SAC112: Minority Statement on the Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process (EPDP)

A Comment from the ICANN Security and Stability Advisory Committee (SSAC)
20 August 2020

Preface

This is a Minority Statement from the ICANN Security and Stability Advisory Committee (SSAC) on the Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process (EPDP).

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits.

Editor's note of 25 August 2020: This version of SAC112 contains corrections to the footnotes in Section 5 on page 9 and Section 8 on pages 15-16. No other changes have been made.

Table of Contents

Executive Summary 3

1 Introduction 4

2 Unfulfilled Charter Items 6

3 Overarching Issues with Prioritization and Responsiveness to Requests 7

4 Objection to Recommendation 6 on Priority Levels 8

5 Objection to Recommendation 10 on Determining Variable SLAs for response time for SSAD 9

6 Objection to Recommendation 12 on Disclosure Requirement 10

7 Objection to Recommendation 14 on Financial Sustainability 11

8 Other Comments 15

9 Acknowledgments, Statements of Interests, Dissents, Alternative Views and Withdrawals 17

9.1 Acknowledgments 17
9.2 Statements of Interest 17
9.3 Dissents and Alternative Views 17
9.4 Withdrawals 18

Executive Summary

The SSAC cannot endorse the Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited PDP[1] (hereinafter as "The Final Report") as it currently stands.

Firstly, we believe that a much better system is possible within the limitations imposed by the general data protection regulation (GDPR), and that the EPDP has *not* provided outcomes that are reasonably suitable for security and stability.

Secondly, the Final Report does not recommend a commitment to finish unaddressed charter items. The SSAC conditioned its participation in and support of Phase 2 EPDP based on the promise that several Phase 1 issues would be examined. Unfortunately, they were not examined, and remain unaddressed.

Thirdly, in addition to the issues discussed above, there are some specific recommendations to which the SSAC objects, namely:

- *Recommendation 6: Priority Levels.* The classification of cybersecurity threats as "Priority 3" is insufficient to address the reality of serious online threats.
- *Recommendation 10: Determining Variable SLAs for response time for SSAD.* The SSAC is concerned about long response times, that the SLAs are not practically enforceable, and that the implementation advice may allow contracted parties to respond to data requests more slowly over time.
- *Recommendation 12: Disclosure Requirement.* The SSAC is concerned that contracted parties may, at their discretion, reveal the identities of data requestors, rather than doing so only when data protection law requires. Revealing the identities of data requestors may endanger them and compromise investigations.
- *Recommendation 14: Financial Sustainability.* The recommendation contains flawed language that unfairly shifts costs onto victims, is inconsistent with normal business practices, and goes against previous SSAC advice to the ICANN Board. The recommendation was not drafted according to GNSO procedures, is unsupported by evidence, and may not be compliant with the GDPR.

The system for standardized access/disclosure to non-public registration data (SSAD) as envisioned in Phase 2 can become an improvement over the status quo, if some of the recommendations are changed, and if the GNSO commits to completing work that was part of the EPDP's charter but remains unaddressed. Once the GNSO can guarantee that the natural-versus-legal persons, privacy/proxy, and data accuracy issues will be promptly examined via formal policy development, the SSAC might be able to endorse the Final Report.

[1] See Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-31jul20-en.pdf

1 Introduction

The SSAC has participated in the EPDP in a spirit of professionalism and good faith, devoting thousands of volunteer hours over both phases, and working diligently with our colleagues across the ICANN community.

As stated in SAC111:

> The SSAC has compromised on many matters, as most participants have, in the interest of moving forward and getting a system online. For the avoidance of doubt, the Phase 2 Report and its recommendations currently fall far short of what the SSAC believes is necessary and possible to address security and stability issues within ICANN's remit. The SSAC does not think that the initial version of the System for Standardized Access/Disclosure (SSAD) will deliver data in a way and at speeds that will satisfy many operational security needs. We believe that a better system is possible within the limitations imposed by the GDPR. In order to move things forward today, the SSAC supports building a solid foundation that can be improved upon in a timely manner rather than holding out for an ideal system.[2]

The SSAC stands by the statement. We cannot endorse the overall results of Phase 2 as it currently stands.

