FINAL Comments of the IPC
on the Interim Report of Phase 2 of the EPDP

Recommendation 1: Accreditation [insert hyperlink]

1. **Please choose your level of support for Preliminary Recommendation 1:**
   Mark only one oval.

 Support Recommendation as written

 Support Recommendation intent with wording change

 No opinion

 Significant change required: changing intent and wording

 Recommendation should be deleted

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

The IPC supports the framework and principles outlined in this recommendation and believes it will form a solid foundation to ensure an effective, efficient and legally sound access to the SSAD system.

We believe however that it should be improved to include the concept of an Accredited Entity who is also a Trusted Notifier. Accredited Entities who are also Trusted Notifiers are subject matter experts that have been additionally vetted to monitor and investigate issues of illegal activity and abuse. Befitting their designation, Accredited Entities who have been vetted to be a Trusted Notifier have an established reputation for accuracy, a recognized relationship with the ecosystem and a proven record of following the defined process for requesting access to non-public Registration Data via the SSAD.

The accreditation period should be as long as possible, to reduce the burden of having to frequently seek re-accreditation.

There should be a specified appeal mechanism for any decisions to de-accredit an accredited user on the basis of an alleged violation of the system.

Recommendation 2: Accreditation of governmental entities

3. **Please choose your level of support for Preliminary Recommendation 2:**
   Mark only one oval.

 Support Recommendation as written

Support Recommendation intent with wording change

 No opinion

 Significant change required: changing intent and wording

 Recommendation should be deleted

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

Under “Objective of accreditation,” the statement “SSAD SHOULD ensure reasonable access….” ought to be changed to “SSAD MUST ensure reasonable access….”

Under “Accreditation procedure,” the statement “This authority SHOULD publish the requirements….” ought to be changed to “This authority MUST publish the requirements….”

Recommendation 3: Criteria and Content of Request

5. **Please choose your level of support for Preliminary Recommendation 3:**
   Mark only one oval.

 Support Recommendation as written

□ **Support Recommendation intent with wording change**

□ No opinion

□ Significant change required: changing intent and wording

□ Recommendation should be deleted

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

Regarding the intent of the recommendation. The recommendation should clarify what is meant by "standardization" in this context. In other instances, the Interim Report uses "standardization" and "standardized" in the context of how the Contracted Parties decide whether to disclose or not. Here, since requests will be submitted via a centralized SSAD Central Gateway, the gateway will have a *unique* - rather than merely "standardized" - set of information the requestor must submit. However, if "standardization" refers to standardization between different types of requests (between cybersecurity, IP enforcement, consumer protection, etc.), then we support this objective and ask that this meaning be spelled out.

Regarding the wording of the recommendation. First, the Central Gateway should present lists of pre-populated fields to the requestor (e.g. a list of third party purposes/justifications.) These lists may or may not be exhaustive, depending on the fields. This would streamline the request and decision-making process and thus help the SSAD reach its predictability objective. Second, the wording of Recommendation 2 needs to be aligned with that of Recommendation 6:

1. in c) replace "specific rationale" and "basis or reason for the request" with "legitimate interest or other lawful basis"; and
2. in e) replace "adequate, relevant and limited to what is necessary" with "necessary."

Recommendation 4: Third Party Purposes/Justifications

7. **Please choose your level of support for Preliminary Recommendation 4:**
   Mark only one oval.

Support Recommendation as written

Support Recommendation intent with wording change

No opinion

Significant change required: changing intent and wording

Recommendation should be deleted

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

No comment required

Recommendation 5: Acknowledgement of Receipt

9. **Please choose your level of support for Preliminary Recommendation 5:**
   Mark only one oval.

Support Recommendation as written

Support Recommendation intent with wording change

No opinion

 Significant change required: changing intent and wording

 Recommendation should be deleted

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

The wording of the first paragraph should be aligned with the wording of Recommendations # 8 (Response Requirements) and 16 (Automation), to read: “The EPDP Team recommends that the Central Gateway provide an immediate and synchronous response that indicates the receipt of a valid request”, rather than “without undue delay”, which won’t be a problem for an automated system and will maximize its efficiency. There is no reason to impose on a computer system a promptness requirement that is more appropriate for humans.

