**Compilation of Issues Received by Tuesday 4 February 2020**

Instructions: Please review this list, noting, in particular, the proposed changes provided the rightmost column. If your group cannot live with any of the proposed changes, please flag these to the Staff Support Team for further discussion during Thursday's call. Specifically, in advance of Thursday's meeting, please flag the numbers for the issues your group would like to further discuss. Proposed changes not flagged by any group are deemed to be acceptable for inclusion in the Initial Report. As you will note below, the list is divided into two sections. The first table represents the "cannot live with" items, and the second set of issues (beginning on p. 12) represents either minor typographical changes or proposed changes not rising to the level of cannot live with. However, if there are issues in the second list that your group will not accept for inclusion in the Initial Report, please also flag these using the corresponding numbers.

**CANNOT LIVE WITH ITEMS**

| Issue | Line number(s) | Cannot live with rationale | Proposed changes |
|---|---|---|---|
| 1. | 220-224<br>…the SSAD must be automated where technically feasible AND legally permissible…<br><br>Flagged by: NCSG<br><br>Requested to be discussed by: IPC | The MUST language makes automation of disclosure a policy goal that is required whenever possible. This was not the agreement. Automated disclosure should be a narrowly scoped exception to the general practice of manual disclosure review. Automation must have a compelling rationale that makes the specific use case justify it. In practice, automated disclosure means *guaranteed, immediate disclosure of redacted data to any accredited requestor who has presented a properly formatted and complete request*. Since accreditation is available to anyone, automated disclosure *recreates the same indiscriminate access to private data* as the prior Whois regime. That regime was clearly illegal under GDPR and many | ~~Full automation[1] of the SSAD may not be possible, but the EPDP Team recommends that the SSAD must be automated where technically feasible AND legally permissible. Additionally, in areas where automation is not both technically feasible and legally permissible, harmonization is the baseline objective.~~<br><br>**The EPDP Team recommends that the receipt, authentication and transmission of SSAD requests be fully automated insofar as it is technically feasible. The EPDP team recommends** |

[1] See Automation Preliminary Recommendation for further details.

| | | | |
|---|---|---|---|
| | | other DP regimes. The Temp Spec and phase 1 of the EPDP redacted data elements from public Whois precisely because there *should not* be automated or indiscriminate access to those data elements. For this report to define disclosure automation as a "must" contradicts the spirit of the whole EPDP proceeding and risks making the policy legally noncompliant.<br>All language regarding automation must distinguish between the automation of **request processing at the gateway,** and automated **disclosure**. In our view, automation of the former is a policy goal but the latter is not. | **that disclosure decisions should be automated only where technically and commercially feasible, legally permissible and there is a compelling security, stability or resiliency rationale for doing so. In areas where automation does not meet these criteria, standardization of disclosure decisions is the baseline objective.** |
| 2. | p. 9, l. 223<br><br>Flagged by: GAC<br><br>Requested to be discussed by: | "Harmonize" suggests variation and may defeat our goal of trying to keep responses to requests consistent among the 2500+ contracted parties | Full automation[2] of the SSAD may not be possible, but the EPDP Team recommends that the SSAD must be automated where technically feasible AND legally permissible. Additionally, in areas where automation is not both technically feasible and legally permissible, ~~harmonization~~ **standardization** is the baseline objective.<br><br>Change "harmonize" back to "standardize"<br><br>Note: p. 38, l. 1395 uses "standardize," should be consistent no matter what word we choose |

[2] See Automation Preliminary Recommendation for further details.

| | | | |
|---|---|---|---|
| 3. | 227-232<br>In recognition of the expected evolving nature of SSAD and in an effort to avoid having to conduct a PDP every time a change needs to be made, a feedback mechanism, which focuses solely on the implementation of the SSAD and does not contradict ICANN Bylaws, GNSO PDP Procedures and Guidelines, and/or contractual requirements would need to be put in place to oversee and guide the continuous improvements of the SSAD.<br><br>Flagged by: NCSG<br><br>Requested to be discussed by: IPC | Unacceptable for a number of reasons.<br><br>1. Stating that our goal is to "avoid PDPs" invites abuse of process and de-legitimizes the multistakeholder model. Avoiding PDPs is not needed to create an oversight and improvement mechanism.<br><br>2. Strangely, the list of things that should not be contradicted does not include the data subject's privacy rights, the EPDP's policies, and GDPR and other data protection laws. These things must be included.<br><br>3. The formulation of this objective is muddled. It seems to be a halfway house between a true "feedback mechanism" and a "standing committee," many aspects of which were rejected. A feedback mechanism cannot by itself change anything, nor can it "guide," and thus cannot contradict bylaws, procedures, law or policy. In order to avoid evasion of policy and legal constraints, we propose that the "mechanism" be an oversight committee which is a subcommittee of the GNSO, and that its recommendations must be reviewed by the Council to determine whether they involve policy changes | Use this language:<br><br>In recognition of the **need for experience-based adjustments in the functioning of the** ~~expected evolving nature of~~ SSAD ~~and in an effort to avoid having to conduct a PDP every time a change needs to be made, a feedback mechanism, which focuses solely on the implementation of the SSAD and does not contradict~~ **and recommend improvements that could be made. Improvements recommended through this process must not contradict the data subject's privacy rights, the policies established by the EPDP, data protection laws**, ICANN Bylaws **or**~~,~~ GNSO ~~PDP~~ Procedures and Guidelines~~, and/or contractual requirements would need to be put in place to oversee and guide the continuous improvements of the SSAD~~. |

