ICANN Business Constituency (BC) TEMPLATED COMMENT ON EPDP PHASE 2 INITIAL REPORT
23-Mar-2020
These comments were drafted by Mason Cole and Andrew Bennett.
They were approved in accord with the BC Charter.

Recommendation #1: Accreditation

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

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

Support Purpose as written

X **Support Purpose intent with wording change**

Significant change required: changing intent and wording

Purpose should be deleted

No opinion

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

- No assurance of Whois data accuracy is enumerated, and this threatens to disrupt the integrity of Whois at the outset. Though neither GDPR nor any other law protects fake data, this report shirks the responsibility of ensuring accuracy as part of an accountable and effective Whois framework.
- Based on the Implementation Guidance that concludes Recommendation #1, the EPDP clearly recognizes the importance of accuracy and accountability for accreditation applicants that will be required to present "a business registration number and the name of the authority that issued this number," along with "information asserting trademark ownership". A significant proportion of Whois data is inaccurate and the absence of an accuracy and accountability framework for that data set contradicts the principles the EPDP seeks to establish for the SSAD accreditation policy as well as the principles of GDPR itself: as the GAC and ALAC stated in their joint Statement on the EPDP: "In accordance with Article 5 of the GDPR, every reasonable step must be taken to ensure the accuracy of the data in view of the purposes for which it is processed."
- While specific suggestions are outlined below, the BC adds here that the EPDP team's recommendations can be improved by including the concept of an Accredited Entity who is also a Trusted Notifier. Accredited Entities who are also Trusted Notifiers would be subject matter experts that have been additionally vetted to monitor and investigate issues of illegal activity and abuse. Trusted Notifiers would 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.
- Principle d): The BC prefers that disclosure decisions be automated/centralized to the greatest extent possible and limit to the greatest extent possible the number of individualized disclosure decisions being made by individual registry operators and registrars. Further, the BC supports that references to "registrar," "registry," and "central gateway manager" be changed to "Controller," as that is what GDPR

requires. Limiting to "Controller" would allow the recommendation to scale according to the ultimate decision on who the "Controller" is in this scenario.

- Principle h): The report should define which types of requests could be responded to in an automated manner. For purposes of disclosure, the BC supports automated or quasi-automated (i.e. human review by the central managing authority for provision of required information) access/disclosure decisions in cases of well-founded allegations of abuse (e.g., cybersquatting, phishing, trademark or copyright infringement, etc.), as evidenced in the assertions and supporting materials produced in connection with same/with the disclosure request itself.

- Principle i): Does the referred-to code of conduct comply with Art. 40 of the GDPR and will it contain mechanisms which enable the body referred to in Art. 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it? Further, how is the Accreditation Authority the "authority" on the proper application of data protection laws? The report should clarify.

- Principle j): The BC poses the following:

    - Regarding the definition of eligibility requirements for accredited users, will this be reviewed and revised over time with learnings from the accreditation process? Preliminary eligibility requirements may be unnecessarily exclusive.

    - Regarding identity credential revocation procedures, there must be an appeal or escalation process enumerated.

    - Regarding "requirements beyond the baseline listed [above] may be necessary for certain classes of requestors," these should be available to applicants prior to application.

- Principle k): This language should be sharpened to be more specific, if in fact it refers to an appeal or escalation process. Such a mechanism must include due process checks and balances.

- Principle l): In addition to accredited authorities being audited for compliance, so should the accreditation provider to ensure compliance with timely and reasonable accreditation grants. The report also should detail how often the audits should occur.

- Principle n): The cadence of reports "on a regular basis" should be enumerated.

- Principle o): "Abuse of the system" should be defined and differentiated (if applicable) from violation of the code of conduct.

- Principle p): Regarding "abuse of the system," the report should also identify who supervises the accreditation authority in the instance of "abuse" on its part (e.g., over-restrictive granting of credentials or arbitrary revocation of credentials).

- Principle q): While the BC appreciates the notion of graduated penalties, again here, there should be included an appeal or escalation process in the event of a dispute over penalties or potential revocation.

- Principle r): Will graduated sanctions be enumerated in advance? Will graduated sanctions be uniform across all accreditation authorities? There may be entities seeking accreditation from multiple providers.

- Principle t): Again here, an appeal mechanism should be included.