We believe that a much better system is possible within the limitations imposed by the GDPR, and that the EPDP has not provided outcomes that are reasonably suitable for security and stability. Furthermore, the Final Report does not recommend a commitment to finish unaddressed charter items. SSAC conditioned its participation in and support of Phase 2 based on the promise that several Phase 1 issues would be examined. Unfortunately, they were not examined, and remain unaddressed.

Of the twenty-two recommendation in the Final Report, the SSAC objects to four of them, namely:

- *Recommendation 6: Priority Levels.* The classification of cybersecurity threats as "Priority 3" is insufficient to address the reality of serious online threats.
- *Recommendation 10: Determining Variable SLAs for response time for SSAD.* The SSAC is concerned about long response times, that the SLAs are not practically enforceable, and that the implementation advice may allow contracted parties to respond to data requests more slowly over time.
- *Recommendation 12: Disclosure Requirement.* The SSAC is concerned that contracted parties may, at their discretion, reveal the identities of data requestors, rather than doing so only when data protection law requires. Revealing the identities of data requestors may endanger them and compromise investigations.

[2] See SAC11, page 5

- *Recommendation 14: Financial Sustainability.* The recommendation contains flawed language that unfairly shifts costs onto victims, is inconsistent with normal business practices, and goes against previous SSAC advice to the ICANN Board. The recommendation was not drafted according to GNSO procedures, is unsupported by evidence, and may not be compliant with the GDPR.

We do not object to the rest of the recommendations in the Final Report. That does not mean we are enthusiastic about all of them. For example, the SSAC supports the idea of SSAD accreditation, because accreditation is a safeguard designed to satisfy the GDPR, providing confidence for and documentation of legitimate requests. However, we do not know if accreditation will be an effective tool. Under the proposed policy, whether data is revealed or not will depend entirely upon the decision-making of each registrar and registry operator, which will vary greatly in their evaluation methods and standards, and will provide uneven, subjective, and unpredictable outcomes. The proposed policy may not provide effective recourse for data requestors who have their demonstrably legitimate requests denied. Thus, regardless of the strength of the accreditation program that is put in place, it may not deliver results, and may not justify the good efforts of the data requestors. This is not a reliable outcome and delivers less than what the GDPR allows.[3]

Several recommendations in the Final Report have failed to receive consensus, receiving formal opposition from a notable number of the participant bodies. However, some members of the community claim that the GNSO Council must now perform one "up or down" vote on the entire Final Report, approving all of the recommendations or none at all. We believe that such an "all or nothing" approach would circumvent the consensus process. It would also violate GNSO procedure, which says that, "In the event that the Final Report includes recommendations that did not achieve the [sic] consensus within the PDP Team, the GNSO Council should deliberate on whether to adopt them or remand the recommendations for further analysis and work."[4]

We note that while the recommendations attempt to create an overall program, there is not such a tight interdependence among them all that necessitates an "all or nothing" vote. There is certainly room to modify recommendations. Some recommendations (and certainly some of the many sub-recommendations) could be rejected while leaving the rest intact. The idea that the entire work will unravel without all the recommendations passing, or without passing as currently written, is a false narrative. The GNSO's procedures go on to say that, "the GNSO Council may adopt all or any portion of the recommendations contained in the Final Report" and may supervise the work of revising recommendations. Hard work may be required, but that is the duty of the GNSO Council, and of the ICANN Board, which will also need to consider the

[3] In July 2018 the European Data Protection Board wrote to ICANN Org and affirmed that "the personal data processed in the context of WHOIS can be made available to third parties who have a legitimate interest in having access to the data, provided that appropriate safeguards are in place to ensure that the disclosure is proportionate and limited to that which is necessary and the other requirements of the GDPR are met ...", See "Letter to Göran Marby from the European Data Protection Board," https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

[4] See GNSO Policy Development Process Manual, Section 13 "Council Deliberation," page 8, https://gnso.icann.org/sites/default/files/file/field-file-attach/annex-2-pdp-manual-24oct19-en.pdf. This procedure also applies to EPDPs.

results. The legitimacy of ICANN and its multi-stakeholder process are under the microscope here.

The rest of this statement details key areas of SSAC's concern.