| | | | |
|---|---|---|---|
| 4. | p. 20, l. 651<br><br>Flagged by: GAC<br><br>Requested to be discussed by: | "law enforcement authorities" is sometimes interpreted to mean only criminal LEAs<br><br>Add "Civil and criminal" before "[l]aw enforcement authorities" | Accreditation by a countries'/territories' government body or its authorized body would be available to various eligible government entities that require access to non-public registration data for the exercise of their public policy task, including, but not limited to:<br>• **Civil and criminal** law enforcement authorities,<br>• Judicial authorities,<br>• Consumer right's organizations,<br>• Cybersecurity authorities, including national Computer Emergency Response Teams (CERTs),<br>• Data protection authorities |
| 5. | p. 22, l. 765, 766<br><br>Flagged by: GAC<br><br>Requested to be discussed by: | De-accreditation is a drastic remedy. Should not de-accredit based on unconfirmed complaints or have an overbroad catch-all<br><br>Insert "verified" before "third-party complaint"; delete "otherwise for any" | De-Accreditation will occur when the accreditation authority determines that the Accredited entity has materially breached the conditions of its Accreditation based upon either; a) a **verified** third-party complaint received; b) results of an audit or investigation; or c) otherwise for any misuse or abuse of the privileges afforded. |
| 6. | Rec #3 – Contents of Requests<br><br>Line 775 | The use of the phrase "at a minimum" is problematic as it will allow disclosers (contracted parties) to deny/reject a request simply by asserting they require information that is not | Strike "at a minimum"<br><br>"The EPDP Team recommends that each SSAD request must |

| | | | |
|---|---|---|---|
| | Flagged by: BC/IPC<br><br>Requested to be discussed by: | specified in the existing list. To ensure we meet our principle of predictability we must not allow a situation where a request is denied if additional information not described in this section (and by policy) is required.<br><br>We note however that some information specified in other sections of this policy is missing and should be added. Including 1) the ability to indicate the urgency of a request and 2) to allow LEA to indicate that the request should not be disclosed to the registrant. (There may be others….) | include~~, at a minimum,~~ the following information:" |
| 7. | Rec #5 – Ack. Of Receipt<br><br>Line 812<br><br>Flagged by: BC/IPC<br><br>Requested to be discussed by: | A 2-hour SLA for acknowledgement of receipt of a request is unacceptable. Remember that we are assuming the use of modern web services/web protocols/web servers/etc. In that environment a web client will typically time out after 120 seconds - long before the 2-hour mark hits. (As a thought exercise try to Imagine the last time you submitted a form on a web page and had to wait up to two hours for a response.)<br><br>Note that this recommendation applies to the Central Gateway, not the Contracted Party (i.e. the authorizer/discloser)<br><br>This recommendation also is in conflict with the Automation Recommendation # 16 which states "The SSAD must allow for the automation of an immediate and synchronous response that | The wording in Rec #5 should reference (or be consistent with the language in Rec 16. (line 988)<br><br>e.g.<br>"….by the Central Gateway Manager must be without undue delay and result in an immediate and synchronous response that indicates the receipt of a valid request and some indication that it will be processed. (cf. Recommendation #16 line 988)." ~~not more than two (2) hours from receipt.~~ |

| | | | |
|---|---|---|---|
| | | indicates the receipt of a valid request and some indication that it will be processed. " | |
| 8. | p. 25, l. 899-901<br><br>Flagged by: GAC<br><br>Requested to be discussed by: | Legal proceedings often require public disclosure and this should not weigh against granting a request<br><br>Incorporate bracketed language ("provided that. . .") | ***Scope of processing***. Consider information from the disclosure request or other relevant circumstances that indicates whether data will be [securely] held (lower risk) versus publicly disclosed, made accessible to a large number of persons, or combined with other data (higher risk), ~~[~~provided that this is not intended to prohibit public disclosures for legal actions or administrative dispute resolution proceedings such as the UDRP or URS~~]~~. |
| 9. | 957-961, 1005-1008<br><br>Flagged by: ICANN Org Liaisons<br><br>Requested to be discussed by: | These sections contemplate that CPs may request that the Central Gateway automate approval of additional categories of requests (and retract or revise automation). Is the intention of this to require the Gateway Operator to comply with such requests, or does the Gateway Operator have discretion to determine what additional categories, if any, it will automate upon request? What if a registrar requests automated approval of all requests (is this an acceptable result to the EPDP Team and under the GDPR)? | |
| 10. | 959-960<br>Contracted Party MAY request the Central Gateway to fully automate all, or certain | This sounds like automation of disclosure could be requested by a CP regardless of what our policy is. Obviously not acceptable. | Contracted Party MAY request the Central Gateway to fully automate all, or certain types of, disclosure requests~~, irrespective of the ultimate policy requirements.~~ |