- Principle u): The BC poses the following:

    - Regarding "prevent abuse of data received," the term "abuse" should be defined.

- Regarding "de-accreditation if they are found to abuse use of data," due process and checks and balances should be required.

- Principle v): Regarding a "demonstrable threat to the SSAD," the BC advises there needs to be a definition and metric so that decisions are objective and not subjective.

- Regarding fees, the BC recommends updating the language of that recommendation to read: The accreditation service will be a *not-for-profit* service that is financially sustainable.

- Regarding implementation guidance, the BC offers the following:

  - a): "Recognized, applicable and well-established organizations" needs definition as it applies to supporting the Accreditation Authority. Also, the recommendation does not identify who would provide "vetting" as it applies to Recommendation j [above].

  - b): "Information asserting trademark ownership" could be clarified – does this refer to information demonstrating ownership of a trademark by the accredited party or that the accredited party is acting on behalf of a trademark owner (or both)? What kinds of information would this entail? A copy of TM registration / certificate? Power of Attorney or other form demonstrating agency?

  - d): When the team recommends that "logged data SHALL only be disclosed, or otherwise made available for review," by whom is the review conducted? Is this part of a formal process? This needs clarification.

Recommendation #2: Accreditation of governmental entities

https://docs.google.com/document/d/1NOTbh3PeQSaDr3O4GKjGjJPHgpB3bVIMTyJvz7pzpsU/edit.

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

Support Recommendation as written

X **Support Recommendation intent with wording change**

Significant change required: changing intent and wording

Recommendation should be deleted

No opinion

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

- a): In the definitions section, "public policy task" needs a definition.

- b): Wording change: The BC recommends changing "SHOULD" to "MUST."

- b) continued: Regarding the section describing an accreditation procedure, does the EPDP team envision this as any different than the accreditation procedure outlined earlier in the report? Or would this section envision a separate channel for access for government entities (including LEA)? Clarification is needed.

- c): Regarding accreditation by countries' or territories' government body or its authorized body, does this refer only to national governments? The BC may predict that localized jurisdictional authorities may seek accreditation; exclusive vesting such authority to national bodies may prove bureaucratic and unnecessarily slow for sub-national and other government entities to obtain accreditation. This needs to be carefully considered and clarified.

- c) continued: Are cybersecurity authorities "public" or government-sanctioned only? Or would this include private cybersecurity teams?

- d): Regarding "country/territory nominated Accreditation Authority," this too is undefined. Does it refer to nomination by a country/territory body? Would that exempt a city's police department, for example, or would that department have to queue with others applying to the country/territory government to determine eligibility?

- e): Referring to the recommendation that an "accreditation process SHOULD take account of a number of requirements," are these requirements subject to review or expansion by the community? Does the authority make those decisions independently? This needs clarification and higher prioritization as well.

- e) continued: Regarding the recommendation that "The requirements SHALL be listed and made available to eligible government entities," the BC asks whether they should be made generally available, without pre-determining which entities might be eligible?

- e) continued: In the bulleted recommendations, the BC advocates for the following wording changes/additions:

    - Be subject to *graduated penalties and*, ultimately, de-accreditation if they are found to violate any of these requirements.

    - *Provide due process mechanisms in review, de-accreditation and graduated penalties processes.*

- f): Regarding the Accreditation Procedure, will the authorities, or the accreditation scheme, be reviewed by the community from time to time, in case of the need for revisions sourced from the community? The BC recommends this.

- f) continued: In the same paragraph describing the Accreditation Procedure, the BC recommends changing SHOULD to MUST.

- f) continued: At the end of the list of bullets, the EPDP team recommends that "The accreditation authority reserves the right to update what credentials or other material are required for accreditation." The BC asks that this recommendation include a provision that proper advance notice is required for changes to requirements and terms.

- a): Regarding the recommendation that "Each accreditation authority SHOULD determine an appropriate time limit," the BC advocates for uniformity of time limits among accreditation providers, in order to lessen user confusion.

- c): The EPDP team's recommendation reads: "Audits SHOULD be conducted by either the data protection authority or by the country/territory designated auditor." The BC poses the following:

    - How is a data protection authority vested to perform this kind of audit? Wouldn't they be performing their own independent reviews of this system pursuant to their obligations to enforce applicable privacy law?

- This system would need a mechanism to maintain independence from the accreditation authority so as not to be subject to undue influence.

