Yellow Items – for discussion / clarification by EPDP Team

(Note, only those sections for which issues have been flagged are included here – for the full context, please see the draft Final Report)

Recommendation #1 – Accreditation

(…)
1.7 Accredited non-governmental entities or individuals:

a) MUST agree to:
   i. only use the data for the legitimate and lawful purpose stated;
   ii. the terms of service, in which the lawful uses of data are described;
   iii. prevent abuse of data received;
   iv. ~~[~~cooperate with any audit or information requests as a component of an audit;~~]~~
   v. be subject to de-accreditation if they are found to abuse use of data or accreditation policy / requirements;
   vi. store, protect and dispose of the gTLD registration data in accordance with applicable law;
   vii. only retain the gTLD registration data for as long as necessary to achieve the purpose stated in the disclosure request.

b) The number of SSAD requests that can be submitted during a specific period of time MUST NOT be restricted, except where the accredited entity poses a demonstrable threat to the SSAD, or where they may be otherwise permitted under these recommendations (e.g. as part of graduated penalties, etc.). It is understood that possible limitations in SSAD's response capacity and speed may apply. For further details see the response requirements recommendation.

c) MUST keep the information required for accreditation and verification up to date and inform the Accreditation Authority promptly when there are changes to this information, which MAY result in re-accreditation or re-verification of certain pieces of information provided.

(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
1. ICANN org	1.7.(a) seems redundant with the policies outlined in the combined Rec. 10-13-14, which cover Terms of Use, Disclosure Agreement and Acceptable Use. Would the EPDP team consider referencing those recommendations instead to provide greater clarity during implementation?	N/A	EPDP Team to confirm whether there are any concerns about removing the requirements in this section but instead refer to recommendations 10-13-14 that cover terms of use, disclosure agreement and acceptable use. **Input provided**:

			• RrSG has indicated that they do not have any concerns about this. *Discussed during 16/6 meeting: leave as is, but staff support team to review whether any requirements that are not yet included in rec #10 – 13 – 14 need to be duplicated there.*
2. BC	Original comment: RySG 1.7 b) Will not be restricted in the number of SSAD requests that can be submitted during a specific period of time For clarity, and to ensure proper safeguards for registrant / data subject rights at the core, there are instances in the recommendations that may restrict the number of requests e.g. graduated penalties etc., we cannot create a contradiction in the recommendations.	The number of SSAD requests that can be submitted during a specific period of time will not be restricted, except where the accredited entity poses a demonstrable threat to the SSAD, or where they may be otherwise permitted under these recommendations (e.g. as part of graduated penalties etc.). It is understood that possible limitations in SSAD's response capacity and speed may apply	Change applied. **Flagged for discussion**: BC: the parenthetical is too broad. Proposed text: "... or where they may be otherwise permitted under recommendation 1.4(d).". *Discussed during 16/6 meeting: Not resolved. Flag for future review, Staff to review entire doc for other exception issues. 12(b) is possible example]*

[FN12] Implementation guidance: ICANN org should use its experience in other areas where verification is involved, such as registrar accreditation, to put forward a proposal for verification of the identity of the requestor during the implementation phase. The level of verification may vary dependent on the type of applicant.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
3. RySG	Original comment: ALAC 1.3(a) or the footnote should note that the thoroughness of the verification may		Change applied – see footnote 12. **Flagged for discussion:**

	vary with the type of applicant (ie verifying that someone claims to be Microsoft will be at a different level than verifying that the e-mail address provided by a one-time user is used by that person).		RySG: What does it mean that "The level of verification may vary dependent on the type of applicant"? Would the level of verification be communicated to the disclosing entity? Would this also be a factor in determining if the requested data should be disclosed? Having different levels of verification hasn't been flushed out and seems problematic to add now. Remove the text "The level of verification may vary dependent on the type of applicant" from footnote 12. *Discussed during 16/6 meeting: Agreement to remove addition ("The level of verification may vary dependent on the type of applicant")*

1.2(c): The Accreditation Authority MUST develop a privacy policy in accordance with the Privacy Policy for Processing of Personal Data for SSAD Users as outlined in recommendation #13.
(…)
1.3 (e): The Accreditation Authority MUST develop a specific privacy policy for the processing of personal data it undertakes as well as terms of service for its accredited users.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
4. ICANN Org	Original Comment: RySG We need to add a requirement that Accreditation Authorities have Terms of Service for accredited users.	Add to 1.1(c): The Accreditation Authority MUST develop a specific privacy policy for the processing of personal data it undertakes as well as	Change applied – note this aligns with the requirements in the SSAD Terms and Conditions recommendation. EPDP Team members to flag if they cannot live with this change.