2 Unfulfilled Charter Items

In SAC111, the SSAC stated its concern that items in the EPDP's Charter were not receiving discussion and decision-making. It noted, "important issues involving the subject areas of natural-versus-legal persons, privacy/proxy service, and data accuracy are in danger of going unaddressed by the EPDP."[5] Those topics were deferred in Phase 1. The SSAC conditioned its participation in and support of Phase 2 based on the promise that those issues would be examined. Unfortunately, they were not examined, and remain unaddressed. For example,

- Commitments to examine the natural-versus-legal issue via PDP are not mentioned in the Final Report.
- The Final Report states: "Conclusion – Accuracy and WHOIS Accuracy Reporting System: per the instructions from the GNSO Council, the EPDP Team will not consider this topic further; instead, the GNSO Council is expected to form a scoping team to further explore the issues in relation to accuracy and ARS to help inform a decision on appropriate next steps to address potential issues identified." A scoping team is not a promise to pursue any work. PDP-level decision making is necessary here.
- Privacy/proxy issues: The Proxy Services Accreditation Issues (PPSAI) work of 2016 does not address important issues posed by the GDPR and under the remit of the EPDP, and the PPSAI and EPDP work streams remain siloed. More work is necessary.
    - It is necessary to discuss how affected parties may request underlying domain contact data from ICANN-accredited privacy/proxy providers, which are data controllers. Being able to request that registration data is the entire point of the EPDP and SSAD. The Final Report means that ICANN is leaving all privacy/proxy-protected domains outside of the SSAD, and outside of its SLAs and accountability mechanisms.
    - This was within the EPDP's charter. The EPDP charter's mission and scope section says, "The EPDP Team shall consider what subsidiary recommendations it might make for future work by the GNSO which might be necessary to ensure relevant Consensus Policies, including those related to registration data, are reassessed to become consistent with applicable law."[6] The EPDP has not done so on this subject.

The natural-versus-legal issue remains unaddressed in part because of an unexplained failure to perform research in a timely manner. The EPDP Phase 1 report recommended that ICANN undertake "as soon as possible" research that considers the feasibility and costs of differentiating

[5] See SAC111, page 8
[6] See EPDP Final Adopted Charter - 19 July 2018, https://community.icann.org/display/EOTSFGRD/EPDP+Team+Charter?preview=/88574674/90767676/EPDP%20FINAL%20Adopted%20Charter%20-%2019%20July%202018.pdf

between legal and natural persons, how other industries and organizations have successfully differentiated between legal and natural persons, and privacy risks to registered name holders of differentiating legal and natural persons (recommendation 17.2).[7] On 15 May 2019 the ICANN Board accepted that recommendation and directed ICANN staff to execute the project as input to the EPDP Phase 2 work.[8]

There were two failures:

1. The research report was delivered to the EPDP on 8 July 2020, *after* the Final Report was done, too late in the process to give the legal vs. natural persons its due consideration.
2. The research report did not look at some of the most relevant and obvious examples, such as how and why natural and legal person data is collected and published in real estate registries, company registries, and trademark registries inside the EU; and how such registries outside the EU handle the data of subjects who reside in the EU. While the report stated that "most EU ccTLD operators continue to publish some (and sometimes all) contact data fields for domains registered by legal persons,"[9] the report did not provide the details, such as a list of which ccTLDs publish what data.

The SSAC requests that the GNSO Council and the ICANN Board provide an explanation as to why the report was so late and why the Board's resolution was not fulfilled for the intended beneficiaries: the community's participants in the EPDP. To inform future decision-making, the report may eventually need to be revised to supply the missing analysis noted above and other relevant information.

As noted in SAC111: "The GNSO creates charters explicitly so that working groups and the participants in them understand the deliverables. The GNSO has working group standards and procedures designed to carry out work in predictable and fair ways, and groups participating in working groups should be able to meet the commitments they make to each other…. When the established processes fail and critical elements are not addressed, it threatens the legitimacy of ICANN policy making on critical issues of global interest."[10]

3 Overarching Issues with Prioritization and

[7] See Final Report of the Temporary Specification for gTLD Registration Data Expedited Policy Development Process, https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf

[8] See ICANN Board Resolution of 15 May 2019, https://features.icann.org/consideration-gnso-epdp-recommendations-temporary-specification-gtld-registration-data and accompanying ICANN Board scorecard, Recommendation #17, page 5, https://www.icann.org/en/system/files/files/epdp-scorecard-15may19-en.pdf