| | | | |
|---|---|---|---|
| | types of, disclosure requests, irrespective of the ultimate policy requirements.<br><br>Flagged by: NCSG<br><br>Requested to be discussed by: | Delete the phrase "irrespective of the ultimate policy requirements." End sentence at "…requests." | |
| 11. | 970 – 973<br><br>Flagged by: Staff Support Team<br><br>Requested to be discussed by: | In response to requests to provide the community more insights into possible use cases being discussed while at the same time not including cases that have not been fully baked, the staff support team would like to propose including a footnote that would lead to a wiki page where automation uses cases that are under review by the EPDP Team are posted. | The EPDP Team will further consider if other types of disclosure requests can be fully automated Day 1*. Over time, based on experience gained and/or further legal guidance, the ~~SSAD Advisory Group~~ **Mechanism for the continuous evolution of SSAD** is expected to provide further guidance on which types of disclosure requests can be fully automated.<br><br>***(footnote) – to review the other types of disclosure requests that the EPDP Team is considering, please see [include link to wiki page].** |
| 12. | 972-972<br>SSAD Advisory Group is expected to provide further guidance on which types of | There is no "SSAD Advisory Group" anymore; there is a "feedback mechanism," which we suggest be an oversight committee which is a subcommittee of the GNSO Council. Also, we want to add the words "if any" to indicate that automation is not necessarily in order | Replace with this:<br><br>"The Council oversight subcommittee is expected to provide further guidance on which types of disclosure requests, if any, can be automated." |

| | | | |
|---|---|---|---|
| | disclosure requests can be fully automated.<br><br>Flagged by: NCSG<br><br>Requested to be discussed by: | | ***Staff note****: This was an oversight – it should read 'The mechanism for the continuous evolution of SSAD' as it is being referenced in other parts of the document. Staff would recommend to use this language as it is made clear in other parts of the document that further discussion will take place to determine what this mechanism will look like. The updated language would read:* ~~SSAD Advisory Group~~ **The mechanism for the continuous evolution of SSAD** is expected to provide further guidance on which types of disclosure requests can be fully automated. |
| 13. | 991-993<br>…the Central Gateway Manager MUST provide a recommendation to the Contracted Party whether to disclose or not.<br><br>Flagged by: NCSG<br><br>Requested to be discussed by: | It makes no sense to require a disclosure recommendation in all cases by the central gateway. By using MUST (which was never agreed in LA) this provision effectively shifts primary responsibility for ALL disclosure decisions to the central gateway manager, i.e. ICANN. Total centralization was an option that could never achieve consensus. The basic model is centralization of requests, decentralized disclosure decisions. Our understanding was that CPs could tell the central body to automate certain decisions, at their discretion. Full automation at the gateway only arise in a few well-defined, carefully circumscribed cases. | DELETE Section c)<br><br>***Staff note****: This was an oversight – the EPDP Team agreed in LA to change 'MUST' to 'MAY'. Also note that this is a recommendation from the Central Gateway, not a requirement for CP to follow. Staff would recommend to make this change as agreed by the EPDP Team in LA and not delete this section. The sentence would read: the Central Gateway Manager* ~~*MUST*~~ ***MAY*** *provide a recommendation to the* |

| | | | |
|---|---|---|---|
| | | | *Contracted Party whether to disclose or not.* |
| 14. | 1069-1070, 1092-1112<br><br>Flagged by: ICANN Org Liaisons<br><br>Requested to be discussed by: IPC | The language in 1069-1070 could result in disagreements in implementation over whether the response times are mandatory or "best effort targets?"<br><br>In addition, the SLAs as outlined in 1092-1112 seem contradictory and may be difficult to implement as written. For example, is the recommendation to measure response times based on mean response times, or compliance target percentages as indicated in the table? In addition, Phase 3 (18 months of compliance) for Priority 3 seems to be missing from the bullets in lines 1097-1098. Who and how should SLAs be measured? Are these measurements self-reported or measured based on responses to requests via the Central Gateway? Would the team consider leaving some of these details to implementation? | |
| 15. | Rec #8 – Response Requirements<br><br>Line 1010<br><br>Flagged by: BC/IPC<br><br>Requested to be discussed by: | The requirement to respond to denied requests with a rational should not be optional. | Update line 1009-1010 as follows<br><br>"e) Responses where disclosure of data (in whole or in part) has been denied ~~should~~ **MUST** include: rationale sufficient…" |