- d): The BC recommends a complaint procedure that not only deals with unauthorized access to or improper use of data, but also a procedure that addresses complaints about the accreditation authority itself.

- e): With regard to the following EPDP team recommendations:

  - "Accreditation is required for a party to participate in the access system (SSAD). Unaccredited parties can make data requests outside the system, and contracted parties should have procedures in place to provide reasonable access." The BC suggests this be required to be equivalent to the Temp Spec's reasonable access requirements and appropriate service level agreements.

  - "Accredited entities will be required to follow the safeguards as set by the disclosing system." The BC suggests that this requirement track applicable law and not safeguards provided by the disclosing system.

  - "Disclosure of RDDS data to the type of third parties MUST be made clear to the data subject. Upon a request from a data subject inquiring about the exact processing activities of their data within the SSAD, relevant information SHOULD be disclosed as soon as reasonably feasible. However, the nature of legal investigations or procedures MAY require SSAD and/or the disclosing entity keep the nature or existence of these requests confidential from the data subject. Confidential requests can be disclosed to data subjects in cooperation with the requesting authority, and in accordance with the data subject's rights under applicable law." Will there exist mechanisms to rectify improper disclosure by the accrediting entity or controller of the existence or nature of a confidential disclosure request?

- f): The BC observes the lack of appeal or due process recommendations in this section, and advocates for their inclusion. Further, in the bullet list, "special circumstances" needs definition.

Recommendation #3: Criteria and Content of Requests

https://docs.google.com/document/d/1_w7EJHo4RzPtRiszKgyJ4GzmY3KvGjk_-o03n7Yuzk/edit.

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

Support Recommendation as written

X **Support Recommendation intent with wording change**

Significant change required: changing intent and wording

Recommendation should be deleted

No Opinion

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

Regarding f (request type), the BC observes that this self-designation of priority could be misused. Perhaps the centralized system can automatically designate priority levels based on the nature of the request (e.g. LEA criminal

investigations are flagged as priority, cybersecurity as next highest priority, IP/consumer protection as next highest priority, etc.).

Recommendation #4: Third Party Purposes/Justifications

https://docs.google.com/document/d/1Xrx96CiQMhMffdmCQWtomZ_ATISzgqRBSm72z0bzTA/edit?usp=sharing.

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

Support Recommendation as written

X **Support Recommendation intent with wording change**

Significant change required: changing intent and wording

Recommendation should be deleted

No Opinion

14. If your response requires an edit of Recommendation #4, indicate revised wording and rationale here.

- At the end of the first bullet ("Registered name holder consent, contract or responses to registered name holders' requests exercising their right of access"), the BC suggests a closer look at GDPR, which may require access under these circumstances.
- Regarding the final bullet ("Assertion of one of these specified purposes does not guarantee access in all cases but will depend on evaluation of the merits of the specific request, compliance with all applicable policy requirements, and the legal basis for the request."), the BC reflects the comment immediately above -- under some of the enumerated purposes, the GDPR requires disclosure (e.g. Right of Access).

Recommendation #5: Acknowledgement of receipt

https://docs.google.com/document/d/140U4AsH3so8tSojhdCEUa8I2QkD8OwBXxK9NcIjiCx4/edit?usp=sharing

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

Support Recommendation as written

X **Support Recommendation intent with wording change**

Significant change required: changing intent and wording

Recommendation should be deleted

No opinion

16. If your response requires an edit of Recommendation #5, please indicate revised wording and rationale.

- Regarding the following recommendation: "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." -- the BC urges the EPDP to agree to a more specific and firm timeframe for acknowledging receipt. We suggest a wording change to specify two to four hours and see no reason why acknowledgement of receipt could not be automated like most technological ticketing systems.

- Another wording change recommendation: Where the report states "Should the Central Gateway Manager determine that the request is incomplete, the Central Gateway Manager MUST reply to the requestor with an incomplete request response, detailing which required data is missing, and provide an opportunity for the requestor to amend its request.", the BC suggests changing the wording to "with a response indicating that the request is incomplete..." Current wording makes it sound like the Central Gateway Manager is sending an incomplete response.