Recommendation 6: Contracted Party Authorization

11. **Please choose your level of support for Preliminary Recommendation 6:**
    Mark only one oval.

 Support Recommendation as written

 Support Recommendation intent with wording change

 No opinion

 Significant change required: changing intent and wording

 Recommendation should be deleted

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

Bullet point 1

The second sentence should be edited as follows:

- "Legally and technically permissible": ‘technically permissible’ doesn’t make sense, so the wording should be aligned with that of the automation Recommendation to read "legally permissible and technically feasible."
- “Not explicitly prohibited” creates a clear bias against automated review, which is unwarranted in cases where it is “legally permissible.” Replace with “allowed.”

Bullet point 2

No comments.

Bullet point 3

No comments.

Bullet point 4

GDPR requires that data be processed if it is necessary to the purpose of processing. That assessment is normally relatively easy for a controller because they ‘know their business’: they know their purpose and how it can/must be pursued. In the context of requests by a third party, that assessment becomes much more difficult: with a large number of different types of requestors pursuing a wide variety of purposes and operating in different legal jurisdictions with potentially different legal requirements (if the request’s purpose is to support a lawsuit), how can the requestor have any meaningful expertise in what data elements are “more than

desirable but less than indispensable or absolutely necessary" to the pursuit of each and every one of these purposes? The IPC recommends the following:

- The gateway must present to requestors an indicative list of necessary data elements, with corresponding explanations of their respective necessity. This list shall be developed by the gateway on the basis of the use cases created by the EPDP (https://community.icann.org/display/EOTSFGRD/d.+Use+Cases). This list may be adapted, over time, by the Mechanism for the Evolution of SSAD on the basis of: its review of proposals by Contracted Parties to remove data elements from the list; its review of proposals presented by experts; and additional data elements whose necessity has been accepted by Contracted Parties.
- The requestor may use the indicative list, in whole or in part, in which case the Contracted Party shall accept the necessity of the data elements that are on the indicative list;
- In addition to or instead of the indicative list, the requestor may request data elements not on the list but whose necessity the requestor can explain. The Contracted Party shall determine whether these data elements are necessary.

The IPC also recommends changes to the first sentence of the second to last paragraph of p.26: while the lack of a lawful basis may be grounds for denying an entire request, the lack of necessity of a specific data element should not. The sentence should therefore read:

> "If the requestor has not provided a legitimate interest or other lawful basis in processing the data, the Contracted Party MAY deny the request, or require further information from the requestor before proceeding to bullet #5 below. If a requested data element is not necessary to the requestor's stated purpose, the Contracted Party may

deny disclosure of this data element, or require further information from the requestor before proceeding to bullet #5 below."

Bullet point 5

"May" should be changed to "must" in the first sentence, to require the CP to determine whether personal data is present. If it is not, the protections required by privacy laws like the GDPR and contained in bullet point 5 should not be extended to non-personal data.

In the second sentence, the purpose of bullet point 5 is incorrectly stated. It should be restated as follows: "The purpose of bullet point #5 is to determine whether the data requested contains personal information, and if it does to determine how the balancing test should be performed." In any case, the second sentence says bullet point 6 is about meaningful human review: it's not. Delete "whether bullet point 6" from the sentence.

We have an opportunity to tighten up this bullet: "The applicable lawful basis and whether the requested data contains personal data for the Contracted Party to determine if the balancing test, similar to the requirements under GDPR's 6.1.f, as described in paragraph 6 below is applicable and proceed accordingly." Since, the preceding paragraph addresses the absence of personal data and, bullet 5 describes the balancing test we should update the sentence to read: "The applicable lawful basis to determine if the balancing test, similar to the requirements under GDPR's 6.1.f, is applicable and proceed accordingly."

The IPC also recommends the following changes and additions to the factors the CP should evaluate in its balancing test:

- Additional factor: evaluate the importance of the legitimate interests pursued by the requestor, including the defense of rights recognized by Article 17 (property rights) and Article 27 (moral and material interests resulting from scientific, literary or artistic production) of the Universal Declaration of Human Rights, and by applicable national laws such as Article 1, Section 8, Clause 8 of the Constitution of the United States (intellectual property.)
- Changed factor: under “scope of processing”, the EPDP should clarify when the combination of data elements does and does not create a higher risk.

