntYecIg10wB__4/edit? usp=sharing .

34. **Choose your level of support of Recommendation #13:**

Support recommendation as written
[✓ Support intent of recommendation with edits]
Intent and wording of this recommendation requires amendment
Delete recommendation
No opinion

35. **If you believe edits are needed for Recommendation #13, please propose edits and rationale here.**

Remove paragraph, “Further consideration should be given during implementation whether updates to the RAA are necessary to ensure compliance with these recommendations”. Changes to the RAA are out of scope of implementation.

Recommendation #14: Retention and Destruction of Data

Please find a link to Recommendation #14 here:
https://docs.google.com/document/d/1tBf2jEWIXydskYXxYAjOObebuFgL4iYIHqhBwdo86pU/edit? usp=sharing .

36. **Choose your level of support of Recommendation #14:**

[✓ Support recommendation as written]
Support intent of recommendation with edits
Intent and wording of this recommendation requires amendment
Delete recommendation
No opinion

37. **If you do not support Recommendation #14, please provide proposed edits and rationale here.**

Recommendation #15: Financial Sustainability

Please find a link to Recommendation #15 here:
https://docs.google.com/document/d/1EN7mDz44BkxoW_RVlDsgjxhSLkUgrW5XwxIX-O-0TEk/edit? usp=sharing .

38. **Choose your level of support of Recommendation #15:**

Support recommendation as written
[✓ Support intent of recommendation with edits]
Intent and wording of this recommendation requires amendment
Delete recommendation
No opinion

39. **If you believe edits are needed for Recommendation #15, please propose edits and rationale here.**

The working group MUST consider costs against expected volume of requests and the fees that would need to be charged and agree that the system is financially viable before agreeing to these recommendations.

In order to understand the financial viability of the SSAD system, the financial model must be fully considered by the working group. Registries note that the working group has requested cost estimates from ICANN org on what it is expected to cost to build and maintain the SSAD system.

“Legal risk fund” is mentioned in passing here but not described or explained here or anywhere else.

Registries support the language in Recommendation #15 that states “data subjects MUST NOT bear the costs for having their data disclosed to third parties;" The creation, maintenance and operation of the SSAD system but not result in an increase in the cost of a domain name registration.

The reference in the last paragraph of Recommendation 15 related to the EPDP Teams' request relating to the "three models". The choice of the Hybrid Model by the EPDP team is not taken into account here, and ensure that ICANN are properly focussed on assessing only the chosen model.

Recommendation #16: Automation

Please find a link to Recommendation #16 here:
https://docs.google.com/document/d/1_gqq1JKHcDqVKKfdwOdfAghPYm-ErV2t9qxJVDsDjWc/edit? usp=sharing .

40. **Choose your level of support of Recommendation #16:**

Support recommendation as written
[✓ Support intent of recommendation with edits]
Intent and wording of this recommendation requires amendment
Delete recommendation
No opinion

41. **If you believe changes are needed for Recommendation #16, please provide proposed edits and rationale here.**

We suggest to replace the current last paragraph:

> "The SSAD MUST allow for automation of the processing of well-formed, valid, complete, properly-identified requests from accredited users with some limited and specific set of legal basis and data processing purposes which are currently described in Preliminary Recommendation #7 but still under discussion. These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention."

By (last sentence amended):

> "The SSAD MUST allow for the automation of the processing of well-formed, valid, complete, properly-identified requests from accredited users with some limited and specific set of legal basis and data processing purposes which are currently described in Preliminary Recommendation #7 but still under discussion. These requests MAY be automatically processed and that automation MUST be to ensure that the actual source of the authoritative data be directed to provide the response requested for each request and disclose the non-public RDS data without human intervention."

Use of "typically" on page 40 is confusing – the working group should clarify exactly what they are recommending?

We would like to re-emphasize our comments on Recommendation 7 regarding the use cases and the language in the recommendation - rather it is SHOULD where technically and commercially feasible AND legally permissible - and reiterate that any automation use cases should be opt-in for Contracted Parties.

Recommendation #17: Logging

Please find a link to Recommendation #17 here:
https://docs.google.com/document/d/1zG2myy1br-xbXBHBvd34gm_J-vXPEr6GoBOoWFqi9RQ/edit?usp=sharing .

43. **Choose your level of support of Recommendation #17:**

Support recommendation as written
Support intent of recommendation with edits
[✓ Intent and wording of this recommendation requires amendment]
Delete recommendation
No opinion

Overall the logging requirements should be simplified, the language should be kept light and the logging entity should be given flexibility to follow relevant data protection law while also maintaining records sufficient to demonstrate compliance with the SSAD recommendations and related Policies.