Recommendation #6: Contracted Party Authorization

https://docs.google.com/document/d/1-iiPCpZMdpYmhPLzqbHHbG7NvfKt80-AbjPPj-isHnM/edit?usp=sharing

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

Support Recommendation as written

X **Support Recommendation intent with wording change**

Significant change required: changing intent and wording

Recommendation should be deleted

No opinion

18. If your response requires an edit of Recommendation #6, indicate revised wording and rationale here.

- In the first bullet point of this recommendation, which addresses the fact that automated review is not expressly prohibited where legally and technically permissible, the BC suggests it could be helpful to prioritize elaboration on scenarios where automated review would be possible, and further where automated disclosure may be possible. In addition, this should perhaps read "legally permissible and technically feasible for the Contracted Party".

- Regarding the third bullet, the BC recommends changing "contracted party" to "controller." This change should be made throughout the document as appropriate.

- With regard to the following: "Are the data elements requested necessary to the requestor's stated purpose?", the BC notes this is subjective and not objective review. A statement of necessity, for example, a legal claim, cannot necessarily be assessed by a contracted party. This should be changed to verify that a reasonable statement of necessity has been made.

- The BC notes the following recommendation:

  "The Contracted Party MAY evaluate the underlying data requested once the validity of the request is determined under bullet point #4 above. The Contracted Party's review of the underlying data SHOULD assess at least: Does the data requested contain personal data?"

  The BC urges a language change from "MAY" to "MUST" and recommends rewording "under bullet point #4 above," which is confusing when the document contains multiple bullet points. Further, the EPDP team should add a bullet documenting that if not prevented by applicable law, data MUST be released (GDPR does not prevent disclosure of legal person data).

  Regarding the following recommendations, in order:

- "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 SHOULD consider the totality of the circumstances outlined below:"

  The BC reiterates that "authorization provider" should be changed to "controller," with the change populated throughout.

  - "**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, this shall be taken into account during the decision-making."

    The BC recommends a language change to include the provision that the controller MUST consider the public interest and legitimate interests pursued by the requestor to, for example, maintain the security and stability of the DNS.

  - "**Nature of the data.** Consider the level of sensitivity of the data as well as whether the data is already publicly available."

    This recommendation should include that the controller MUST consider whether the data is covered by applicable law (e.g., legal vs. natural person).

  - "**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."

    The BC is unclear on how combination with other data presents a higher risk. The EPDP team should clarify.

- "**Reasonable expectations of the data subject.** Consider whether the data subject would reasonably expect data to be processed/disclosed in this manner. Whenever the circumstances of the disclosure request or the nature of the data to be disclosed are material to the legal, efficient, and transparent operations of the DNS, a reasonable expectation by the data subject to preserve these objectives should be assumed.

  - "**Status of the controller and data subject.** Consider negotiating power and any imbalances in authority between the controller and the data subject."

    The BC is unsure how this is relevant, when it is known that the disclosing party, under the proposed system, will be a registry operator or registrar. The EPDP team should clarify.

  - "**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."

    The BC submits that if no applicable law would prohibit disclosure, then disclosure should be mandatory.

  - The BC recommends the addition of the following language to the end of this bullet list:

Recognition of human rights impacts. Consider Article 17 of the Universal Declaration of Human rights, that states (1) Everyone has the right to own property alone as well as in association with others. (2) No one shall be arbitrarily deprived of his property. Consider Article 27, concerning the "right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author."

- Finally, the BC reiterates this section of its input regarding Recommendation 1: While specific suggestions are outlined below, the BC adds here that the EPDP team's recommendations can be improved by including the concept of an Accredited Entity who is also a Trusted Notifier. Accredited Entities who are also Trusted Notifiers would be subject matter experts that have been additionally vetted to monitor and investigate issues of illegal activity and abuse. Trusted Notifiers would 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 BC recommends the following wording changes to the end set of recommendation #6:

  - Where the recommendation reads: "If, based on consideration of the above factors, the Contracted Party determines that the requestor's legitimate interest is outweighed by the interests or fundamental rights and freedoms of the data subject, the request may be denied. The rationale for the denial MUST be documented and logged and MUST be communicated to the requestor, with care taken to ensure that no personal data is revealed to the requestor within this explanation."

    The BC believes such a denial must be appealable, with documentation provided to the entity seeking the data regarding procedures for appeal.

  - Where the recommendation reads: "The application of the balancing test and factors considered in bullet point #5 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."

    The BC believes such revisions should be subject to community review.