[9] See Differentiation between Legal and Natural Persons in Domain Name Registration Data Directory Services, https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20200708/5f72ece1/Rec17.2_Legal-Natural_8jul201-0001.pdf

[10] See SAC111

Responsiveness to Requests

These two recommendations are tightly coupled, with Recommendation 6 providing a concept for "Priority" of data disclosure requests, and Recommendation 10 defining very precisely the expected responsiveness to such requests by the relevant contracted parties. Providing policy recommendations that create differentiated priorities for various types of data disclosure requests is useful, since some data may be needed nearly immediately to mitigate issues that are time-sensitive and/or highly impactful in nature, while others so not present urgent or exigent needs. Providing policy guidance to contracted parties and others involved in the disclosure process on expected timeframes for responses (including status of requests and requested data if approved) is also very useful for creating a system with consistency and accountability.

Unfortunately, the resulting recommendations went well beyond the needed policy recommendations and prescribed very specific implementation details for those policies. Those details are rigid, inadequately nuanced, and poorly designed to address many of the most urgent needs for access to RDS data, particularly in the realm of cybersecurity. While well-intentioned, putting such a detailed implementation plan into policy may well have the net effect of creating a complex, hard-to-officiate system that overburdens contracted parties for many categories of requests, while leaving many data requestors woefully underserviced for other types of requests.

The SSAC supports the high-level goals of creating a prioritization and response expectation framework. However, implementation work should be left to the implementation team. That team should include representatives of the contracted parties that will be providing data for requests, the parties who routinely make data requests most frequently, and the ICANN staff that will be tasked with managing the SSAD and oversight. Priorities and response times can be worked out by this team and should reflect the use cases typically seen and their relative urgency with respect to timeliness, impact, and/or other mutually agreed-upon factors. The list in Recommendation 6.1.1 for Priority 1 requests in the report provides a starting point for such discussions but is by no means complete. Final recommendations for the implementation to support this framework should be reviewed and approved by the GNSO council. Over time these factors can be revisited and adjusted using the evolutionary mechanism as envisioned in Recommendation 18 or its equivalent that is finally adopted.

4 Objection to Recommendation 6 on Priority Levels

Absent of a better approach to the question of priorities and SLAs as outlined above, the SSAC objects to 6.1 and 6.2.

The classification of cybersecurity threats as "Priority 3" falls woefully short of addressing today's online threats. These classifications fail to address some of the most serious online attacks perpetrated today that require nimble responses. Such attacks are creating massive financial impacts and exposing millions of sensitive personal records online, e.g. ransomware, data exfiltration networks, and massively scaled DDoS attacks for extortion. This classification system needs further work to reflect the timeliness and impacts of various forms of attacks. At the very least, such a system would provide a policy framework that can guide practical implementation processes for addressing the need for timely data depending upon multiple

factors. If recommendation 6 is not updated to account for the need for timely responses for various attacks, then tighter limits under recommendation 10 (Determining Variable SLAs for response time for SSAD) are needed to provide data to support response efforts to such attacks. The SSAC previously outlined further rationale for this approach in SAC111, Section 3.2.[11]

5 Objection to Recommendation 10 on Determining Variable SLAs for response time for SSAD

Absent of a better approach to the question of priorities and SLAs as outlined above, the SSAC objects to Recommendation 10. While the recommendation has a good goal, the SSAC does not support this recommendation as written. Its logic is flawed, and it does not provide a reasonable SLA for responding to security threats. This is, in part, due to the classification of security threats as "Priority 3" in recommendation 6 (Priority Levels).[12] This is too slow to address cybersecurity incidents.[13]

The SLA target in Phase 1 is five (5) days. But then Section 10.11 says: "In Phase 2, Contracted Party compliance targets for SSAD Priority 3 requests will be ten (10) business days." Unfortunately, there is no binding SLA at all in Phase 1, and a binding SLA with a penalty only comes into effect in Phase 2. The Phase 2 SLA allows contracted parties to respond *more slowly* than in Phase 1, rather than more quickly as they gain experience. Ten days is simply too long for security and stability purposes. This proposal has not changed significantly since the preliminary report, and at the time, the SSAC noted its objection to this contradictory approach in SAC111, Section 3.2:

> These targets are misaligned with the reasons that the SSAD is being created. Cybersecurity requests are usually a high priority. They will usually be operational in nature and are about preventing active and ongoing harm to multiple victims of the public during attacks (e.g., malware and phishing). Nor are operational cybersecurity requests less urgent than URS requests. Further, the overall model for the SSAD assumes that cybersecurity requests will be made by accredited parties, within an accountable system, thus mitigating the need for an extended review. SSAC recommends that operational security requests (by accredited parties) be moved to Priority 2. If the volume of cybersecurity requests is of concern to the Contracted Parties, then a compromise for response within three (3) business days would be reasonable.
>
> Requestors and contracted parties will gain confidence and improve efficiency over time, and so there is no reason for the response times to get longer and more relaxed over time. Thus, it does not make sense to increase the length of time a data controller has to respond (as defined in the SLA) from Phase 1 to Phase 2 for any priority level of requests—they should stay the same or decrease between phases for the same priority.

[11] See SAC111

[12] Other than the rate cases involving "an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation."

[13] Only a tiny percentage of security issues and cybercrimes will reach the high bar for Priority 1 handling, which requires "an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation."

The SSAC is concerned that the SLAs are not practically enforceable, and that the implementation advice presents issues. The response time SLA involves a rolling average of all response times. A contracted party could reject all data requests quickly or could request more information for all requests immediately. This will generate a very low average response time for the contracted party. This would then allow the contracted party to delay other requests for long time periods before violating the response SLA. Such automated actions are not prohibited by Recommendation 8.1. It is therefore important that ICANN's Compliance Department be able to determine whether contracted parties are examining requests and have replied in compliance with Recommendation 8. We are not sure how ICANN Org staff could determine this, and so we are not sure the SLAs are practically enforceable.

6 Objection to Recommendation 12 on Disclosure Requirement

Recommendation 12.2 will allow contracted parties to reveal the identities of data requestors whenever they desire, even allowing the "outing" of data requestors as a routine and automated procedure. The recommendation therefore may exceed or violate advice given to ICANN by the European Data Protection Board (EDPB), which said it is not necessary to push the identities of data requesters to data subjects (registrants). Revealing the identities of data requestors will compromise investigations and may endanger the safety and rights of data requestors, and may chill the use of Article 6 requests, which was surely not an intent of the GDPR. The contracted party may need to satisfy a balancing test in order to reveal a requestor's identity, because third-party data requestors are data subjects and have rights under GDPR as well.

Recommendation 12 should prohibit contracted parties from revealing the identities of data requestors unless and until it is *required* by applicable law. We recommend that data controllers comply with the law and not do more. Reiterating SAC055 and SAC101v2, "the SSAC believes that law enforcement and security practitioners have a legitimate need to access the real identity of the responsible party(ies) for a domain name. Such access must comply with legal requirements."

In its letter of 10 May 2018, ICANN asked the European Data Protection Board (EDPB):

> "a) Must the identity of the person/entity submitting a WHOIS query be required to be visible to the registrant or other third parties?" …
>
> b) Must requests from law enforcement for access to non-public WHOIS be required to be visible to the registrant or third parties?"

In response, the EDPB said:

> "Ensuring traceability of access through appropriate logging mechanisms does not necessarily require active communication (pushing) of log information [the identities of data requestors] to the registrant or third parties. It is up to ICANN and other controllers participating in the WHOIS system to ensure that logging information is not disclosed to

> unauthorized entities, in particular with a view of not jeopardizing legitimate law enforcement activities."[14]

The GDPR requires that data controllers must, when offering services, generally inform data subjects about what *types* of parties may process their data. The GDPR does not require that data subjects be actively notified when their data has been requested. The GDPR may only require that data controllers turn over the identities of third-party data requesters to data subjects *if and when the data subject requests that information*.

Revealing the identity of a data requestor poses some issues for the Contracted Parties. Revealing the identities of data requestors prejudices and chills the use of GDPR Article 6 requests. It can seriously impair the procurement of data that is required for legitimate purposes under GDPR—such as the mitigation of cybercrime, the defense of victims, and investigations that may lead to court cases or enforcement actions. There is apparently an exception in the GDPR regarding a data subject's right to be informed, when revelation or notification may impair the ability of a party (such as a third-party requester) to achieve its legitimate purposes.[15] This may occur in an investigatory context.[16]

These issues were not examined by the EPDP, and the EPDP did not receive adequate legal advice about them. We wonder what rights data requestors are entitled to—they are data subjects, and their data is protected under GDPR too. In order to make an Article 6(1)f request, can a data requestor be forced to give up its privacy rights to the data subject or to the data controller? (GDPR says that no data subject can be compelled to give up its privacy rights as a condition of a contract.) And would it not be fair that the contracted party tell the data requester that the contracted party has shared the requestor's identity with the registrant, thereby notifying both parties?