Bullet point 6

First, the revisions should not be limited to taking into account legal developments pertaining to the GDPR, but also to legal developments pertaining to other applicable laws. Second, the revisions should be subject to community review.

Recommendation 7: Authorization for automated disclosure requests

13. Please choose your level of support for Preliminary Recommendation 7:
Mark only one oval.

 Support Recommendation as written
 Support Recommendation intent with wording change
 No opinion

Significant change required: changing intent and wording

 Recommendation should be deleted

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

The IPC believes that automation of the receipt, authentication, and transmission of SSAD requests as well as automated disclosure of non-public registration data is an important and positive mechanism that will allow more efficient response to DNS abuse. However, as currently written, Recommendation #7 too narrowly limits the types of disclosure requests that are authorized for Day 1 automation, listing only: (1) Requests from Law Enforcement in local or otherwise applicable jurisdictions; and (2) Responses to UDRP and URS Providers for registrant information verification.

The IPC believes this strict limitation is a counter-productive way to implement the otherwise very useful and efficient mechanism of automation. Rather, there should be full automation from Day 1 for as many types of disclosure requests as are practically and legally possible. At a minimum, the IPC suggests Recommendation #7 be revised to include, on top of the initial two types of requests listed above, the following:

1. Requests where:
    a. the data subject is a legal person [to the extent that such information is not publicly available in WHOIS]; and/or
    b. neither the data subject nor the Contracted Party are subject to EU law [to the extent that such information is not publicly available in WHOIS]; and/or
    c. the data subject has consented to make their registration data public;
2. Requests that are made by officers of the court, made under penalty of perjury, and include a good faith assertion that a clearly identified and protectable IP right is being infringed through use of an identified domain name;

(https://www.americanbar.org/news/reporter_resources/midyear-meeting-2020/house-of-delegates-resolutions/101b/)

3. Requests relating to domains registered in new gTLDs that only permit legal entities to register domain names (e.g., .BANK)
4. The other use cases identified and examined by the EPDP team (https://community.icann.org/download/attachments/126424070/Use%20Cases%20That%20Support%20Automated%20Disclosure%20Decisions%20v2.01.docx?version=1&modificationDate=1581343809000&api=v2)

The language in subsection 1 "(and is confirmed during the implementation phase)" is confusing and potentially problematic. The policy should not require confirmation during the implementation phase; it should simply be implemented. Also in subsection 1 the reference to "the criteria established in these policy recommendations" is too ambiguous. This recommendation should clearly include all requirements for a request to qualify for automation.

The IPC cautions that Contracted Parties should neither be asked nor expected to evaluate the merits of a potential trademark claim or the need for a trademark investigation. We appreciate the desire to reduce Contracted Parties' risk, and to protect data subjects' privacy rights, and we remain committed to these objectives. However, we must caution that delegating trademark-related access requests to contracted parties does not further these interests, and actually increases risk.

Finally, the IPC believes that if the Mechanism for the evolution of SSAD identifies additional categories of requests that could be fully automated, the SSAD ***must***

allow for automation of their processing and the requests ***must*** be

automatically processed and result in the disclosure of non-public RDS data without human intervention if legally permissible.

Recommendation 8: Response Requirements

15. **Please choose your level of support for Preliminary Recommendation 8:**
    Mark only one oval.

□ Support Recommendation as written
X Support Recommendation intent with wording change
□ No opinion
□ Significant change required: changing intent and wording
□ Recommendation should be deleted

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

The IPC generally supports Recommendation #8, but believes certain revisions to the recommendation will make the SSAD more efficient.

In c) under "For the Central Gateway Manager":

- The report should clarify that the gateway will provide automated recommendations (to disclose or deny disclosure), rather than have personnel review requests and generate these recommendations. The gateway will be uniquely positioned to provide automated

recommendations because it will have access to considerable amounts of data about the SSAD: categories of requests, track record of requestors, ambiguity (or lack thereof) of certain types of requests, etc.

- Instead of allowing the Central Gateway Manager to provide a recommendation to the Contracted Party whether to disclose or not, the Central Gateway Manager should be required ("must" instead of "may") to do so, because it is unclear when it may not be advisable or possible for the Central Gateway Manager to do so. For the same reason, we believe that specifying *when* the Central Gateway Manager may provide such recommendations (e.g. for certain types of requests or requestors) would not be sufficient either.