  - In the section labeled Implementation Guidance, the BC recommends the following wording changes:

    - An interest is [DELETE generally] [INSERT deemed] legitimate so long as it can be pursued consistent with data protection and other laws.

    - Examples of legitimate interests include: (i) [DELETE enforcement] [INSERT establishment, exercise or defense] of legal claims;

Recommendation #7: Authorization for automated disclosure requests

https://docs.google.com/document/d/11BSAUqIUOWJmZOSTaQIW0QZncnywljKJPWUtCTtnCHY/edit.

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

Support Recommendation as written

X **Support Recommendation intent with wording change**

Significant change required: changing intent and wording

Recommendation should be deleted

No opinion

20. If your response requires an edit of Recommendation #7, indicate revised wording and rationale here.

The BC recommends the following wording changes:

> 1. The Central Gateway Manager MUST confirm that all required information as per preliminary recommendation #3 'criteria and content of requests' is provided and that the request meets the criteria established in these policy recommendations (and is confirmed during the implementation phase) to qualify [DELETE as] [INSERT for] an automated disclosure request.
>
> 2. Should the Central Gateway Manager determine that the request is incomplete, the Central Gateway Manager MUST reply to the requestor [DELETE with an incomplete request response] [INSERT indicating that the request is incomplete,] detailing which required data is missing, and provide an opportunity for the requestor to amend its request.

Finally, where the EPDP team recommends: "With respect to disclosure requests that would be sent to a Contracted Party for manual evaluation, a Contracted Party MAY request the Central Gateway to fully automate all, or certain types of, disclosure requests. A Contracted Party MAY retract or revise a request for automation that is not required by these policy recommendations at any time.", the BC:

- agrees with the Belgian DPA's input to ICANN Org (see https://www.icann.org/news/blog/icann-meets-with-belgian-data-protection-authority) regarding its preference for a centralized model as a better, "common sense" model -- the BC supports a centralized system; and

- believes there should be a notice period before retraction or revision would go into effect. Otherwise this could unduly prejudice requestors who are anticipating an automated process.

Under implementation guidance, the BC asserts the following:

As cited, "The EPDP Team expects that the following types of disclosure requests can be fully automated (in-take as well as response) from the start:

- Requests from Law Enforcement in local or otherwise applicable jurisdictions."

Clarification is needed here regarding "local or otherwise applicable jurisdictions." Is this local to the registry, registrar, CGM, ICANN, registrant? All of the above?

The BC advocates for the following to be added to this bulleted list:

- Requests for disclosure of data not prohibited for release by applicable law.

Finally, where the EPDP says: "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 Mechanism for

the evolution of SSAD is expected to provide further guidance on which types of disclosure requests can be fully automated.", the BC asserts the following:

- It would be helpful to also automate responses to trademark or copyright owners or their agents who demonstrate ownership of IP rights (and agency, if needed) and provide evidence supporting a reasonable need to investigate a domain for cybersquatting, trademark or copyright infringement, phishing, or related activity involving potentially unauthorized use of the requestor's (or their client's) property.
- "Over time" should be defined more precisely. Perhaps a one-year timeframe is appropriate.

Section 3, EPDP Phase 2 Recommendations #8-9

Recommendation #8: Response Requirements

https://docs.google.com/document/d/1U6iEnJzxls_824MsBzgW1tk7Qa2W6eY72B3QkdMu2Uk/edit?usp=sharing.

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

Support recommendation as written

X **Support intent of recommendation with edits**

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

23. Do you recommend a change to wording of Recommendation 8? Indicate proposed edits and rationale here.

The BC offers the following input regarding the following recommendations:

For the Central Gateway Manager:

a): …the Central Gateway Manager MUST provide, [INSERT within 24 hours,] an opportunity for the requestor to amend and resubmit its request.

b): Regarding "the responsible Contracted Party," the EPDP team should clarify how this is determined. Is it sent to the registrar or registry? Both? At the option of the requestor?

c): Regarding "the Central Gateway Manager MAY provide a recommendation to the Contracted Party whether to disclose or not. The Contracted Party MAY follow this recommendation.", the BC respectfully inquires about how and when would this be determined and on what basis? Inconsistent CMG replies could be viewed as prejudicing/advantaging certain parties which could be problematic for the system as a whole. Further, this appears to be the insertion of another balancing test, which the BC does not favor. At the very least, this additional layer of "recommendation" requires enhanced transparency: if the CGM's recommendation to the CP is to *not disclose*, then this recommendation, along with a rationale, must be shared with the requestor.