| | | | |
|---|---|---|---|
| 16. | p. 29, l. 1044<br><br>Flagged by: GAC<br><br>Requested to be discussed by: | GAC Montreal Communiquè advised ICANN compliance to create a separate complaint form and track these issues under a separate process, so arguably, these issues w/n fall within ICANN's "standard" process<br><br>Delete "standard" | If a requestor is of the view that its request was denied erroneously, a complaint should be filed with ICANN Compliance. ICANN Compliance should be prepared to investigate complaints regarding disclosure requests under its ~~standard~~ enforcement processes. |
| 17. | 1091<br><br>Flagged by: Volker and Mark SV | Need to add a clarification that the matrix is expected to be further reviewed in response to public comment. | **For the avoidance of doubt, the below matrix and accompanying text represent a starting proposal to gather community feedback. Accordingly, the proposed times are subject to change based on comments received.** |
| 18. | p. 31, l. 1113<br><br>Flagged by: GAC<br><br>Requested to be discussed by: | We discussed that review of the SLA targets should take place more frequently than once a year.<br><br>Replace "annually" with "quarterly" | Response Targets and Compliance Targets shall be reviewed, at a minimum, **quarterly** ~~annually~~. A review mechanism will be further developed by the EPDP Team, but community input in response to the public comment period will be helpful. |
| 19. | 1391-1395<br>See issue #1. Language is similar but this statement includes "financially (or commercially) reasonable" which is not mentioned earlier.<br><br>Flagged by: NCSG | See Issue #1. We favor substituting our language from Issue #1 for the lines 1391-1395. The following text actually differentiates between request automation and disclosure automation and can be retained. | ~~The EPDP Team acknowledges that full automation of the SSAD may not be possible, but recommends that the SSAD must be automated where technically feasible, legally permissible and financially (or commercially) reasonable. Additionally, in areas where automation is not both technically feasible and legally permissible, the EPDP Team~~ |

| | | | |
|---|---|---|---|
| | Requested to be discussed by: IPC | | ~~recommends standardization as the baseline objective.~~<br><br>**The EPDP Team recommends that the receipt, authentication and transmission of SSAD requests be fully automated insofar as it is technically feasible. The EPDP team recommends that disclosure decisions should be automated where technically and commercially feasible, legally permissible and there is a compelling security, stability or resiliency rationale for doing so. In areas where automation does not meet these criteria, standardization of disclosure decisions is the baseline objective."** |
| 20. | Rec #17 – Logging<br><br>Line 1438<br><br>Flagged by: BC/IPC<br><br>Requested to be discussed by | In order to ensure transparency, an additional logging requirement is necessary to support the analysis and measurement of data associated with disclosure responses. This will aid and support the continuous evolution of the SSAD over time. | Add the following bullet to the list of EPDP recommendations :<br><br>**f) Periodic reports of log data should be published in aggregate and without PII to enable an assessment of disclosure request responses on a per contract party basis.**<br><br>[We note this may be better suited as an addition in the Auditing section – specifically the "Audits of the Central |

| | | | |
|---|---|---|---|
| | | | Gateway Manager & Contracted Parties" Section] |

**MINOR EDITS / NON CANNOT LIVE WITH ITEMS PUT FORWARD**

Proposed changes, but not rising to the level of "cannot live with" (GAC):

| | | | |
|---|---|---|---|
| 1. | p. 22, l. 771<br><br>Flagged by: GAC<br><br>Requested to be discussed by: | Use of "will" makes it sound like we're mandating delays. Possible that non-SSAD requests may be quick in certain cases<br><br>Change "will" to "may" or "will likely" | De-accreditation does not prevent the requestor from submitting future requests under the access method provisioned in Recommendation 18 of the EPDP Phase 1 Report, but that they will not be accredited, and thus ~~will~~ **may** be subject to delays, and manual processing. |
| 2. | p. 23, l. 810-12<br><br>Flagged by: GAC<br><br>Requested to be discussed by: | The concept of automated responses which had been discussed seems to have dropped out of this draft<br><br>Add as last sentence, l. 812 a reference to the preference for immediate automated acknowledgment of receipt responses. | The EPDP Team recommends that the response time for acknowledging receipt of a SSAD request by the Central Gateway Manager must be without undue delay, but not more than two (2) hours from receipt.<br><br>***Staff Support Team note****: This was intended to be covered by the 'undue delay' reference. The EPDP Team agreed in LA not to bring this down to an SLA of seconds but instead focus on the maximum delay with the understanding that this normally would be instantaneous.* |