In d) under Contracted Parties: the sentence "such exceptional circumstances (...) established SLAs" should be deleted because it creates three problems. First, Recommendation # 9 (SLAs) neither includes nor implies "numbers of requests" that are beyond the SLAs (nor should it), so the sentence creates a loophole for SLA compliance; for example, CPs should be required to staff up to a level that enables them to process usual and unusual numbers of requests. Second, it does not actually limit in duration the circumstance in which a large number of requests allows non-compliance with SLAs (not that the IPC would support such a time-bound exception), so we are concerned that large numbers of requests that come in over months and months would excuse non-compliance with the SLAs.

In e) under Contracted Parties: responses where disclosure of data has been denied should also identify how to appeal a determination or re-submit a request to address or overcome the reasons for denial.

In f) under "Urgent SSAD Requests": the IPC recommends greater clarity of the criteria for urgent requests beyond the broad "circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation." Clarification, ideally with illustrative examples, will be important to mitigate disputes between requestors and Contracted Parties as to what qualifies as an urgent request. Additionally, requestors are not given much clarity with this language to help them avoid penalties for abusing urgent SSAD requests, which a requestor could accidentally incur despite best intentions given the current language.

In the first paragraph of p.31: the CP should be required to document the rationale for non-disclosure and communicate it to both the requestor and ICANN Compliance in all circumstances, regardless of the reason for denial and without requiring that ICANN Compliance request it. Additionally, the requestor should be afforded the right to appeal a denial, and be informed by the gateway of the procedure for such an appeal.

The second paragraph of p.31, should make it clear that ICANN Compliance MUST investigate all complaints, and not just "be prepared to investigate" them. Additionally, greater detail should be included here to outline what criteria ICANN Compliance will use to evaluate these complaints.

Recommendation 9: Determining Variable SLAs for response times fo SSAD

17. **Please choose your level of support for Preliminary Recommendation 9:**
    Mark only one oval.

 Support Recommendation as written

Support Recommendation intent with wording change

 No opinion

 Significant change required: changing intent and wording

 Recommendation should be deleted

18. **If your response requires an edit or deletion of Recommendation #9, please indicate the revised wording and rationale here.**
19. **If you do not agree with the proposed SLA matrix and/or accompanying description, please provide your rationale and proposed alternative language.**

The IPC supports this Recommendation with the following proposed changes.

Incorporate the clarifications offered by the BC in this document https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20200304/72314f67/EPDPPhase2SLAproposaldetailclarification-0001.pdf into the final EPDP Phase 2 report.

Mirroring a policy recommendation from the RPM WG Initial Report (https://gnso.icann.org/sites/default/files/file/field-file-attach/rpm-phase-1-initial-18mar20-en.pdf), the IPC recommends that the Registry Agreement and Registrar Accreditation Agreement include a provision stating that the contracted party shall not act in such a way as to have the

effect of circumventing the purpose of SSAD, e.g. defaulting to denials of disclosure to meet SLAs etc.

Changes regarding priority level 3 (normal requests)

1. Each disclosure request MUST receive a substantive response in 5 business days or less. When it doesn't, the gateway shall send an automated alert to ICANN Compliance and ICANN Compliance shall investigate without undue delay.
2. SLA enforcement form 1 needs to be strengthened.
    a. In addition to requiring that a CP that does not meet its 5 day response target "participate in a review with [ICANN] Compliance to establish the root cause for exceeding the average response time expectation", ICANN Compliance shall be required to develop a Remedial Plan on the basis of the review. Each Remedial Plan shall be published by the gateway.
3. SLA enforcement form 2 needs to be strengthened.
    a. Every breach of the 10 business days SLA shall be investigated by ICANN Compliance and result in a SLA Breach Report.
    b. The SLA Breach Report shall include: the findings of the investigation; any previous form 1 Remedial Plan developed by ICANN Compliance for the CP in question; and the penalties imposed by ICANN Compliance.
    c. The gateway shall publish the SLA Breach Report.
    d. To determine potential penalties, in addition to complaint volumes and CP size, ICANN Compliance shall take into account: whether and to what extent the CP had implemented all its previous form 1 Remedial Plan; and all aspects of a CP's compliance with the requirements of this SSAD policy.

e. The gateway shall without delay send the SLA Breach Report to each requestor whose request did not receive a response within 10 business days during the relevant time period from the CP in question.
f. A breach of the 10 business days SLA is a breach of the RAA, unless ICANN Compliance provides an explanation to the contrary in its SLA Breach Report.

