Recommendation #12 – Query Policy

"The EPDP Team recommends that Contracted Parties:

MUST NOT reject disclosure requests from SSAD on the basis of abusive behavior which has not been determined abusive by the CGM as per a) and b) above. "

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
63. BC IPC /ALAC	There should be a similar recommendation that applies to Contracted Parties regarding the Query Policy.	Add "In addition, the Contracted Party MUST NOT reject queries from the SSAD on the basis of abuse which have not been determined Abusive by the CGM."	Change applied as follows: added "The EPDP Team recommends that Contracted Parties: MUST NOT reject disclosure requests from SSAD on the basis of abusive behavior which has not been determined abusive by the CGM as per a) and b) above. " **Flagged for discussion**: RrSG: Not ok with the proposed change RySG: We strongly disagree with this addition. This is encroaching beyond the procedural remit of the disclosure decision. The controller must consider all evidence available to them when considering the impact to the rights of the affected data subject. ICANN/CGM may decide censure for use of the SSAD, but they are not the arbiter for a fundamental abuse of data subject rights. A controller, in their decision to disclose must consider any abusive activity which is apparent to them, which, they, in

			their opinion as the controller, deem relevant. Consider the consequences. Should the controller not release, the data, there is no impact on the data subject's rights. A requester may appeal, procedural expectations under the SSAD may give recourse where such a decision is deemed arbitrary and lacking in transparency If the controller releases the data of the data subject, ignoring valid indicators of abusive activity by the requester because 'the policy forces the controller to ignore what are otherwise valid suspicions of abusive activity, because ICANN/CGM haven;t agreed they breached the rules of the SSAD, then any misuse of that data is a prime facie data breach by the controllers, who have failed in their duty to properly vindicate the data rights of the data subject. ALAC - The proposed language speaks about the acceptance/rejection of queries; it does not speak about the disclosure of the data. After the relevant CP accepts the request for disclosure it may accept or reject the disclosure of the data based on its assessment and as outlined in other recommendations. If "as determined Abusive by the CGM" is too strong, what alternative is suggested by the

			CP to ensure that requests are not rejected capriciously? ISPCP - One of the fundamental principles of the GDPR is that it prohibits processing of personal data unless there is a legal basis for doing so. Thus, the requirements for compliance processing must be present before the data is processed. If there is doubt whether nor not abuse is given, I,.e. whether or not the data might be processed in an illegal manner, the requests should not be processed by the CP. Whether denial is the right way can be discussed. It is also possible to suspend the processing of such requests until a determination is made whether or not abuse is given or not. *Discussed during 23/6 meeting: No agreement to apply changes.*

The EPDP Team recommends:
(…)
The SSAD MUST be able to save the history of the different disclosure requests, in order to keep traceability of exchanges between the SSAD requestors and Contracted Parties via the SSAD. Appropriate safeguards need to put in place to safeguard this information. **Appropriate access** to such relevant records should be provided to the CPs, as deemed necessary, to ensure that all relevant information relating to requests for disclosure are available for consideration in such disclosure decisions.

Group	**Text & Rationale**	**Proposed updated text**	**For EPDP Team Consideration**
64. ICANN Org			Can the EPDP team please clarify what "appropriate access" means? Who deems what is "necessary" and "relevant?" Are

			Contracted Parties entitled to see all historical requests from any and all requestors, whether the requests were approved or denied, including requests sent to other Contracted Parties Input provided: ISPCP - CPs should only see the data pertaining to the registration they handle based on the principle of data minimisation. As joint controllers, though, they might need to have rights to audit / verify more data, so further processing cannot be ruled out entirely. ALAC - Agree, CPs should be able to see the data associated with them and not with others. There is no need for the words "Appropriate" and " Necessary" *Discussed during 23/6 meeting: CPs should be able to see own data, not data of others. Change data to activity statistics.*

Recommendation #15 – Financial Sustainability

"The EPDP Team expects that the costs for developing, deployment and operationalizing the system, similar to the implementation of other adopted policy recommendations, to be initially borne by ICANN org, Contracted Parties and other parties that may be involved. As part of the operationalization of SSAD, ICANN org is expected to consider building on existing mechanisms or using an RFP process to reduce costs rather than building the SSAD and its components from scratch. It is the EPDP Team's expectation that the SSAD will ultimately result in equal or lesser costs to Contracted Parties compared to manual receipt and review of requests."
(…)

It is the EPDP Team's expectation that the SSAD will ultimately result in equal or lesser costs to Contracted Parties compared to manual receipt and review of requests as a measure of commercial and technical feasibility.