For Contracted Parties:

a): The BC recommends the following wording change: MUST provide a disclosure response [DELETE without undue delay] within 72 hours.

b): Where the recommendation reads: "Additionally, in its response, the entity receiving the access/disclosure request MUST include information on how public registration data can be obtained.", the BC finds that responses should also describe how to appeal a determination or re-submit a request in order to address reasons for denial, and describe whether/how applicable law prohibits the disclosure of data.

f) With regard to urgent SSAD requests: Where the recommendation details "the criteria to determine...an urgent request", the potential economic harm and risk to livelihoods that result from phishing attacks, credit card fraud, and other crimes that threaten financial devastation and lead to SSAD requests should be accounted for. Additional criteria like "devastating financial harm" should be considered.

e): Where the recommendation reads: "Contracted Parties MUST maintain a dedicated contact for dealing with Urgent SSAD Requests which can be stored and used by the Central Gateway Manager, in circumstances where an SSAD request has been flagged as Urgent. Additionally, the EPDP Team recommends that Contracted Parties MUST publish their standard business hours and accompanying time zone in the SSAD portal (or in another standardized place that may be designated by ICANN from time to time.", the BC points out that there are provisions in the RAA about 24/7 availability of abuse mitigation contacts and proper resourcing. Why not the same for "urgent" requests if they involve threat to human life or other imminent harm?

Further in the recommendations under #8, the EPDP team writes: "If a requestor is of the view that its request was denied erroneously, a complaint MAY be filed with ICANN Compliance. ICANN Compliance should be prepared to investigate complaints regarding disclosure requests under its enforcement processes." The BC strongly believes that language should be added here giving ICANN Compliance authority under the Registrar Accreditation Agreement to enforce. Further, language needs to be added about resources afforded to Compliance to handle this, and a timeline for investigations. Otherwise, they will languish.

Implementation guidance:
b) The CGM's "incomplete request response" needs to be issued in a timely manner -- the BC suggests within 24 hours.

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

https://docs.google.com/document/d/1QwHyvI1SnFgVi8WGGIheCu0-fG76I_SIUFBe-sph-Ew/edit.

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

Support recommendation as written

X **Support intent of recommendation with edits**

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

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

- Where the EPDP team writes: “Priority is a code assigned to requests for disclosure that contain agreed to, best effort target response times.”, the BC asks what if best efforts repeatedly fall short of target response times? Is there a remediation path, and can it be mandated?

- Regarding: “In Phase 1, registrar response targets for SSAD Priority 3 requests will be five (5) business days.”, the BC advocates an at maximum three (3)-day response time, noting that Friday and weekend attacks are already a common practice designed to exploit response downtimes.

- Regarding: “In Phase 2, Contracted Party compliance targets for SSAD Priority 3 requests will be ten (10) business days.”, the BC finds this to be far too long and advocates for a three (3)-day response time.

- Where the EPDP team recommends: “The SSAD will calculate Contracted Party’s mean compliance target every 3 months. If the Contracted Party’s mean compliance target exceeds ten business days, Contracted Party will be subject to compliance enforcement.”, the BC finds that language needs to be added to the RAA to allow Compliance to enforce. Similarly, it is insufficient to suggest only a Compliance inquiry for the failure to provide a rationale for missing the five-day target in Phase 1 and highlights the need for enforcement measures and procedures.

- Regarding: “Small Team recommends SSAD response times and associated statistics be as transparent as legally permissible in order to improve the SSAD and keep the community informed.”, the BC favors elucidation of a publication schedule in order to improve transparency and accountability. We recommend at least every 90 days.

- Finally, where the EPDP team writes: “These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention if legally permissible.”, the BC requests additional detail be added. Any requests that can legally be automated MUST be. Further, who decides whether/ when such automated disclosure is legally permissible?

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

Please refer to the BC’s reply to Recommendation 9 question 25 for specifics.

Section 3, EPDP Phase 2 Recommendations #10-16

Recommendation #10: Acceptable Use Policy

https://docs.google.com/document/d/1JHgbtfvnHezDhEJLkj6KxvGC1bvGu1v7XZA73Z47IMA/edit?usp=sharing.