4. Our recommendations for the mechanism by which the SLA targets shall be reviewed are the same as those we make for the Mechanism for the Evolution of the SSAD (Rec 19.)

Changes regarding priority levels 1 and 2

1. Currently, urgent requests are proposed to be addressed in one business day. The IPC raises concern that if an urgent request is made on a Friday, it will not be addressed until three calendar days later. In these urgent cases, the IPC thinks it best to have a 24 hour response time.
2. To avoid misuse of the priority 1 and 2 levels, the report should require evidence. Recommendation 9 only requires the requestor to assert a priority level, whereas Recommendation 8 (see f), under Urgent SAD requests) mentions "requests for which evidence is supplied to show an immediate need for disclosure." Recommendation 9 should therefore: a. explicitly require the requestor to provide evidence supporting his assertion that a request is a priority 1 or 2; b. provide examples of what evidence would be sufficient for each priority level; and c. if confidential or legally privileged evidence cannot be provided, allow the evidence to be provided in the form of affidavits.
3. The procedure for setting the priority level should be clarified. The following sentence is unclear, as it seems to imply incorrectly that it is the gateway that sets the priority level:

"When selecting a priority, the Central Gateway Manager will clearly state the criteria applicable for an Urgent Request and the potential consequences of abusing this priority setting." The sentence should instead read: "When a requestor sets the priority level of a request as Priority 1 or 2, the Central Gateway will clearly state the criteria applicable for these priority levels and the potential consequences of abusing these priority settings."

4. For the avoidance of doubt, Recommendation 9 should include this sentence from Recommendation 8: "the use of 'Urgent' SSAD Requests is not limited to LEA."

Finally, this recommendation should include an SLA for the Central Gateway's uptime, set at an industry standard level such as 99.9%.

Recommendation 10: Acceptable Use Policy

20. Please choose your level of support for Preliminary Recommendation 10:
Mark only one oval.

□ Support Recommendation as written
□ Support Recommendation intent with wording change
□ No opinion

X Significant change required: changing intent and wording

□ Recommendation should be deleted

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

Preamble: “For the avoidance of doubt, every request does not have to go through an enforcement procedure; the enforcement mechanism MAY, however, be triggered in the event of apparent misuse.” Comment: It should be clarified regarding who can trigger the enforcement mechanism regarding “apparent misuse.” The Centralized Gateway Manager? A Contracted Party? A third-party?

(a) Limiting requested data to only the current RDS data will impose a challenge on brand owners and other third-party requestors. There are a number of reasons it is very important to have the ability to also obtain historical data, for instance to learn the approximate date on which that registrant acquired the domain name (which may differ from the domain’s original creation date by a prior registrant). Accordingly, there should be an option to also obtain historical data that is retained by the Contracted Party upon request.

(b) The “representations” required by this portion of the Recommendation must not be unduly burdensome and should, ideally, be satisfied by a check-the-box list of common reasons for such requests (with a catch-all “Other” checkbox and free text field for stating uncommon reasons). As for the “corresponding purpose and lawful basis for the processing”, the comments set forth pertaining to Preliminary Recommendation #3 “Criteria and Content of Requests” are incorporated here as well.

(c) No comment. We support this criterion.

(d) It is unclear what is meant by the “representation regarding the intended use of the requested data”. If this simply means that the requestor represents that the stated intended use is the actual intended use, then this should be satisfied by a simple checkbox. However, if its meaning is intended to be broader and mean that the intended use must be specifically stated, this seems to be redundant to other parts of the process set out in the recommendations. If the latter is the case, then the representation should be satisfied by a standardized check-the-box list of common intended uses (with a catch-all “Other” checkbox and free text field for stating uncommon uses). Further, the “representation that the requestor will only process the data for the stated purpose(s)” should be satisfied with a simple checkbox.

(e) No comment.

Recommendation 11: Disclosure Requirement

22. Please choose your level of support for Preliminary Recommendation 11:

Mark only one oval.