Question:

1. Even though the EPDP Team dismissed the idea of separating out implementation guidance from policy recommendations for this recommendation previously (it is currently all a policy recommendation), several parts read like implementation guidance ("expects", "it is the expectation"). Is the EPDP Team willing to reconsider moving expectations to an implementation guidance section? If not, is the EPDP Team comfortable in rewriting this so it reads like policy recommendations (e.g. ICANN org, Contracted Parties and other parties that may be involved MUST initially bear the costs for developing, deploying and operationalizing the system, similar to the implementation of other adopted policy recommendations.

(…)
The EPDP Team recognizes that the fees associated with using the SSAD may differ for users based on request volume or user type among other potential factors. The EPDP Team also recognizes that governments may be subject to certain payment restrictions, which should be taken into account as part of the implementation.
(…)

Group	**Text & Rationale**	**Proposed updated text**	**For EPDP Team Consideration**
67. ALAC	The ALAC supports the SSAC comment above. ment says the fee structure will be determined during implementation but it is not specific on who will do that. In the normal course of events, it is possible that the formally constituted IRT may not have sufficient representation from the users of the SSAD and there must be an explicit requirement for suitable consultation and involvement.	Add to the paragraph starting "The EPDP Team recognizes that the fees …" The prospective users of the SSAD, as determined based on the implementation of the accreditation process and Identity Providers to be used, must be fully involved in the discussions on setting usage fees for the SSAD. In particular, those potential SSAD requestors who are not part of the ICANN community must explicitly be included."	EPDP Team to indicate if there are any concerns about this proposed addition ("The prospective users of the SSAD, as determined based on the implementation of the accreditation process and Identity Providers to be used, must be fully involved in the discussions on setting usage fees for the SSAD. In particular, those potential SSAD requestors who are not part of the ICANN community must explicitly be included."). **Input received**: ● RrSG – Do not agree

			• ICANN Org: The proposed new language seems to be phrased as Implementation Guidance. ICANN org notes that fees are typically derived from a variety of sources, including financial analysis, projections, and others. This could include consultation with potential users as described here; however, it may not be possible to arrive at a fee model supported by all potential stakeholders. • ISPCP - No change to report language required. • ALAC - Why? [RrSG – Do not agree] Prospective users will not likely be part of the full IRT but their input MUST be factored in when deciding on prices and pricing models.

(…)
The objective is that the SSAD is financially self-sufficient without causing any additional fees for registrants. Data subjects MUST NOT bear the costs for having their data disclosed to third parties; requestors of the SSAD data should primarily bear the costs of maintaining this system. ICANN MAY contribute to the (partial) covering of costs for maintaining the Central Gateway.[1]
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
70. NCSG	Paragraph 6 in rec#15: "Data subjects MUST NOT bear the costs for having their data disclosed to third parties;"	Data Subjects MUST NOT bear the costs for having data disclosed to third parties. Furthermore, Data Subjects	EPDP Team to indicate if there are any concerns about these proposed changes and addition ("Data subjects MUST NOT bear the

[1] Although it is understood that registrants are ultimately the source of much of ICANN's revenue, this is not deemed to be a violation of "Data subjects MUST NOT bear the costs for having their data disclosed to third parties".

	This indicates that the only true restriction on Data Subjects bearing the costs is associated with disclosure of their own data to third parties. This leaves a loophole where the costs of processing of disclosure requests may be distributed among Data Subjects, even if they are not explicitly paying for the costs of having "their" data disclosed. Furthermore, it does not address the costs of processing disclosure requests in which the request has been denied.	MUST NOT bear the costs of processing of data disclosure requests, which have been denied by Contracted Parties following evaluation of the requests submitted by SSAD users.	costs for having ~~their~~ data disclosed to third parties. **Furthermore, Data Subjects MUST NOT bear the costs of processing of data disclosure requests, which have been denied by Contracted Parties following evaluation of the requests submitted by SSAD users.**) Input provided: ISPCP - No problem with the suggested clarification.