We miss a consideration that logs will almost certainly contain personal data and will require safeguards and protections to ensure that the data is handled appropriately.

e.ii) “Logs should be further available to data protection authorities, ICANN, and the auditing body” Contracted Parties should be able to access these logs upon request as well in order to verify their own reliance on the SSAD mechanisms.

The automation envisage relating to the the intake and completeness checks although, in theory, are completely acceptable, noting that such ‘automated completeness checks’ are linked now linked to the timing of the SLA and compliance enforcement, and potential censure for the CPs, the RySG cautions the over reliance on automated review that is currently theoretical and likely incapable of having the ability to ascertain the actual completeness of a submission, and will merely assess completeness of fields in a purely functional matter. This can but lead to dispute and far more clarity as to the realistic result of automation as opposed to the aspirational and theoretical would be preferred.

The RySG again reminds that the Central Gateway does not currently hold any data relating to requests; it does not process the registrant data. High levels of caution must be advised where any ‘disclosure of non-public data without human intervention’ will attempt to process registrant data - this includes the initiation of a process to disclosure data automatically at the disclosing party as that action/command is factually a processing of personal data that will be carried out at the sole decision of the SSAD, therefore will attract greater responsibility. This has knock on effects for the other involved parties who permit this automation. The legal role of the SSAD must be considered at all junctures. This will create enhanced risk for all parties, but mainly for the party administering the SSAD. This is why the RySG continues to advise that such automation must be at the option of the disclosing party and cannot be mandatory.

Under contracted party logging – Disagree that contracted party logs should be put in escrow.

Recommendations #18-19, Implementation Guidance

Recommendation #18: Audits

Please find a link to Recommendation #18 here: https://docs.google.com/document/d/1GnR5m5kdHrNCn3TxHhwtUJF0j-Zl1gdVAauQ47WqGBQ/edit? usp=sharing .

44. **Choose your level of support of Recommendation #18:**

Support recommendation as written
[✓ Support intent of recommendation with edits]
Intent and wording of this recommendation requires amendment
Delete recommendation
No opinion

45. **If you do not support Recommendation #18, please provide proposed edits/changes and rationale here.**

The expense of audits should be considered and taking into account in financial sustainability.

Results of audits should be published including deficiencies identified. The steps taken to address deficiencies should be reported.

The last paragraph of accrediting authority seems to exempt ICANN from audits; the working group should revisit and confirm if this is the recommendation – "as" should be "if" (first word).

The recommendations don't' address the frequency of audits – the working group should revisit and confirm if this is intentional.

Recommendation #19: Mechanism for the Evolution of the SSAD

Please find a link to Recommendation #19 here:
https://docs.google.com/document/d/12KdBUNUXy8m_exDvFL3D2rBUYUTMmJpM9RqoWlZL_0o/edit? usp=sharing.

46. **Choose your level of support of Recommendation #19:**

Support recommendation as written
Support intent of recommendation with edits
[✓ Intent and wording of this recommendation requires amendment]
Delete recommendation
No opinion

47. **If you do not support Recommendation #19, please provide proposed edits or changes and rationale here.**

The RySG recognizes that the SSAD may need to evolve over time as both requesters and disclosers gain operational experience with the system, and more importantly, as the legal landscape around data privacy continues to evolve. This is an area of law that is changing rapidly. The commitment to evolving the SSAD should be mindful of this fact and not assume that future evolutions will necessarily move toward increased automation of access to non-public registration data.

We appreciate the EPDP Team's recognition that "The Mechanism...must not contravene the ICANN Bylaws, the GNSO PDP and/or existing contractual provisions for the development of new requirement for Contracted Parties" (p. 44). However, we have serious concerns about the scope of matters this Mechanism is intended to address. Specifically, items (b) and (c) listed out in Recommendation 19 are topics that are not matters of implementation, but are critical policy questions. Phase 2 of the EPDP was tasked with considering which users could or could not be granted access to non-public registration data, and leaving these questions (along with the question of which requests can be automated) to an as-yet-undetermined Mechanism to answer is not appropriate. Before the RySG can support any Mechanism to evolve the SSAD, the scope of that mechanism must be clearly defined, and suitable checks and balances must be put into place.

48. **What existing processes / procedures, if any, can be used to meet the above responsibilities?**

The appropriate Mechanism will depend on the scope of matters that will be addressed. Wherever possible, the EPDP Team should avoid recommending a brand new mechanism and rely on existing processes and procedures. Because the RySG believes that the items the Mechanism would be addressing are matters of policy, the most appropriate process to leverage is the existing PDP. We believe that establishing a new Mechanism could have the unintended, but grave, consequence of circumventing ICANN's established policy development process.