□ Support Recommendation as written

□ Support Recommendation intent with wording change

□ No opinion

□ **Significant change required: changing intent and wording**

□ Recommendation should be deleted

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

As an initial matter, same comments as above regarding who/how mechanism is triggered regarding "apparent misuse."

(a) No comment.

(b) See comments pertaining to Recommendation 10 concerning disclosure of historical data.

(c) No comment.

(d) Comments on logging appear in the Logging section, Recommendation 17.

(e) With respect to the "balancing test", the comments pertaining to the balancing test set out in Recommendation 6 are incorporated here as well.

(f) The term "reasonable request" as used in this context (as opposed to the disclosure request context) should be further defined so as to avoid any improper denials of requested data and any unnecessary delays in processing the same. This section should also clarify that the "request" in this context is by the data subject itself.

(g) While we do not object to this concept in principle, and agree that such rights are prescribed under certain laws like GDPR, the right to erasure cannot be presented or used as a means of preventing disclosure of data in connection with a reasonable request that has met the applicable balancing test or other criteria for disclosure.

(h) The "privacy policy for the SSAD and standard language (relating to the SSAD) to inform data subjects" should be developed by the SSAD stakeholders and put out for public comment to ensure clarity, accuracy, and neutrality.

(i) It is important that “the nature of legal investigations or procedures” not be limited to criminal investigations by law enforcement or other governmental entities. There are situations where civil investigations may require that requests be kept confidential from the data subject (e.g., where counterfeit goods may be quickly sold or destroyed by a data subject in an attempt at frustrating the enforcement of intellectual property rights). It may be helpful to explicitly confirm this in this section.

Finally, The IPC recommends: that the domain name that is the subject of a disclosure request be locked (using the UDRP definition) during the pendency of a disclosure request; and that any notice to data subjects of disclosure requests not be permitted during the pendency of a disclosure request.

Recommendation 12: Query Policy

24. Please choose your level of support for Preliminary Recommendation 12:

Mark only one oval.

 Support Recommendation as written

 Support Recommendation intent with wording change

 No opinion

X Significant change required: changing intent and wording

 Recommendation should be deleted

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

(a) No comment.

(b) The reference to “ICANN org” as used in this section should be made more specific [“In the event the entity receiving requests makes a determination based

on abuse to limit the number of requests a requestor, further, to point b, the requestor MAY seek redress via ICANN org if it believes the determination is unjustified."] Which part of ICANN Org specifically would have responsibility? ICANN Compliance?

(c) In addition to disclosure relating to "specific domain name[s]" identified in a request, provision should be made for disclosure, upon request, of all domain names owned by the same registrant who is the owner of a specific domain name that is the subject of the initial request about which the Contracted Party to whom the request is directed has such additional information. In addition, EPDP should consider introducing some kind of "trusted requestor" program to expedite responses to similarly-situated requests from a trusted requestor based on pre-defined criteria and use cases. This will help alleviate the cost of examining each request "on its own merits" where the same requestor who has previously demonstrated a pattern of good faith, reasonable, and well-founded requests, submits further requests of a substantially similar nature. Finally, we reiterate our other comments regarding disclosure of historical registration data.

Recommendation 13: Terms of Use

26. Please choose your level of support for Preliminary Recommendation 13:

Mark only one oval.

□ Support Recommendation as written

X Support Recommendation intent with wording change

□ No opinion

□ Significant change required: changing intent and wording

□ Recommendation should be deleted

27. If your response requires an edit or deletion of Recommendation #13, please indicate the revised wording and rationale here.

In general, we support the concept of using appropriate agreements, such as terms of use, a privacy policy and a disclosure agreement to provide rights, duties and obligations concerning access and disclosure of data through SSAD. However, such agreements must be carefully drafted and vetted by the community so that they accurately reflect EPDP policy recommendations and not impose additional obligations or duties or provide imprecise access or disclosure rights. All SSAD stakeholders should be involved in developing these agreements. The EPDP should also clarify how a code of conduct would relate to terms of use and the other agreements discussed in this recommendation, and consider whether all of these agreements could be covered under a single terms of use document.