The SSAC presented questions about these issues to the EPDP and its legal sub-team, proposing that the questions be sent for outside legal advice. The EPDP denied this request and the questions were never sent to Bird & Bird. As a result, the EPDP is not fully informed, and is allowing excesses that are not necessary and will be harmful.

7 Objection to Recommendation 14 on Financial Sustainability

SSAC rejects Recommendation 14.2 and 14.6.

The following language in 14.2 is unacceptable:

[14] See Letter from Andrea Jelinek, Chairperson EDPB, to Goran Marby, ICANN CEO, 5 July 2018, https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf
[15] See GDPR Article 14, paragraph 5
[16] See The Right to Be Informed: Are There any Exceptions? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/are-there-any-exceptions/#:~:text=There%20is%20no%20automatic%20exception,a%20specific%20exception%20or%20exemption

> The objective is that the SSAD is financially self-sufficient without causing any additional fees for registrants. Data subjects MUST NOT bear the costs for having data disclosed to third parties; Requestors of the SSAD data should primarily bear the costs of maintaining this system. Furthermore, Data Subjects MUST NOT bear the costs of processing of data disclosure requests, which have been denied by Contracted Parties following evaluation of the requests submitted by SSAD users. ICANN MAY contribute to the (partial) covering of costs for maintaining the Central Gateway. For clarity, the EPDP Team understands that registrants are ultimately the source of much of ICANN's revenue. This revenue does not per se violate the restriction that "[d]ata subjects MUST NOT bear the costs for having data disclosed to third parties.

1) Data requestors should not primarily bear the costs of maintaining the system.[17] Requestors should certainly pay the cost of getting accredited and maintaining their access to the system. But the current language of 14.2 makes victims and defenders cover the costs of the system's operation, which is unfair and is potentially dangerous for Internet security. As the SSAC noted in SAC101v2, "A non-free system [where data requestors must pay fees for queries] could make the cost of the queries required to locate and mitigate domain abuse prohibitively expensive and very difficult operationally."

2) This pronouncement is sweeping and can still be misinterpreted: "Data subjects MUST NOT bear the costs for having data disclosed to third parties." It was then modified with this language: "For clarity, the EPDP Team understands that registrants are ultimately the source of much of ICANN's revenue. This revenue does not per se violate the restriction that "[d]ata subjects MUST NOT bear the costs for having data disclosed to third parties."

That language still prevents registrars from passing the costs of the SSAD program on to their registrants in the normal course of business. Contracted parties generally execute their core responsibilities as a cost of doing business and may pass the costs on to their customers.[18] But 14.2 prohibits that. No previous PDP has protected registrants from having the costs associated with "core" registration services or the implementation of consensus policies being passed on to them. No previous PDP has tried to manipulate the functioning of market forces as is proposed in Recommendation 14.

If the goal is simply to prohibit registrars from charging a service fee to a registrant when a third party actually requests that registrant's data, then just say that, clearly and concisely.

3) The SSAD should not necessarily be "financially self-sufficient," and there is insufficient rationale provided by the EPDP to require that. As previously stated,[19] The SSAC believes that the initiation of charges for RDDS access, or any significant future changes in fees for RDDS access, must include a formal assessment of user impacts and the security and stability impacts. The EPDP did not study the associated issues as requested and has not justified the policy recommendation as required by GNSO procedure. The language in 14.2 also ignores SSAC

[17] See also Recommendation 14.6

[18] See SAC101v2, section 5.4

[19] See SAC101v2 and SAC111

advice to the ICANN Board, which the Board passed to the GNSO. All of these factors make Recommendation 14 premature.