In relation to the accreditation framework:
(…)
c. Fees are to be established by the accreditation authority.
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
72. ICANN org	c) "Fees are to be established by the accreditation authority." ● Can the EPDP team please clarify if the Accreditation Authority outsources the Identity Provider function, would the Identity Provider be able to set its own fee schedule?		EPDP Team to clarify if the Accreditation Authority outsources the Identity Provider function, would the Identity Provider be able to set its own fee schedule? Input received: ● RrSG – no opinion ● ISPCP - This should be discussed. There is no problem with the identity provider determining its own fee as long as the fees are reasonable.

			• ALAC - The ultimate responsibility lies with the accreditation authority so if the accreditation authority outsources the function of the identity provider, the identity provider could be allowed to set its own fees but after consulting with the accreditation authority.

Implementation Guidance

There are various implementation details that may have policy implications, particularly with respect to cost distribution and choice of party who performs various data protection functions. These issues are collected here under Implementation Guidance for consideration.
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
73. NCSG	From Implementation Guidance: "There are various implementation details that may have policy implications, particularly with respect to **cost distribution** and choice of party who performs various data protection functions. These issues are collected here under Implementation Guidance for consideration." Rationale: It is unclear why "cost distribution" is in this part of Implementation Guidance, especially considering its relevance to recommendation 19. Although costs cannot be determined at this time, what does their distribution mean in this context? Does it mean that the burden of	The intent of use of "cost distribution" needs to be clarified.	EPDP Team to clarify intent of use of "cost distribution" Input provided: ISPCP - As NCSG has brought up the issue, do they have a suggestion?

	bearing the costs may be changed as an implementation measure?		

Recommendation #17 – Logging

a. The activity of all SSAD users MUST be logged. (for further details, please see the implementation guidance below).

(…)

d. Logs SHOULD NOT contain any personal information. If any information is logged that does contain personal information, appropriate safeguards need to be in place. Logs may be made publicly available as long as any personal information has been removed (see also recommendation #NEW on reporting requirements). Logged data that contains personal information MUST remain confidential.

(…)

f. Relevant log data MUST be disclosed, when legally permissible, in the following circumstances:
   - In the event of a claim of misuse, logs may be requested for examination by an accreditation authority or dispute resolution provider.
   - Logs should be further available to ICANN and the auditing body.
   - When mandated as a result of due legal process, including relevant enforcement and regulatory authorities, as applicable.

   Relevant logged data MAY be disclosed for:
   - General technical operation to ensure proper running of the system.

   Relevant logs should also be made available in SSAD to allow requestors and Contracted Parties to review their own statistics. These logs shall not contain any personal data

(…)

Implementation guidance:

At a minimum, the following events MUST be logged

- **Logging related to the Identity Provider**
- Logging related to the Accreditation Authority
  - Details of incoming requests for Accreditation
  - Results of processing requests for Accreditation, e.g., issuance of the Identity Credential or reasons for denial
  - Details of Revocation Requests
  - Indication when Identity Credentials and Signed Assertions have been Validated.
  - Unique reference number
- Logging related to the Central Gateway Manager

- Information related to the contents of the query itself.
- Results of processing the query, including changes of state (e.g., received, pending, in-process, denied, approved, approved with changes)
- **Rates of:**
    - **disclosure and non-disclosure**;
    - **use of each rationale for non-disclosure;**
    - **divergence between the disclosure and non-disclosure decisions of a CP and the recommendations of the gateway**.

- Logging related to Contracted Parties
    - Request Response details, e.g., Reason for denial, notice of approval and data fields released. **Disclosure decisions including a written rationale must be stored; access to such rationale however will be subject to applicable law; and shall be strictly limited with due regard to necessity or review, and any and all access itself should be appropriately monitored and logged**.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
80. ICANN org	"Logging related to the Identity Provider" As there are no sub-bullets listed under this item, can the EPDP team please clarify whether this means there are no requirements related to loggin for the Identity Provider?		EPDP Team to clarify what the logging requirements are for Identity Providers **Input received:** ● RrSG – no opinion
81. ICANN org	"Rates of: disclosure and non-disclosure; use of each rationale for non-disclosure; divergence between the disclosure and non disclosure decisions of a CP and the recommendations of the gateway." Can the EPDP team please clarify how rates relate to logging? Furthermore, are the rates related to disclosure and non-discosure by requestor or by Contracted Party? Finally, the guidance contemplates that rationales would be		EPDP Team to clarify how rates relate to logging? Furthermore, are the rates related to disclosure and non-disclosure by requestor or by Contracted Party? Finally, the guidance contemplates that rationales would be captured. Have these rationales been compiled somewhere? Does the EPDP team anticipate that the Central Gateway will be categorizing rationales? Given that these are likely to be free form descriptions, this may be challenging to implement. Perhaps the team could suggest implementation guidance