We recommend the following revised wording of Recommendation 13:

"The EPDP Team recommends that appropriate agreements, such as terms of use for the SSAD, a privacy policy and a disclosure agreement are put in place that accurately reflect the recommendations of the final reports of the EPDP Team. These agreements are expected to be developed and negotiated by all SSAD stakeholders, taking the below implementation guidance into account and any such draft agreements will be published for public comment prior to implementation."

With respect to recommendations concerning proposed Terms of Use, we would suggest that a standard of mere "misrepresentation" to trigger requestor indemnification should be revised to an "intentional, reckless or willful misrepresentations" standard.

Further we note the text stating "The EPDP recommends, at a minimum, the privacy policy SHALL include: Relevant data protection principles, for example,". This sentence appears to abruptly cut off - were there supposed to be particular examples listed here?

Further, we note the text stating "Applicable prohibitions Disclosure". Should this say "Applicable prohibitions on Disclosure"? Please clarify.

Recommendation 14: Retention and Destruction of Data

28. Please choose your level of support for Preliminary Recommendation 14:

Mark only one oval.

□ Support Recommendation as written

X Support Recommendation intent with wording change

□ No opinion

□ Significant change required: changing intent and wording

□ Recommendation should be deleted

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

We support the intent of this recommendation but note that the second sentence of Recommendation 14 might create a contradiction with the requirement of the first sentence in cases where the registration data must be retained under law applicable to the requestor for other reasons or for a longer duration not specific to achieving the purpose of original disclosure. Accordingly, we would suggest the following revision to the wording of Recommendation 14:

"The EPDP Team recommends that requestors MUST confirm that they will store, protect and dispose of the gTLD registration data in accordance with applicable law. Requestors MUST retain only the gTLD registration data for as long as necessary to achieve the purpose stated in the disclosure request, unless otherwise required to retain such data for a longer period under applicable law."

Recommendation 15: Financial Sustainability

30. **Please choose your level of support for Preliminary Recommendation 15:**

Mark only one oval.

□ Support Recommendation as written

X Support Recommendation intent with wording change

□ No opinion

□ Significant change required: changing intent and wording

□ Recommendation should be deleted

31. **If your response requires an edit or deletion of Recommendation #15, please indicate the revised wording here.**

There needs to be a delineation in costs between the development of the SSAD system and its operational costs. We agree that development costs should be initially borne by ICANN Org and Contracted Parties, but that subsequent operational costs should be covered on a cost recovery basis that may take into account historical costs within reasonable parameters.

EPDP should clarify in this recommendation what it means by “smaller operators” in the context of disproportionately high burdens - it seems to imply contracted parties, but it is unclear. No fees for accreditation or disclosure requests must be so high for any class of user or accreditation applicant so as to circumvent their ability to make meaningful use of the SSAD. Overall, the financial burden on all parties to the system should be equal or at least proportionate. System costs should be a component of audits.

We would also support allocation of ICANN Org budget toward offsetting the costs for maintaining the Central Gateway and in general for setting up and maintaining this system.

We would like further specifics regarding the suggested legal risk fund and why such a fund is necessary as part of the costs of this system. All businesses and systems operate subject to some legal risk, so it is not clear why this system necessitates a special fund for its risks.

Finally, this section refers to “input from ICANN Org concerning the expected costs of developing, operationalizing and maintaining the three different models.” This should be updated now that three models are not being considered.

Recommendation 16: Automation

32. **Please choose your level of support for Preliminary Recommendation 16:**

Mark only one oval.

Support Recommendation as written

Support Recommendation intent with wording change

No opinion

Significant change required: changing intent and wording

Recommendation should be deleted

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

Recommendation 17: Logging

34. **Please choose your level of support for Preliminary Recommendation 17:**

Mark only one oval.

Support Recommendation as written

Support Recommendation intent with wording change

No opinion

Significant change required: changing intent and wording

Recommendation should be deleted

35. **If your response requires an edit or deletion of Recommendation #17, please indicate the revised wording and rationale here.**

Subject to the inclusion of our edits, the IPC can likely support the proposed requirements for logging requests and responses. With this information logged, ICANN Compliance can better audit the actions of disclosing entities, identify any instances of systemic non-compliance, and take appropriate enforcement action. This will function as an important backstop to ensure the SSAD system is functioning properly, and free from abuse by accredited individuals or entities that materially breach the conditions of accreditation. Additionally, accredited users who are in compliance can rest assured that a safety net is in place by way of the logging and audit systems—if ever a user needs to challenge a denial of a data disclosure request, the relevant data will be stored and accessible by the appropriate entities.