	The recommendation requires that an Accreditation Authority have a Code of Conduct applicable to them (see footnote 5) but no requirement that an Accreditation Authority have Terms of Service for accredited users (even though accredited users will assert that they will adhere to any terms of service.)	terms of service for its accredited users.	**Flagged for discussion:** ICANN Org - This seems to revisit language that was replaced in 1.2 c) "The Accreditation Authority MUST develop a privacy policy in accordance with the Privacy Policy for Processing of Personal Data for SSAD Users as outlined in recommendation #13." Can the EPDP team please explain how these are different? If the requirements are the same, suggest using the language in 1.2 c) and deleting 1.3 e). 1.2 c) can also include a reference to Terms of Use as outlined in Recommendation #13: The Accreditation Authority MUST develop a privacy policy in accordance with the Privacy Policy for Processing of Personal Data for SSAD Users and Terms of Use for SSAD Users as outlined in recommendation #13." *Discussed during 16/6 meeting: Action item for RySG team to review this input offline and provide feedback on the mailing list.*

Recommendation #3 – 5 – 8

Recommendation #3
(…)

The EPDP Team recommends that each SSAD request MUST include all information necessary for a disclosure decision, including the following information:
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
5. ICANN org	Rec #3, 2nd paragraph: "The EPDP Team recommends that each SSAD request MUST include all information necessary for a disclosure decision, including the following information: " For implementation purposes, could the EPDP team clarify whether a request could refer to a signed assertion, which may provide all of the required information in b-c-d? Or would this information be provided in a separate form in the request?	N/A	EPDP Team to clarify for implementation purposes whether a request could refer to a signed assertion, which may provide all of the required information in b-c-d? Or would this information be provided in a separate form in the request? **Input provided:** • RrSG: May refer to signed assertion • IPC: Yes, the request would include signed assertions. These would not be separate. *Discussed during 16/6 meeting: Agreement that a signed assertion could provide all of the required information.*

Recommendation #5
a) Acknowledgement of receipt
    a) Following confirmation that the request is syntactically correct and that all required fields have been filled out, the Central Gateway Manager MUST immediately and synchronously respond with the acknowledgement of receipt and relay the disclosure request[1] to the responsible Contracted Party.
(…)

[1] Implementation guidance: the Central Gateway Manager is expected to relay the disclosure request as well as all relevant information about the requestor to the Contracted Party. In the case of disclosure requests for which automated processing of the disclosure decision applies (see recommendation Automation) , the relay of the disclosure request and all relevant information may happen at the same time as the Central Gateway Manager would direct the Contracted Party to automatically disclose the requested data to the requestor.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
6. BC IPC ALAC	3rd paragraph needs to be updated to allow ICANN to make decisions centrally at the gateway. It requires all requests to be sent to the CPH.	Update the 3rd Paragraph to require only those requests that are not decided by the CGM to be relayed to the contracted party.	It is the staff support team's understanding that even for disclosure requests for which it is confirmed that the criteria for automated processing of the disclosure decision apply, the disclosure request and related information must also be provided to the CP for its records and to allow it to review the CGM determination – this relay, as outlined in the footnote, may be provided at the same time as the CP is directed to disclose, but it could also be provided at another point. If this is an incorrect understanding, the EPDP Team should indicate this so this can be updated accordingly in the recommendation, for example by adding "By default, the Central Gateway Manager MUST relay the disclosure request to the Registrar of Record, **unless it concerns a disclosure request to which automated processing of the disclosure decision applies"**. **Input provided**: • RrSG has expressed support for the staff support team's understanding. • IPC: Staff's understanding is incorrect, or is at least it is inconsistent with our understanding. For disclosure requests which are

			automated or centralized, CPs have no need for this information, and are also more likely open to liability if they have this information. The language added in bold below is a good start, and should more accurately read, "automated and/or centralized processing" • ALAC: Depending on the outcome of this discussion, ALAC may have a cannot live with here. There should be no separate step of having the CP consider requests eligible for centralized/automated decision. • RySG: This should not be changed. The CGM does not hold data. The request must be only forwarded to the disclosing party in full. The current language is sufficient. *Discussed during 16/6 meeting: Leave as is – relay of disclosure request in case of automated disclosure decisions is for CP record keeping, not to review/approve CGM determination that criteria for automated disclosure decision have been met.*
7. IPC	Make Footnote 5 part of the policy recommendation. Also must strike "to the requestor" to allow for the CP to provide the data to the CGM, thereby making them not part of the "same processing" for joint and several liability purposes.	Footnote 5 as implementation guidance is insufficient.	The footnote reads: "Implementation guidance: the Central Gateway Manager is expected to relay the disclosure request as well as all relevant information about the requestor to the Contracted Party. In the case of disclosure requests

			for which automated processing of the disclosure decision applies (see recommendation Automation) , the relay of the disclosure request and all relevant information may happen at the same time as the Central Gateway Manager would direct the Contracted Party to automatically disclose the requested data to the requestor." Text to be updated, if necessary, in line with outcome of previous discussion. EPDP Team to indicate if there are concerns about this to the policy recommendation, and removing 'to the requestor'. **Input provided:** IPC: Staff's understanding is incorrect, or is at least it is inconsistent with our understanding. For disclosure requests which are automated or centralized, CPs have no need for this information, and are also more likely open to liability if they have this information. The language added in bold below is a good start, and should more accurately read, "automated and/or centralized processing" RrSG: Agree with move to policy but not strike 'to the requestor