| | | | |
|---|---|---|---|
| 3. | p. 37, l. 1354-55<br><br>Flagged by: GAC<br><br>Requested to be discussed by: | Practically speaking, need to make sure that language forbidding "profit" isn't read to prevent subcontractors for SSAD from making modest profit for their work. Not convinced "market cost" meets this concern.<br><br>Replace reference to "market cost" with proper economic term for reasonable profit margin. | The SSAD should not be considered a profit-generating platform for ICANN or the contracted parties. Funding for the SSAD should be sufficient to cover costs, including for subcontractors at ~~market cost~~ **fair market value** and to establish a legal risk fund. It is crucial to ensure that any payments in the SSAD are related to operational costs and are not simply an exchange of money for non-public registration data. |
| 4. | p. 41, l. 1546<br><br>Flagged by: GAC<br><br>Requested to be discussed by: | The audit mechanism, something that is burdensome, should be triggered by verified complaints<br><br>Insert "verified" before "complaints" | Appropriate mechanisms must be developed in the implementation phase to ensure accredited entities' and individuals' compliance with the policy requirements as defined in the accreditation preliminary recommendation. These could include, for example, audits triggered by **verified** complaints, random audits, or audits in response to a self-certification or self-assessment. |

Misc. typos and word choice issues (GAC)

5. P. 6, l. 135 (awkward phrasing, consider instead "Potential Purpose for the Office of the Chief Technology Officer")
6. P. 9, l. 233 (spell out SLAs, "service level agreements")
7. P. 11, l.305 ("Mechanism" suggests an automated process and I don't think that's what we want to imply; perhaps go back to "steering" or "advisory" committee; see also reference to "feedback mechanism" on p. 9, l. 228)
8. P. 11, l. 306 (change "provide" to "providing"

9. P. 11, 653 (delete apostrophe from consumer rights)
10. P. 20, l. 689 (change " fall short or in violation" to "violate" ("fall short" is vague and colloquial)
11. P. 34, l. 1243-47 (choose whether to include bracketed language about historical data but if included, do so only once)
12. P. 36-37 l. 1343-45 (delete bracketed language because it has been replaced with last sentence of ¶ ("The EPDP also recognizes. . .")
13. P. 43 l. 1606-09 (isn't this repetitive? See l. 1236)

Not die in a ditch items but a few points that have been raised (ISPCP):

14. Line 363

    If you look at the note starting at line 196, we are making our recommendations meet the requirements of the GDPR as it is impossible to make it compliant with all applicable data protection laws.

    Line 363 needs to be amended and the words "and other applicable data protection legislations for all parties" should be deleted.

    "The SSAD must be compliant with the GDPR ~~and other applicable data protection legislations for all parties~~".

15. Line 802

    "Registered name holder consent or contract" should be changed to:
    Registered name holder consent, contract or responses to registered name holders' rights exercising their right of access.

    "Third parties may submit data disclosure requests for specific purposes such as but not limited to: (i) criminal law enforcement, national or public security, (ii) non law enforcement investigations and civil claims, including, intellectual property infringement and UDRP and URS claims, (iii) consumer protection, abuse prevention, digital service provider (DSP) and network security, or (iv) Registered name holder consent**,** ~~or~~ contract **or responses to registered name holders' rights exercising their right of access**.

16. Line 912

    Did we have a section anywhere in the report that decisions must be shared with the central gateway? Also, did we put anything into the report on how to manage objections and make sure all parties concerned get a chance to factor successful objections into their decision-making?

"If, based on consideration of the above factors, the Contracted Party determines that the requestor's legitimate interest is not outweighed by the interests or fundamental rights and freedoms of the data subject, the data shall be disclosed. The rationale for the approval MUST be documented.

Staff Support Team spotted items:

17. Footnote 7: make further clear that the diagram does not represent technical requirements

[1] For a standalone version, please see https://community.icann.org/download/attachments/124847621/Visio-epdp-p2_swimlane_v0.5.pdf?version=1&modificationDate=1580312983428&api=v2. Please note that this is a visual representation of the policy recommendations, not policy in itself. **As this is a policy requirements diagram, it does NOT represent technical requirements.** For the sake of readability, not all aspects may be represented in this graphic. In case of conflict, the policy recommendations are the authoritative source.

18. Line 299 – 300 – 2) was inadvertently deleted

- Identity Provider - Responsible for 1) Verifying the identity of a requestor and managing an Identifier Credential associated with the requestor**, 2) Verifying and managing Signed Assertions associated with the Identifier Credential.** For the purpose of the SSAD, the Identity Provider may be the Accreditation Authority itself or it may rely on zero or more 3rd parties.

19. Preliminary recommendation #6 – lines 825- 924 – incorrect references to other paragraphs and style/readability edits.

3. While the requestor will have the ability to identify the lawful basis under which it expects the Contracted Party to disclose the data requested, the Contracted Party must make the final determination of the appropriate lawful basis **it relies on to** disclose the requested information.
(…)

If the answer to any of the above questions is no, the Contracted Party may deny the request, or require further information from the requestor before proceeding to ~~paragraph 6~~ **bullet #5** below.