Therefore, the IPC recommends that the report include the following:

1. For each CP, the Central Gateway must log data about disclosure and non-disclosure decisions. This must include data to:
    a. Measure the rates of: disclosure and non-disclosure; use of each rationale for non-disclosure; divergence between the disclosure and non-disclosure decisions of a CP and the recommendations of the gateway; etc.
    b. Identify if they exist: patterns of compliance and non-compliance; CPs with outlier rates of non-disclosure or of divergence with the gateway; etc.
2. Care being taken to ensure that personal information has been removed, this data must be published in one or more machine readable formats (e.g. CSV, XML or JSON.)
3. ICANN Compliance must have access to all data logged by the gateway, including the data we recommend above, and must review and analyze it to inform its enforcement

activities and audit contracted parties who are not meeting their obligations to provide access under this policy.

4. In e) relevant logs should also be readily available in the SSAD to allow requestors and contracted parties to review their own statistics. These logs shall not contain any personal data.

Recommendation 18: Audits

36. Please choose your level of support for Preliminary Recommendation 18:
Mark only one oval.

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

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

The IPC agrees that the SSAD needs to have sufficient audit mechanisms to enable monitoring and compliance with law and with ICANN policy. There might be a drafting oversight in this recommendation since it merely “expects” that auditing is done to

ensure compliance, but it does not explicitly recommend auditing contracted parties. IPC formally suggests that Recommendation 18 explicitly recommend to audit contracted parties' compliance with this policy.

Recommendation 19: Mechanism for the Continuous Evolution of the SSAD

38. Please choose your level of support for Preliminary Recommendation 19:

Mark only one oval.

- Support Recommendation as written
- **Support Recommendation intent with wording change**
- No opinion
- Significant change required: changing intent and wording
- Recommendation should be deleted

39. If your response requires an edit or deletion of Recommendation #19, please indicate the revised wording here.

With the added input from the Belgian DPA that a centralized model is a "better, 'common sense' option in terms of security and for data subjects", the EPDP should complete its work based on such a centralized model. This could eliminate the need for such a mechanism to gradually shift the SSAD toward greater centralization.

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

This Mechanism, if it exists, must represent the entire ICANN community, and not only the GNSO. It should take into account SSAD users including law enforcement, cybersecurity, intellectual property owners and agents, and other types of end users.

The Mechanism's remit should be to act unidirectionally toward centralization and automation of all cases possible under the law, and the Mechanism must not be able to unwind centralization established by the EPDP without objective evidence of legal risk. It should have sufficient resources to obtain the legal clarity required to justify the centralization of more use cases over time.

The challenge in developing such a Mechanism is that it must be able to require automation for new request types without that power crossing "the picket fence" or being considered to be policy making under the GNSO's remit. The challenge associated with creating such a unicorn further evidences that a centralized SSAD is better.

41. **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?**

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

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

ADDITIONAL RECOMMENDATIONS

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

ICANN, the GNSO and EPDP cannot enact policies for ccTLDs, but some of them have followed the example of ICANN and terminated open access to WHOIS. Therefore, we expect that some may want to follow suit again and participate in the SSAD. The EPDP should reflect on the implications and provide explicitly for ccTLD participation.

As noted above, the EPDP should revisit the possibility of a fully or more centralized SSAD model, in light of apparently inconsistent comments on this subject, calling into question whether such an approach would actually be impermissible under GDPR. IPC would strongly prefer a more centralized/automated approach to SSAD that is more reflective of the historical WHOIS system in terms of querying and disclosure of data.

The EPDP must also present a recommendation for a mechanism for obtaining historical data, to the extent such data is retained by Contracted Parties/ICANN. Historical data is often critical to many legitimate third-party purposes for which SSAD is being created, for instance in order to help trace the chain of title of particular domain names which may be relevant in the course of certain legal disputes (e.g. a UDRP or URS case), to cybersecurity measures, or to law enforcement, among other possible reasons.

ADDITIONAL COMMENTS ON INITIAL REPORT

45. **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.**