	captured. Have these rationales been compiled somewhere? Does the EPDP team anticipate that the Central Gateway will be categorizing rationales? Given that these are likely to be free form descriptions, this may be challenging to implement. Perhaps the team could suggest implementation guidance related to capturing rationales either in this recommendation or in Rec #6.		related to capturing rationales either in this recommendation or in Rec #6?
82. BC	Original comment: RySG ● Disclosure decisions including a written rationale must be stored. Unsure what the significance of a "written" rationale is. The RYSG also notes again that 'rationale' will ordinarily contain PII. Which is at odds to REcommendation 17 D which states logs should not contain PII. needs to be clearer	Change to: Disclosure decisions including a rationale must be stored; access to such rationale however will be subject to applicable law, and shall be strictly limited with due regard to necessity or review, and any and all access itself should be appropriately monitored and logged.	Change applied **Flagged for discussion:** BC - #12 I'd like to better understand why RySG maintains that rationales will "ordinarily" contain personal data. We may be using the term differently. Revert to original text (minus "written").

Recommendation #2 – Accreditation of Governmental Entities

The development and implementation of an accreditation procedure that specifically applies to governmental entities will facilitate decisions that these data controllers] will need to make before granting access to registration to a particular entity or automated disclosure decisions, if applicable. This accreditation procedure can provide data controllers with information necessary to allow them to assess and decide about the disclosure of data.

86. ICANN org	Use of "data controller" in this paragraph and through the recommendation may be confusing in implementation as it is not yet clear which party/parties will be deemed to be controllers.	ICANN org suggests replacing "data controller" throughout the recommendation with the relevant Contracted Party or the	RrSG: OK with this change ISPCP: OK with this change

		Central Gateway Manager, as applicable.	

[2] Intergovernmental organizations (IGOs) are also eligible for accreditation under recommendation #2. An IGO that wants to be accredited MUST seek accreditation via any relevant Accreditation Authority from the countries that ratified its founding treaty and empower the IGO.

87. ICANN org	Footnote 2 says that any country that ratifies an IGO's treaty may accredit that IGO. ICANN org understood from the team's previous discussion that IGO accreditation would be conducted by the IGO's host country. Can the EPDP team please clarify whether footnote 2 reflects the team's agreement?		RrSG: no opinion

Recommendation #8 –

Original Language:
ICANN Compliance will not be in a position to address the merits of the request itself or the legal discretion of the Contracted Party making the determination.

Alternative language provided by Laureen:
ICANN Compliance will not address the merits of the request itself or the Contracted Party's conclusions, if applicable, in balancing the rights of the data subject with the legitimate interests of the requester. For avoidance of doubt, this does not preclude ICANN Compliance from addressing complaints related to allegations of unreasonable denials of requests to disclose data, especially where there is evidence of widespread and unjustified denials of disclosure requests.

Non-Substantive Items / Clarifications provided

Recommendation #2

Accreditation by a country's/territory's government body or its authorized body[1] would be available to various eligible government entities[2] that require access to non- public registration data for the exercise of their public policy task, including, but not limited to:

- Civil and criminal law enforcement authorities,
- Data protection and regulatory authorities
- Judicial authorities~~,~~
- Consumer rights organizations granted a public policy task by law or delegation from a governmental entity~~,~~
- Cybersecurity authorities granted a public policy task by law or delegation from a governmental entity, including national Computer Security Incident ~~Emergency~~ Response Teams (~~CERTs~~CSIRTs)~~,~~