On 23 June 2019 the ICANN Board considered SAC101v2 and referred its recommendations to the GNSO Council for consideration for inclusion in the EPDP Phase 2 work. The advice stated: "The initiation of charges for RDS access, or any significant future changes in fees for RDDS access, must include a formal assessment of user impacts and the security and stability impacts, and be conducted as part of a formal Policy Development Process (PDP). And: "The ICANN Board should ensure that a formal security risk assessment of the registration data policy be conducted as an input into the Policy Development Process. A separate security risk assessment should also be conducted regarding the implementation of the policy."[20]

Those assessments of user impacts and the security impacts were never conducted anywhere. It is inappropriate for the EPDP to assign costs to SSAD data requesters without assessing the impacts on them, and without assessing the impacts on DNS security.

When the EPDP created Recommendation 14.2, it did not follow GNSO procedures, and it is therefore unjustified as a policy proposal. The GNSO's PDP Manual specifically states that: "The PDP Team should carefully consider the budgetary impacts, implementability, and/or feasibility of its proposed information requests and/or subsequent recommendations." The GNSO PDP Manual also requires "a statement on the WG discussion concerning impact of the proposed recommendations, which could consider areas such as economic, competition, operations, privacy and other rights, scalability and feasibility" be included in the Initial Report".

But the EPDP did not examine the budgetary and implementability impacts on *data requestors*. The EPDP did not examine the budgetary and implementability impacts in general, other than to receive a vague and undocumented estimate of startup costs for the central system provided by ICANN Org staff. The EPDP never studied the competition and operations dimensions and did not assess how access charges will impact security and stability. The language of 14.2 has not been appropriately studied and justified.

After Recommendation 14.2's wide policy pronouncements, the Final Report says that all the details should be handled in the Implementation Phase. The Implementation Phase is an inappropriate place to consider such fundamental policy issues, and any implementation will have to follow the flawed and unjustified principles currently in 14.2.

4) It is not necessary to force data requestors to "primarily bear the costs of maintaining the system." The use of ICANN funds is a viable alternative.

The SSAD is the tiered access system that the ICANN community has long anticipated as a feature of the RDS system.[21] Registration data services have always been a core service offering

[20] See Board resolution of 23 July 2019, https://features.icann.org/consideration-ssac-advisory-regarding-access-domain-name-registration-data-sac101

[21] The ICANN community has thought of tiered or differentiated access as a forthcoming feature of Registration Data Directory Services. For example, the RDAP protocol was designed specifically to provide tiered/differentiated access, because the community understood that privacy laws might require certain kinds of data to be shared only

provided by contracted parties as a public resource.[22] As anticipated for some years, tiered/differentiated access has now been necessitated by changes in the law. The SSAD will serve a core need that is in the public interests. It is therefore unusual that Recommendation 14 basically prohibits ICANN domain registration fees from being used to support the system's operation.

The use of ICANN funds seems highly congruent with ICANN's mission. The Temporary Specification also reminds us that "ICANN is generally committed to "maintaining the existing WHOIS system to the greatest extent possible," and "ICANN's mission directly involves facilitation of third party processing for legitimate and proportionate purposes related to law enforcement, competition, consumer protection, trust, security, stability, resiliency, malicious abuse, sovereignty, and rights protection." For more about the relevant ICANN mission commitments, see SAC101v2, section 5.4.[23]

A similar example is the Central Zone Data Service (CZDS), which ICANN built and maintains with ICANN funds. ICANN does that because zone files are a critical resource used for legitimate purposes by a variety of users. And the CZDS provides benefits not only to its users but also to contracted parties, who receive a convenient way to manage zone file subscriptions. The SSAD presents the same situation and is designed to provide benefits to both its data requesters and to the contracted parties.

5) This sentence was a last-minute addition to Recommendation 14: "Furthermore, Data Subjects MUST NOT bear the costs of processing of data disclosure requests, which have been denied by Contracted Parties following evaluation of the requests submitted by SSAD users." It is unclear why this addition is even necessary, and it calls into question whether costs of evaluating data requests can be passed on to registrants in any way, even in the normal course of business.

6) The recommendation says: "Data subjects MUST NOT be charged a separate fee by the Central Gateway for having their data requested by or disclosed to third parties." We don't see how the Central Gateway could conceivably charge registrants. The Central Gateway has no business relationship with registrants.

7) The actions of *registrants* are generally what cause third parties to submit data requests.

8) The SSAC does not know whether Recommendation 14 will violate GDPR.