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

Support recommendation as written

X **Support intent of recommendation with edits**

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

29. If your response requires an edit of Recommendation #10, indicate revised wording and rationale here.

- Regarding: "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.", this could be clarified regarding who can trigger a misuse enforcement mechanism (e.g., the Central Gateway Manager, a third party, etc.).

Recommendation #11: Disclosure Requirement

https://docs.google.com/document/d/1r6qgmnI0ha0mmYqP0Z3drZr3FJsxG-uW9bRC2bJ4Uo/edit?usp=sharing.

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

Support recommendation as written

X **Support intent of recommendation with edits**

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

31. If your response requires an edit of Recommendation #11, indicate revised wording and rationale here.

- Where the EPDP team writes: "For the avoidance of doubt, every response does not have to go through an enforcement procedure; the enforcement mechanism may, however, be triggered in the event of apparent misuse.", the BC repeats that this could be clarified regarding who can trigger a misuse enforcement mechanism (e.g., the Central Gateway Manager, a third party, etc.).

- f): The BC recommends additional language, as follows: "MUST disclose to the Registered Name Holder (data subject), on reasonable request [INSERT by the data subject] , confirmation of the processing of personal data relating to them, per applicable law;". The BC, however, would consider an exemption to this language in the event of sensitivity of law enforcement investigations.

  Stated another way, a "right to erasure" should not be used to mask a fraudulent or criminal registrant. A criminal made aware of a request for personal data cannot serve as a blanket open door to erasing that data, as it would seriously impact law enforcement actions.

- The BC further recommends the addition of an item j in the alphabetized list, which would read: MUST disclose data where such disclosure is not prohibited by or required by applicable law.

Recommendation #12: Query Policy

https://docs.google.com/document/d/1_ng86GC09Ye5ruCBk4vBrXZN7nCyagAanJT9aSDBrGQ/edit?usp=sharing.

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

Support recommendation as written

X **Support intent of recommendation with edits**

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

33. If your response requires an edit of Recommendation #12, indicate revised wording and rationale here.

- a): The term "appropriate action" needs definition, including the enumeration of graduated penalties.
- 4): This recommendation needs to be re-written. As written, a controller failing SLAs for its own reasons would penalize the submitter, who may not be acting in an abusive way.
- Where the EPDP team writes: "As with other access policy violations, abusive behavior can ultimately result in suspension or termination of access to the SSAD.", the BC is concerned this allows too much latitude for termination. It would be prudent to include graduated penalties vs. the "cliff" of sudden termination, similar to how ICANN warns a registrar prior to revoking their accreditation.
- Regarding the following: "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.", more specificity is required regarding WHERE within ICANN org relief can be pursued. Further, the RAA should be amended to detail enforcement measures.
- Regarding the footnote that reads: "The EPDP Team expects implementation to reasonably determine how many may be submitted at a time and consistent with the Query Policy.", the BC suggests following UDRP rules where, if it can reasonably be argued that there is common ownership of domains at issue, there is no limit to joinder.

Recommendation #13: Terms of Use

https://docs.google.com/document/d/1ou3hY3peDnxgo45FmUBs_cIv4f3qUntYecIg10wB__4/edit?usp=sharing.

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

Support recommendation as written

X **Support intent of recommendation with edits**

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

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

- Overall, the principles and disclosures listed under "Policy for SSAD Users" should be mirrored and made clear to registrants in registrant agreement as required by GDPR and other applicable laws.
- The BC applauds giving consideration to RAA updates in order to ensure compliance with the recommendations.

- Regarding agreements for SSAD users, the BC asks the EPDP team to consider whether or not such an agreement would be redundant to the code of conduct and other agreements.

Recommendation #14: Retention and Destruction of Data

https://docs.google.com/document/d/1tBf2jEWlXydskYXxYAjOObebuFgL4iYIHqhBwdo86pU/edit?usp=sharing.

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

X **Support recommendation as written**

Support intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

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

N/A

Recommendation #15: Financial Sustainability

https://docs.google.com/document/d/1EN7mDz44BkxoW_RVlDsgjxhSLkUgrW5XwxIX-O-0TEk/edit?usp=sharing.