Group	Change that has resulted in cannot live with status & Rationale	Proposed updated text	For EPDP Team Consideration
83. GAC	Use of term CERT - Isn't the correct term "CSIRT" as opposed to CERT (which I believe is a TM 'd term that has become somewhat genericized)?	Replace CERTs with CSIRTs	Change applied Flagged for discussion: GAC disagreed with this change proposed by RySG, noting: CERT is more relevant to governmental entities. ***Staff support team proposed approach: revert back to CERTs.***
84. ICANN org	"Consumer rights organizations granted a public policy task by law or delegation from a governmental entity" ICANN org is unclear how to enforce this requirement. May a government accredit a private entity within its jurisdiction? What about private		RrSG: There is already structure for governments to designate entities as exercising a public policy task which should address these requirements (similar to 3.18.2 of the RAA). Further details can be addressed during the implementation period.

	entities outside its jurisdiction? What about private individuals within its jurisdiction? And private individuals outside its jurisdiction?		***Staff support team proposed approach: See clarification provided by RrSG. Further details to be addressed during implementation period.***

SSAD MUST ~~ensure~~ ~~facilitate~~provide reasonable access to ~~non-public~~ registration data~~RDDS~~ for entities that require access to this data for the exercise of their public policy tasks. In view of their obligations under applicable data protection rules, the final responsibility for granting access to ~~RDDS~~ ~~non-public~~ registration data will remain with the party that is considered to be a controller for the processing of that ~~RDDS~~ ~~non-public~~ registration data that constitutes personal data.

85. GAC	Original comment RySG: The SSAD cannot "ensure" but it can be designed and created to "facilitate".	Change to SSAD MUST facilitate reasonable access to...	Change applied Flagged for discussion: GAC disagreed with this change, and provided, "SSAD MUST provide reasonable access" ICANN org is unclear how this requirement should be implemented. There are several entities that make up the SSAD. How would each implement this requirement? ICANN org understands this statement as an objective. Is ICANN org expected to enforce a requirement of "reasonable access" and against which party? ***Staff support team proposed approach: See response provided by RrSG. Apply change suggested by GAC.***

a) Accreditation emphasizes the responsibilities of the data requestor (recipient), who is responsible for complying with the law.
b) Accreditation will focus on the requirements of the law, such as requirements regarding data retention length, secure storage, organizational data controls, and breach notifications.
c) Renewal, Logging, Auditing, Complaint and De-accreditation will be handled as per Rec. 1
d) Data access

88. ICANN org	d. Data access		As there is no description, ICANN org suggests deleting this bullet. RrSG: Agree with deleting ISPCP: OK with change ***Staff support team proposed approach: Delete d.***

Implementation guidance:
(…)
Accredited users will be required to follow the safeguards as set by the policy. This is without prejudice for the entity to respect safeguards under its domestic law.
(…)
Accredited entities SHOULD provide details to aid the disclosure decision such as any applicable local law relating to the request.

89. ICANN org	Accredited users will be required to follow the safeguards as set by the policy. This is without prejudice for the entity to respect safeguards under its domestic law.		Can the EPDP team please clarify to which safeguards does this guidance refer? Is it the Terms of Use and other policies as defined in Rec 10-13-14? RrSG: Yes. ISPCP: Yes

			Staff support team proposed clarification: ICANN org assumption is correct.
90. ICANN org	"Accredited entities SHOULD provide details to aid the disclosure decision such as any applicable local law relating to the request."		Can the EPDP team please clarify to whom the details would be provided? Would it be included in the request that is sent to the Contracted Party? RrSG: Yes. ISPCP: Yes ***Staff support team proposed clarification: ICANN org assumption is correct.***

Recommendation #15 – Financial Sustainability

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
65. RrSG			This is a general comment rather than response to one specific change. We note that the "data subject" is not always the "registrant" of the domain, and so the text should refer to "data subject" where appropriate throughout the whole Report Input provided: ISPCP - agreed

			Staff support team proposed approach: review consistency throughout the report of use of data subject vs. registrant

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
66. ICANN org	"The EPDP Team expects that the costs for developing, deployment and operationalizing the system, similar to the implementation of other adopted policy recommendations, to be initially borne by ICANN org, Contracted Parties and other parties that may be involved. As part of the operationalization of SSAD, ICANN org is expected to consider building on existing mechanisms or using an RFP process to reduce costs rather than building the SSAD and its components from scratch. It is the EPDP Team's expectation that the SSAD will ultimately result in equal or lesser costs to Contracted Parties compared to manual receipt and review of requests."		This paragraph references what the EPDP team "expects." For clarity, can the team please explain whether this is intended as implementation guidance or should be considered a policy requirement? If the latter, ICANN org suggests rephrasing this language to make clear who must do what. ***Staff support team proposed approach: rephrased in question 1 – under financial sustainability***.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
68. ICANN Org	Original Comment: ALAC The ALAC agrees with "ICANN MAY contribute to the (partial) covering of costs for maintaining the Central Gateway." but it needs a footnote to	Add a footnote to "ICANN MAY contribute to the (partial) covering of costs for maintaining the Central Gateway." saying "Although it is understood that registrants are	ICANN org: Item #4 adds the footnote: "Although it is understood that registrants are ultimately the source of much of ICANN's revenue, this is not deemed to be a violation of