While previous PDPs have not been conducted in a manner that allows for the evolution of a policy over time, the RySG suggests that the EPDP Team consult with the GNSO Council to determine whether this may be an opportunity to exercise some creativity in how the GNSO approaches policy development. For example, the Team could ask the GNSO Council to consider restructuring this EPDP to include recurrent reviews of the final Phase 2 policy (i.e., the SSAD) after it has been fully implemented. The Council would need to set a clear and narrow scope for these reviews, and the reviews would be conducted under all the rules and guidelines of the PDP. The RySG suggests that the GNSO Council could establish an Advisory Council that will be responsible for advising when a review should be triggered (which could include both reviewing relevant current events such as changes to privacy law and/or vetting requests from the ICANN community to initiate a review). The reviews can be conducted by a team substantially similar to the current EPDP Team (e.g., with the same composition of members from different community groups, but not necessarily the exact same individual members), and would take place for a limited duration (e.g., 6-8 weeks). Opportunities for public comment would of course be included. If coupled with an expedited implementation process, this type of approach could potentially achieve the goals identified in Recommendation 19 without requiring the development of a completely new Mechanism.

Conversely, if the purview of the Mechanism is sufficiently narrow such that it only addresses matters of implementation, the process described above would not be necessary.

49. **If no suitable existing processes / procedures can be used, what type of mechanism should be created factoring in: Who should guidance be provided to? How is guidance developed / agreed to? How should it be structured?**

See response to question 48. That said, if the EPDP Team does decide to adopt a new Mechanism, the RySG expects that there will be an additional public comment period during which the ICANN community can provide input on the proposed Mechanism. Recommendation 19 does not actually describe a specific Mechanism, and so anything developed by the EPDP Team will need to be put out for community review.

50. **What information is needed to ensure the continuous evolution of SSAD?**

Accurate and detailed information about the requests made and the responses to those requests, consistent with the implementation guidance included in Recommendation 17, is required to determine whether and how the SSAD should evolve over time.

51. **How is guidance of the Mechanism expected to be implemented?**

Per our response to question 48, decisions made about the evolution of the SSAD would be implemented through an expedited version of ICANN’s policy implementation process.

Implementation Guidance #i.

Please find a link to Implementation Guidance #i. here:
https://docs.google.com/document/d/1uh3VfWkOZyU7NpVupPU7VBuoW6Lo1N65HUUPnGbBgr4/edit? usp=sharing .

52. **Choose your level of support of Implementation Guidance #i:**

Support implementation guidance as written
Support implementation guidance with edits
Intent and wording of this implementation guidance requires amendment
[✓ Delete implementation guidance]
No opinion

53. **If you do not support Implementation Guidance #i, please provide proposed edits or changes and rationale here.**

This is completely redundant with Recommendation #12 (Query Policy).

Reporting Requirements

Implementation Guidance #ii currently provides: Following the public comment period, the EPDP Team will further review what reporting requirements are necessary to support the SSAD.

54. **What type of reporting should be required as part of SSAD?**

The following data should be provided publicly by the SSAD system on at least a quarterly basis (but MAY be provided more often).

Accreditations:

- Number of accreditation requests (total/reporting period)
- Number of accreditations approved/rejected (total/reporting period)
- Number of active accreditations (current total)
- Number of re-accreditations approved/rejected (total/reporting period)
- Number of suspended/revoked accreditations (total/reporting period)

Disclosure Requests:

- Disclosure requests received through SSAD (total/reporting period)
- Breakdown of requests by requestor type (Law Enforcement, Security Researcher, Commercial Litigation, other) (total / reporting period)
- Number of requests rejected by SSAD system vs number forwarded for disclosure consideration (total/reporting period)
- Number of disclosure requests approved (total/reporting period)
- Number of disclosure requests rejected – breakdown by reasons (insufficient data, failed balancing test, privacy/proxy registration, data already public, other) (total/reporting period)

The following individualized data should be made available to disclosing entities on at least a quarterly basis (but MAY be provided more often) and be available to ICANN org in total

- Disclosure requests received by disclosing entity in reporting period – including breakdown by requestor type (Law Enforcement, Security Researcher, Commercial Litigation, other)
- Number of requests approved vs rejected (include breakdown by reasons)
- Average/mean time to respond to disclosure request – (total and calculated against the SLAs per priority grouping)
- Disclosure request responses agreeing vs disagreeing with recommendation provided by gateway
- Disclosure request automated at gateway vs. forwarded to disclosing entity

Other Comments & Submission

55. **Are there any recommendations the EPDP Team has not considered? If yes, please provide details below.**

56. **Are there any other comments or issues you would like to raise pertaining to the Initial Report? If yes, please enter your comments here. If applicable, please specify the section or page number in the Initial Report to which your comments refer.**

The RySG notes several areas for clarification regarding the SSAD principles/concepts noted in the report. In addition, we draw attention to several overarching areas of concern.