5. The Contracted Party may evaluate the underlying data requested once the validity of the request is determined under ~~paragraph~~ **bullet point #** 4 above. ~~The purpose of paragraph 5 is to determine whether the paragraph 6 meaningful human review is required.~~ The Contracted Party's review of the underlying data should assess at least:

- Does the data requested contain personal data?

- If no personal data **is requested**, no further **meaningful human review** ~~balancing~~ is required, and the non-personal data MUST be disclosed.

- The applicable lawful basis and whether **meaningful human review** ~~the requested data contains personal data the authorization provider to determine if the balancing test~~, similar to the requirements under GDPR's 6.1.f **balancing test and** as described in **the** paragraph below, is applicable and proceed accordingly.
- The Contracted Party should evaluate at least the following factors to determine whether the legitimate interest of the requestor is not outweighed by the interests or fundamental rights and freedoms of the data subject. No single factor is determinative; instead, ~~the authorization provider~~ **the Contracted Party** should consider the totality of the circumstances outlined below:
  - Assessment of impact. Consider the direct impact on data subjects as well as any broader possible consequences of the data processing. Whenever the circumstances of the disclosure request or the nature of the data to be disclosed suggest an increased risk for the data subject affected, **the Contracted Party** ~~this~~ shall ~~be~~ taken ~~n~~ **this** into account during the decision-making.
  - *Nature of the data*. Consider the level of sensitivity of the data as well as whether the data is already publicly available.
  - *Status of the data subject*. Consider whether the data subject's status increases their vulnerability (e.g., children, other protected classes).
  - *Scope of processing*. Consider information from the disclosure request or other relevant circumstances that indicates whether data will be securely held (lower risk) versus publicly disclosed, made accessible to a large number of persons, or combined with other data (higher risk), provided that this is not intended to prohibit public disclosures for legal actions or administrative dispute resolution proceedings such as the UDRP or URS.
  - *Reasonable expectations of the data subject*. Consider whether the data subject would reasonably expect their data to be processed/disclosed in this manner.
  - *Status of the controller and data subject*. Consider negotiating power and any imbalances in authority between the controller and the data subject.
  - *Legal frameworks involved*. Consider the jurisdictional legal frameworks of the requestor, Contracted Party/Parties, and the data subject, and how this may affect potential disclosures.

**(…)**

6. The application of **meaningful human review** ~~the balancing test~~ and factors ~~considered~~ **outlined** in **bullet point #**5 **above** should be revised as appropriate to address applicable case law interpreting GDPR, guidelines issued by the EDPB or revisions to GDPR that may occur in the future.

20. Consistency in capitalization of MUST, MAY, etc. – throughout the document

**ICANN Org Liaisons**

| Issue | Line number(s) | Can't Live With Rationale | Proposed changes |
|---|---|---|---|
| 21. | General comment | Harmonize SHOULD/MUST/MAY/SHALL language. Not all capitalized. | |
| 22. | 396 | This definition is confusing. Can the team clarify as the placing of the comma, "or" and "if" leads to multiple possible permutations and interpretations, which may also conflict with the reference to Accreditation Authority Audits in Rec #18. | The entity responsible for carrying out the auditing requirements of the Accreditation Authority, as outlined in Preliminary Recommendation 18. The entity could be an independent body or, if ICANN org ultimately outsources the role of Accreditation Authority to a third party, ICANN org MAY be the Accreditation Authority Auditor. |
| 23. | 448 | Consistent with line 396-399, ICANN org may contract with a third party to run the Accreditation Authority. | Delete "run and" |
| 24. | 456 | Presumably ICANN is included as the authorizer here for automated decisions. However, shouldn't this be the Central Gateway Manager? This would | Change "ICANN" to "Central Gateway Manager." |

| | | | |
|---|---|---|---|
| | | be relevant if ICANN was to outsource this work to a third party and to ensure consistency with the roles as outlined in the model description. | |
| 25. | 469 | Why would the Identity Credential be affiliated with the Accreditation Authority? It seems like it ought to recognize that the requestor is affiliated with its relevant organization? | Change" Accreditation Authority" to "relevant organization." |
| 26. | 490 | Why is the "code of conduct" limited to the ICANN community? Should it be for the participants in SSAD? | Delete "for the ICANN community." |
| 27. | 501 | Please explain "etc?" Could this be deleted? | Delete "etc" |
| 28. | 827-830 | This is likely a drafting error- would require substantive review of automated requests. | Suggested edit: 'The Contracted Party to which the non-automated disclosure request has been routed MUST review every request on its merits…" |
| 29. | 842 | Shouldn't the Identity Provider confirm the identity of the requestor? The CP would not have a relationship with the Accreditation Authority or the Identity Provider to confirm this information. | Suggest deleting this bullet. |
| 30. | 849-851 | These lines appear to be redundant with the element above. | Delete 849-851. |