	make it clear that this is not a violation of the requirement that data subjects not bear the costs for having their data disclosed to third parties	ultimately the source of much of ICANN's revenue, this is not deemed to be a violation of "Data subjects MUST NOT bear the costs for having their data disclosed to third parties".	"Data subjects MUST NOT bear the costs for having their data disclosed to third parties". ICANN org understands this footnote to mean that data subjects must not be charged a separate fee by the Central Gateway for having their data requested by or disclosed to third parties. However, ICANN org notes that registered name holders will always indirectly bear any costs incurred by registrars and registries, as noted in item #10 below. ICANN org is unsure how this recommendation should be implemented. ICANN org understands that the Gateway may not charge a fee to registered name holders. However, the RAA prohibits ICANN from limiting what Registrars may charge. RAA 3.7.12 states: "Nothing in this Agreement prescribes or limits the amount Registrar may charge Registered Name Holders for registration of Registered Names." Input provided: ICANN Org is correct. If a registrar would CHOOSE to add a fee associated with addressing queries (whether to ultimately fund the SSAD or to fund its own query evaluation process, there is nothing ICANN can do about it. Perhaps Rr can offer language that would fulfil the intent of this while not violating

			the RAA. Ultimately we MUST have a guarantee that we will not have an objection filed based on the inherent conflict by most money coming from registrants but ICANN is allowed to contribute. ***Staff support team proposed approach: as no further reactions have been received, it is assumed that the ICANN org clarification is understood.***

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
69. ICANN org	Original Comment: RySG "It is the EPDP Team's expectation that the SSAD will ultimately result in equal or lesser costs to Contracted Parties compared to manual receipt and review of requests."	RySG: It is the EPDP Team's expectation that the SSAD will ultimately result in equal or lesser costs to Contracted Parties compared to manual receipt and review of requests as a measure of commercial and technical feasibility."	ICANN org: ICANN org does not understand how this sentence of the recommendation ought to be implemented: "It is the EPDP Team's expectation that the SSAD will ultimately result in equal or lesser costs to Contracted Parties compared to manual receipt and review of requests as a measure of commercial and technical feasibility." ICANN org previously suggested that most of this recommendation could be listed as Implementation Guidance. ICANN org again suggests the EPDP Team reconsider this suggestion. For example, can the EPDP team please clarify who must do what in order to implement this sentence? Does the EPDP

			mean that Contracted Parties MUST share information about their operational costs? ***Staff support team proposed approach: rephrased in question 1 – under financial sustainability.***

71. ICANN org	"Data subjects MUST NOT bear the costs for having their data disclosed to third parties; requestors of the SSAD data should primarily bear the costs of maintaining this system." ICANN org notes that ultimately registrants will indirectly bear all of these costs. Can the EPDP please confirm ICANN org's understanding that this sentence means registrants should not be charged a separate or direct fee for the SSAD?		EPDP Team to confirm ICANN Org's understanding that 'data subjects must not bear the costs' means registrants should not be charged a separate or direct fee for the SSAD. See also footnote added per comment #4 that may already provide some clarification. **Input received**: ● RrSG – Agree should not be direct or separate fee. There should also not be indirect costs ● ISPCP: Agree with RrSG input. ● ALAC: See ALAC #68 ***Staff support team proposed approach: as no further reactions have been received, it is assumed that ICANN org's understanding is correct.***