Section 3.1, SSAD High Level Principles/Concepts, notes that the automation of requests and transmission of requests must be automated to the extent feasible. The RySG emphasizes the importance of stating consistently that the requirement that submission and transmission be automated only if automation is technically and commercially feasible. This does not appear consistently throughout the report.

Section 3.1 also addresses the automation of data disclosure and notes that disclosure should only be automated where technically and commercially feasible AND legally permissible. Again, this is not consistently emphasised throughout the report.

Automation and disclosure

The RySG looks forward to the SSAD offering more predictability for parties regarding the submission of requests for disclosure of non-public registration data. We do, however, also want to emphasize that while the submission and transmission of requests will be automated, in the majority of cases we expect review of requests to remain manual, per the requirements of the GDPR. There should be an understanding that simply because the submission of a request is automatic, that does not translate to an automatic disclosure.

Disclosing entity:

The Phase II initial report suggests (but is not fully settled on the approach) that *both* registrars and registry operators must consider and respond to requests for disclosure of personal data. I.e., that those seeking personal data may initially make the request from the pertinent registrar and if there is no or a negative response, make the same request to the pertinent registry operator, or may seek the information in the opposite order or simultaneously from both the registrar and registry operator.

The rationale for this approach includes the concern that some registrars will not comply with the Consensus Policy requirement to respond to requests for personal data; therefore, an alternate source is required.

This would be an inappropriate policy choice for each of the reasons described below. Instead, ***the decision to disclose personal data should rest only with the domain name registrar of the domain holder.***

1. ***We cannot create consensus policy with the expectation that it will not be followed.*** The rationale that some registrars will not comply with the Consensus Policy is incongruous with the ICANN Bylaws, the obligations of ICANN contacted parties, and common sense. We do not / can not create Consensus Policy with the idea that some contracted parties will disregard the Consensus Policies and resulting contractual obligations. This is akin to the old adage of creating a law that says, "Do not this, but if you do…"

The EPDP team is striving to create an "implementable" policy that can be enforced in a straight-forward manner. This or any policy cannot be based on the anticipated failure of ICANN Compliance to enforce it. Such an improper accommodation would lead to other negative consequences, some of which are described below.

2. ***Inconsistencies in disclosure has significant negative consequences.*** What are the consequences of a registrar and a registry operator reaching different conclusions on a data request? Is it evidence that one party is violating privacy law? Is it evidence of ICANN contract breach? Inconsistencies will lead to conflict and disputes – each of which distract from the policy goal of disclosing personal data when appropriate. Personal data seekers and privacy advocates will leverage ICANN contracts and courts of advantageous jurisdiction to win individual claims and attempt to intimidate decision makers.

Inconsistencies will raise fundamental questions about the efficacy of ICANN policy making and contractual compliance, bringing into question the utility of the ICANN model on this globally visible issue.

The existence of choice will also lead to forum shopping with certain contracted parties having reputations for lax or strict interpretations of GDPR. This will in turn lead to disputes among combinations of contracted parties, ICANN, interest groups and DPAs.

Due to the complexities that are part of GDPR and ICANN policy, it is likely that the cases of inconsistent decisions and their consequences will greatly outweigh the number of registrars not making best effort to implement the GDPR policy. This is the tail wagging the dog.

3. ***Historically, registries have been required to make registration data available – the reasons for this no longer apply.*** It is true that prior to GDPR implementation that those seeking personal registration data could seek that data from registry operators *or* registrars. Both were obligated to make it available. The rationale for this accommodation is that jurisdictional law or other barriers might impede access to otherwise public data. I.e., there were variances based upon jurisdiction.

The opposite is the case now. It is the objective of the EPDP team to develop a consistent set of standards for the global set of registrars. With the promulgation of different privacy regimes, the decision to disclose is based upon where the *data* resides and *not* where the contracted party resides. Indeed, to create the opportunity for sourcing personal data based on likelihood of success subverts the very nature of the EPDP-developed policy recommendations and the goal of consistency in disclosure consistency.

Privacy by Design

We urge the EPDP Phase 2 Team to incorporate basic data privacy principles such as “privacy by design and by default” into the requirements for this SSAD. There is also no reference to the balancing with ECHR Article 8 considerations, and as such, our accountability requirements under data protection law will be almost impossible to achieve.

Implementation

We note these recommendations leave a large amount of work to implementation. It will be a significant effort for ICANN org (with IRT support) to develop the policy language and to implement the policy.