| | | | |
|---|---|---|---|
| 31. | 852 | This sub-bullet does not appear to be a sub element of the bullet that precedes it. | Make this bullet a new bullet instead of a sub-bullet. |
| 32. | 861 | Shouldn't this reference Paragraph 5, not 6? | Change "Paragraph 6" to "Paragraph 5" |
| 33. | 880-924 | Paragraph 5 refers to the test in Paragraph 6, but the meaningful review seems to be detailed in Paragraph 5, bullet 3 and the subsequent bullets under it (which should be renumbered as paragraph 6). Paragraph 6 would then become paragraph 7. | Change Paragraph 5, bullet 3, and the remaining bullets to "Paragraph 6." Change "Paragraph 6" to "Paragraph 7." |
| 34. | 913 | Should "**shall"** here be a SHALL? | Change "**shall"** to "SHALL" |
| 35. | 992 | Should "MUST" here be "MAY?" We recall discussing this during the F2F and understanding that this would be a "MAY" for the Central Gateway. | Change to "MUST" to "MAY" |
| 36. | 1087-1088 | "The Contracted Party shall provide the requested information…" implied that they must disclose regardless of the priority set. The sentence seems to be missing a clause that indicates the CP determines whether to disclose, and only then provides the requested information or a reason why it cannot disclose under the | Change to: Following receipt of a non-automated disclosure request from the Central Gateway Manager, the Contracted Party is responsible for determining whether to disclose the nonpublic data. Within the below-defined response times, the Contracted Party SHALL respond to the request. If the Contracted Party determines it is unable to disclose the nonpublic data, it SHALL provide a rationale to the requestor and the Central Gateway Manager. |

| | | | |
|---|---|---|---|
| | | below-defined response targets and compliance targets. Separately, the "or" clause seems to indicate that it may disregard the targeted response times? | |
| 37. 305. | 1368-1371 | There are no longer "various models" under consideration. In addition, the line about "various implementation details that may have policy implications," doesn't really provide implementation guidance. | Suggest deleting these lines. |
| 38. 47 | 1393 (in reference to footnote 17) | Suggest editing footnote to add "...will be addressed by ICANN org with the Implementation Review Team." | Change footnote 17 to:Initial consideration of the financial feasibility of automation will be addressed by the ICANN org with the Implementation Review Team and subsequently by the mechanism for the continuous evolution of SSAD, as applicable. |
| 39. | 1432-1436 | Contracted Parties as the entity disclosing the data are missing from this list. Should they be included? | Add "Contracted Parties" |
| 40. | 1476 | Change "entity Authorizing the request" to Contracted Parties to reflect the agreed-upon model. | Change "entity Authorizing the request" to Contracted Parties |
| 41. | 1503 | Please note in this text that ICANN as the Accreditation Authority is not required to audit governmental entities, whose audit requirements are | ICANN as the Accreditation Authority is not required to audit governmental entities, whose accreditation and audit requirements are defined in Preliminary Recommendation #2. |

| | | | |
|---|---|---|---|
| | | defined in lines 722-725 (under Rec #2). | |
| 42. | 1519-1542 | These paragraphs seem to be redundant. | Suggest deleting the first paragraph (1514-1517). |
| 43. | 1562 | This isn't a policy recommendation but a note for further work. Suggest clarifying. | Consider deleting, as audits for the SSAD parties have already been contemplated in Rec #18. |
| 44. | 1601-1609 | This seems to be misplaced as it does not belong under Rec #19. Further, it seems to be captured in lines 1236-1237 under Rec #12 Query Policy. | Suggest deleting. |

From IPC/BC:

Section 1.1

45. o Line 20: Would it make sense to summarize how the phase 1 policy ended up - specifically the answer to the question of if it the temp spec should be made consensus policy or be updated. (I'm not sure there is a short way to do this however)
    · Section 2.5
46. o lines 176-180: Do we want to state up front that this draft of the report does not specifically answer the charter questions but the final report will?
    · Section 3.1
47. o line 223: Why did we substitute the word harmonization for standardization. I don't really know what harmonization means in this context (it means nothing really - harmonize with what?). I would suggest we use the word standardization instead. (This may have been decided by the group so keep or toss)
48. o line 233: I'd like to see us be more specific here and state that these SLAs are not only "put in place" but are also enforceable by ICANN compliance.
49. o line 267: Delete the "4."
50. o line 278-282: We should describe this diagram as a responsibility flow diagram and make it clear it is not a protocol/dataflow diagram. We don't want the implementers to believe their data flows must adhere to what the diagram describes.