Recommendation #17 Logging

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration

74. ICANN org	91. The activity of all SSAD entities MUST be logged. (for further details, please see the implementation guidance below).	RySG: Change SSAD "entities" to SSAD "users"	ICANN org does not understand what is meant by "SSAD users." Can the EPDP team please clarify if this meant to encompass requestors? What about Contracted Parties? The Central Gateway? The Accreditation Authority? Identity Providers? In addition, can the EPDP team please clarify who is expected to do the logging? Input provided: BC - Logging must include more than just Requestors (which I think is the most common interpretation of "Users"). For example, the receipt of a request by the CGM MUST be logged by the CGM. Transmission of a request from the CGM to a CP must be logged by the CGM. The metadata (timestamp, yes/no, rationale, etc) of a disclosure request response MUST be logged by the CGM. Proposed updated text: If the verbiage in #3 is not acceptable, suggest: "The CGM shall make logs of all of the activities of all the entities which interact with the CGM." ***Staff support team proposed approach: apply clarification proposed by BC.***
76. ICANN org	a. The activity of all SSAD entities MUST be logged. (for further details, please see the		Can the EPDP team please clarify who is expected to do the logging?

	implementation guidance below).		***Staff support team proposed approach: See previous clarification provided by BC.***

77. ICANN org	f) "Logged data will MUST remain confidential and relevant log data MUST be disclosed, when legally permissible, in the following circumstances:" In addition under f) "Relevant logged data MAY be disclosed for: General technical operation to ensure proper running of the system." Can the EPDP team please clarify who this logged data may be disclosed to and how it may be verified that these entities are relevant to the general technical operation of the SSAD? Also in d) "Relevant logs should also be readily available in SSAD to allow requestors and Contracted Parties to review their own statistics." Can the EPDP team please clarify what "their own statistics" means? For example, does it refer to how many requests submitted? How many were approved?		EPDP Team to clarify in relation to f) "Relevant logged data MAY be disclosed for: General technical operation to ensure proper running of the system." Who may this logged data be disclosed to and how it may be verified that these entities are relevant to the general technical operation of the SSAD? ***Staff support team proposed clarification: as this is a MAY, it is up to the entity to whom this request has been made to determine whether or not data is disclosed and what verification may need to be in place.*** EPDP Team to clarify in relation to d) "Relevant logs should also be readily available in SSAD to allow requestors and Contracted Parties to review their own statistics."

	d) "These logs shall not contain any personal data." Can the EPDP team please clarify whether this "personal data" is in reference to gTLD registration data? Domain names may be considered personal data. Would they not be included? This seems broad. Suggest deleting or clarifying.		Can the EPDP team please clarify what "their own statistics" means? For example, does it refer to how many requests submitted? How many were approved? ***Staff support team proposed clarification: see response to item #64.*** EPDP Team to clarify what reference to 'personal data' is expected to include. Is this in is in reference to gTLD registration data? Domain names may be considered personal data. Would they not be included? Is this too broad? Should the reference be deleted or clarified? ***Staff support team proposed clarification: This is understood to be personal information in general but as this appears to be duplicative of d. suggest removing.***

78. RySG	Relevant logs should also be readily available in SSAD to allow requestors and Contracted Parties to review their own statistics. These logs shall not contain any personal data. • I don't think we are expecting the logs themselves to be available to requestors	Change to: Relevant logs should be used to make available in SSAD data to allow requestors and Contracted Parties to review their own statistics. This data shall not include any personal data.	Change applied – it is understood that the proposed change is to replace 'readily' to 'made' (it is not exactly clear from the proposed text which appears to be grammatically incorrect – RySG to confirm that this is a correct interpretation. **Input provided:** RySG - Apologies this seemed a tad garbled. The thought was to try and delineate between the log data of all relevant

	(surely this would merely a listing in their individual accounts) and contracted parties, rather the data in those logs		requests being made available to the disclosing entities. “logs” should not be available to the requesters, but surely all that data should be recorded as part of the UI in the SSAD? Proposed updated text: Relevant logs should be used as the source to make available any relevant data. This data should enable requestors and Contracted Parties to review their own statistics. This data shall not include any personal data. ***Staff support team proposed approach: clarification provided – apply proposed change.***

79. RySG	Implementation guidance: At a minimum, the following events MUST be logged The MUST in implementation guidance makes it sound like this is a recommendation, not implementation guidance	Either change to “the working group expects that the following events are logged” Or move to the recommendations section as a MUST.	EPDP Team to confirm whether there is a preference to leave this as implementation guidance or whether to move it to the policy section. **Input received:** ● RrSG – move to policy ● ISPCP – move to policy ***Staff support team proposed approach: Move to policy section***