Recommendation 14 (including 14.6) envisions that data requestors will pay fees to make data requests. A usage fee is the only way to achieve the "cost recovery" model envisioned in Recommendation 14.2 and 14.6, or to run the system without passing costs on to domain holders/data subjects.

with authorized users. Now SSAD is being contemplated as the way to provide sensitive data (and may or may not employ RDAP).

[22] See SAC101v2, section p.4

[23] See SAC101v2

Per GDPR, if data subjects want to receive, update, or request deletion of their data, they cannot be charged for that.[24] Under GDPR, third parties with legitimate interests may receive the data when their right to it outweighs the interests of the data subject. In SSAD, third parties will usually make such requests because they can make a legitimate case that their rights are being violated by a data subject (registrant). The EPDP did not examine whether charges for third-party data requests are allowed under the GDPR, or under what circumstances. The EPDP did not seek legal advice on this issue, even after the SSAC proposed that the question be sent for outside legal advice.

This problem can be avoided if ICANN subsidizes the SSAD.

8 Other Comments

Below are comments on other recommendations, which the SSAC did not object to, but can be improved. We commend these comments to the GNSO for consideration.

Regarding Recommendation 14:
Recommendation 14.8 is flawed and is probably unnecessary. It says: "When implementing and operating the SSAD, a disproportionately high burden on smaller operators should be avoided." We do not believe that anyone knows what a "disproportionately high burden on smaller operators" means, or what the implications of this language are. It is clear that each and every registrar and registry operator, no matter how large or small, will be required to use the SSAD. There may be a minimum amount of effort required for any "operator" to use it. That will be a cost of doing business in the gTLD space and maintaining ICANN accreditation. Our concern is that 14.8 not be used as a way to strip the SSAD of necessary functionality.

Recommendation 14's Implementation Guidance section also needs to be revised accordingly.

Recommendation 18.2.3 says: "Recommendations on SSAD operations and policies developed by the Standing Committee must achieve consensus of the members of the Committee in order to be sent as formal recommendations to the GNSO Council. For recommendations to achieve a consensus designation, **the support of the Contracted Parties will be required**." (emphasis added)

The Standing Committee can make two kinds of recommendations:

- One kind are recommendations for binding contractual changes. When voted on by the GNSO, these must meet a high (supermajority) bar per the ICANN Bylaws. These basically require the approval of the Contracted Parties in order to pass.
- The other kind are implementation recommendations. They will not become contractually binding on the Contracted Parties.

[24] See GDPR Article 15, Article 57(4), and the Information Commissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/. GDPR allows data subjects to be charged only when their requests are "manifestly unfounded or excessive." In the SSAD, data requests that are unfounded or excessive are not allowed and will be rejected.

The problem is that Recommendation 18 applies the high, supermajority bar to both cases, but should only apply to the first case. As written, Recommendation 18 gives the contracted parties veto power over implementation choices. As far as we are aware, it is not a standard GNSO decision-making process to give any party or house veto power over this level of decision.[25]

There is also a practical problem: we do not know if SOs and ACs will want to take part in the Standing Committee if implementation matters can be vetoed by one or two participants.

We do not see how implementation issues would rise to the level of the GNSO Guidance Process, which requires a supermajority vote.

[25] We do not see how implementation issues would rise to the level of the GNSO Guidance Process, which requires a supermajority vote.

9 Acknowledgments, Statements of Interests, Dissents, Alternative Views and Withdrawals

In the interest of transparency, these sections provide the reader with information about aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who contributed directly to this particular document. The Statements of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member's participation in the preparation of this Report. The Dissents and Alternative Views section provides a place for individual members to describe any disagreement with, or alternative view of, the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this report is concerned. Except for members listed in either the Dissents and Alternative Views or Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

9.1 Acknowledgments

The committee wishes to thank the following SSAC members for their time, contributions, and review in producing this report.

SSAC members
Greg Aaron
Benedict Addis
Ben Butler
Steve Crocker
James Galvin
Merike Kaeo
John Levine
Rod Rasmussen
Tara Whalen

ICANN staff
Andrew McConachie
Danielle Rutherford
Kathy Schnitt
Steve Sheng (editor)

9.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2019-11-20-en

9.3 Dissents and Alternative Views

There were no dissents or alternative views.

9.4 Withdrawals

There were no withdrawals.