51. o line 292-293: Update to ensure its clear that the Central Gateway is collecting more than just data on "disclosure decisions taken". Maybe something like "requests, responses and disclosure decisions taken."
    - Section 3.2
52. o lines 326-332: This section could be confusing to the reader (it was to me) because the model we describe in this report is different from the model that ICANN proposed in its Nov 19 Letter.
    - Section 3.4
53. o lines 372-375: If our report will be using RFC 2119 and RFC 8174 language its clear to me we need to scrub through the whole document to ensure we are doing this consistently and with purpose. Currently only some obligations use this convention but most do not. As it makes a huge difference regarding implementation and compliance some time should be focused on this. (FWIW I'm not sure how we do this as a group however.....)
    - **Rec #1 - Accreditation**
54. o lines 377-381: One line 368 we specify that ICANN and CPs re joint controllers. So perhaps we can delete this paragraph? Or at a minimum delete the clause that references controllership?
55. o line 404: As we moved the use of Authorization Credential I would remove the "Credential" heading and define both Identifier Credential and Signed Assertion separately.
56. o line 409 and 413: Remove the square brackets as these are just examples.
57. o line 422: Do we want to list a couple of examples of who may be 3rd party Identity Providers? e.g: WIPO, APWG, M3AAG(????), Gov't LEAs, etc.
58. o line 446: "....using the credentials of an accredited entity (e.g. legal person) warrants..."
59. o line 458: Suggest calling this section "Requirements of the Accreditation Authority"
60. o Line 488: It may be helpful to the reader that the baseline code of conduct we are describing in section i) is defend in GDPR and also in https://edpb.europa.eu/sites/edpb/files/consultation/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf. (maybe put this in a footnote)
61. o line 506: "Definition of eligibility..."
62. o line 602: "Proper vetting, ***as described in j) above,*** must...."
    - **Rec #2 - Accreditation of governmental entities**
63. o General Comment: If possible we could eliminate the overlapping language that already exists in Rec #1.
64. o line 694: Replace "approved accreditation authority" with "approved Identify Provider".
65. o line 714: replace "authentication authority" with "Identity Provider"
66. o line 755: we need to ensure that a flag to indicate the need for confidentiality is included in the "Request Requirements" recommendation. (Rec #3)

- **Rec #3 - Criteria and Content of Requests**

67. o line 778-788: Need to add a field to convey "urgency" and the GAC requirement that requests are kept private from the registrant to this section.
68. o line 791-792: Move this sentence to the front of Rec #3

- **Rec #6 Contracted Party Authorization**

69. o line 845-851: It is not at all clear how these obligations can be standardized (i.e. how can we adhere to our first principle) More language and specificity is needed here.
70. o line 854: Didn't we already specify that a single SSAD request can only contain a single Domain Name? If this is the case we should delete the sentence beginning with "If the submission..."
71. o line 876-879: I read this paragraph several times and it seems the wording has been mangled or perhaps its just too confusing for me. Given its not clear what the point of this paragraph is, its not possible to suggest a fix.
72. o line 879: I think there is a numbering issue here. Doesn't paragraph 5 describe how the balancing test should happen? It doesn't seem like Paragraph 6 does in any case.
73. o line 921: again paragraph 6 should reference paragraph 5 (I think).

- **Rec #8 - Response Requirements**

74. o line 1017-1032 I note that there is no normative language used in this paragraph and thus as currently written there exists no obligation to handle Urgent requests.
75. o line 1037-1040: This is a duplication of e) starting at line 1009. Perhaps it can be removed?

- **Rec #10 - AUP**

76. o line 1142-1153: How are these obligations different from the requirements in Rec #3 - they are (or should be) the same. Is the idea that this section will result in an AUP being authorized that outlines what is required of requestors?

- **Rec #11- Disclosure Requirements**

77. o line 1165-1196: How are these obligations different from the requirements in Rec #6 - they are (or should be) the same.

- **Rec #12 - Query Policy**

78. o line 1224: there doesn't seem to be any point b to further.
79. o line 1230-1232: This is duplicative and stated elsewhere in the report.
80. o line 1236: I thought we explicitly disallowed the inclusion of multiple domain names in a single SSAD request. We clearly want to allow UI/UX that can allows requestors to include multiple FQDNs but that will result in separate requests sent to the SSAD.
81. o line 1243: This requirement is duplicative of a requirement stated elsewhere in the report.
82. o line 1249: Remove - i'm not sure why we need to reference the AUP.

- **Rec #13 - Terms of Use**

83. o line 1257-1257: To which parties does the ToU described here apply? I assume this ToU is between the Requestor and the SSAD. If this is the case we should explicitly state it.
84. o line 1280: Terms of use between who?
85. o line 1320: Disclosure agreements between who?
    - **Rec #15 - Financial sustainability**
86. o line 1368: This report describes a single model - so we can delete this sentence I think.
    - **Rec #16 - Automation**
87. o General: I think it would be very helpful for the reader if this section was moved way up in the doc. I suggest it should be inserted after Rec #1
88. o line 1422: Suggested rewording ".....which are currently described in Recommendation #7 but still under discussion". (given the list traffic this may be more than a nit)