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

Support recommendation as written

X **Support intent of recommendation with edits**

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

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

- Where the EPDP team writes: "The subsequent running of the system is expected to happen on a cost recovery basis whereby historic costs may be considered.", the BC asks for clarification on the parameters of "historic costs."
- Regarding: "Similarly, some of the cost of running the SSAD may be offset by charging fees to the users of the SSAD.", fees, if charged, should be based strictly on a cost recovery model.
- The BC notes that fees may violate data privacy laws that prevent companies from selling personal information -- the EPDP team should take care in this regard.
- The BC agrees that "The SSAD SHOULD NOT be considered a profit-generating platform for ICANN or the contracted parties." However, the statement that "Funding for the SSAD should be sufficient to cover

costs, including for subcontractors at fair market value and to establish a legal risk fund." is vague. A legal risk fund seems excessive.

- Regarding: "The EPDP Team also recognizes that the SSAD fee structure may need to be reviewed over time.", the BC recommends adding language about frequency of reviews and by whom.

Recommendation #16: Automation

https://docs.google.com/document/d/1_gqq1JKHcDqVKKfdwOdfAghPYm-ErV2t9qxJVDsDjWc/edit?usp=sharing.

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

Support recommendation as written

Support intent of recommendation with edits

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

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

- The EPDP team writes: "This automation allows for efficient queue management on the discloser's side and assists in ensuring the principal (*sic*) of "predictability" is met." The BC advises that predictability is met only if there's a communication to the requestor outlining timing expectations. Otherwise, requestors are left uninformed.

- Where the EPDP team recommends: "These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention.", the BC believes, again, that any requests that can be responded to in an automated manner MUST/SHOULD be.

Section 3, EPDP Phase 2 Recommendation #17

Recommendation #17: Logging

https://docs.google.com/document/d/1zG2myy1brxbXBHBvd34gm_J-vXPEr6GoBOoWFqi9RQ/edit?usp=sharing.

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

Support recommendation as written

X **Support intent of recommendation with edits**

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

- Regarding: "Logs MUST be retained for a period sufficient for auditing and complaint resolution purposes, taking into account statutory limits related to complaints against the controller", the BC advises the retention period must be sufficiently long, at least at first, to accommodate all parties' adoption to the system and to support "evolution" of automation efforts.

- Where the EPDP team recommends that "Disclosure decisions including a written rationale must be stored and put in escrow so it can be accessed by ICANN and the contracted parties in case of objections or legal claims raised to support a legal defense.", the BC believes this also should include the same latitude for compliance purposes by ICANN, such as responding to complaints, auditing contracted parties, and/or enforcing against parties not meeting their disclosure obligations.

- The BC recommends further that data to measure disclosure/non-disclosure rates (along with decisional rationale) MUST be logged and archived, that data MUST be analyzed and measured, then audited and publicly reported (after ensuring personal information is removed).

Section 3, EPDP Phase 2 Recommendations #18-19,

Implementation Guidance

Recommendation #18: Audits

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

Support recommendation as written

X **Support intent of recommendation with edits**

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

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

- Regarding: "If ICANN outsources the accreditation authority function to a qualified third party, the accrediting authority MUST be audited periodically to ensure compliance with the policy requirements as defined in the accreditation preliminary recommendation.", the BC recommends audits yearly for the first three years, then every two years following. We recommend the same for audit frequency of identity providers.

- In terms of auditing the Accreditation Authority, if ICANN org is not the authority, would the authority be required to audit governmental entities, or would any authority be exempt from auditing governmental entities?

- The BC suggests an audit of Controllers to ensure proper disclosures -- e.g., no controllers that systematically deny or ignore requests through SSAD.

Recommendation #19: Mechanism for the Evolution of the SSAD

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

Support recommendation as written

X **Support intent of recommendation with edits**

Intent and wording of this recommendation requires amendment

Delete recommendation

No opinion

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

The BC advises that any working group "controlling" the evolution of the SSAD MUST include the GAC, ALAC and SSAC; further, their decisions should not be subject to reversal by the GNSO.

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

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

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

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

Implementation Guidance #i.

https://docs.google.com/document/d/1uh3VfWkOZyU7NpVupPU7VBuoW6Lo1N65HUUPnGbBgr4/edit?usp=sharing.

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

X **Support implementation guidance as written**

Support implementation guidance with edits

Intent and wording of this implementation guidance requires amendment

Delete implementation guidance

No opinion

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

N/A

Reporting Requirements

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

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

N/A

Other Comments & Submission

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

N/A

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