			RySG: This should not be changed. The CGM does not hold data. The request must be only forwarded to the disclosing party in full. The current language is sufficient. *Discussed during 16/6 meeting: Leave as is.*

Recommendation #8
(…)
For Contracted Parties
(…)
e. If the Contracted Party determines that disclosure would be in violation of applicable laws or result in inconsistency with these policy recommendations, the Contracted Party MUST document the rationale and communicate this information to the requestor and ICANN Compliance (if requested).
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
8. ICANN org	Rec #8, bullet d Can the EPDP team please clarify whether "(if requested)" only applies to ICANN Contractual Compliance so that the rationale must only be supplied to ICANN Contractual Compliance should ICANN Contractual Compliance request the rationale?	N/A	EPDP Team to clarify whether "(if requested)" only applies to ICANN Contractual Compliance so that the rationale must only be supplied to ICANN Contractual Compliance should ICANN Contractual Compliance request the rationale? (this paragraph reads: "If the Contracted Party determines that disclosure would be in violation of applicable laws or result in inconsistency with these policy recommendations, the Contracted Party MUST document the rationale and communicate this information to the requestor and ICANN Compliance (if requested)."

			Input provided: • RrSG: 'If requested' only refers to ICANN Compliance *Discussed during 16/6 meeting: Confirmation that 'if requested' only refers to ICANN Compliance. Staff support team to review whether clarification of the text is necessary.*

c. By default, the Central Gateway Manager MUST relay the disclosure request to the Registrar of Record. However, where the Central Gateway Manager is aware of any circumstance, assessed in line with these recommendations, that necessitates the provision of a disclosure request to the relevant gTLD Registry Operator, the Central Gateway Manager MAY relay the disclosure request to the relevant gTLD Registry Operator, provide that the reasons necessitating such a transfer of a request, are provided to the registry operator for their consideration. It must be possible for the requestor to flag such circumstance to the Central Gateway Manager, but the Central Gateway Manager MUST make its own assessment of whether the identified circumstance necessitates the provision of the disclosure request to the relevant gTLD Registry Operator. For clarity, nothing in this recommendation prevents a requestor to directly contact, outside of SSAD, the relevant gTLD Registry Operator with a disclosure request.

~~"If there are jurisdictional issues that would justify consideration of the request by the gTLD Registry Operator. In this specific case, the Central Gateway Manager MUST provide the response of the Registrar of Record to the gTLD Registry Operator as well as identify the jurisdictional issues that resulted in submitting this request to the gTLD Registry Operator."~~

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration

9. BC/IPC	Original Comment: RySG The entirety of the circumstances by which a requestor may request the sending of the request to the Ry are not agreed. • If the Registrar of Record is non-responsive to the disclosure request within the established SLAs; The SLAs contain a number of variables relating to the application of SLAs. The above is not a standalone or valid indicator. Apart from the fact that this falsely assumes some form of breach or SLA failure (which it cannot), this could lead to duplication of processing, duplication of resources. Additionally this should not be 'at the request of the requester' it MUST be based on identifiable and measurable metrics within the central gateway in conjunction with ICANN compliance. A request shall be directed as the systems decides - not as the requester decides. If it is known that the Registrar of Record is unlikely to respond due to circumstances such as bankruptcy or de-accreditation;	By default, the Central Gateway Manager MUST relay the disclosure request to the Registrar of Record. However, where the Central Gateway Manager is aware of any circumstance, assessed in line with these recommendations, that necessitates the provision of a disclosure request, to the relevant registry operator, the Central Gateway Manager, MAY, relay the disclosure request to the relevant gTLD Registry Operator, provided that the reasons necessitating such a transfer of a request, are provided to the registry operator for their consideration.	Change applied but with the addition of the following sentence: "It must be possible for the requestor to flag such circumstance to the Central Gateway Manager, but the Central Gateway Manager MUST make its own assessment of whether the identified circumstance necessitates the provision of the disclosure request to the relevant gTLD Registry Operator." **Flagged for discussion:** BC/IPC: We agreed that a requestor could elect to direct a request to the Registry Operator, at the requestor's option. Revert to original language. *Discussed during 16/6 meeting: Leave as is.*

	As above, this is not a matter for a requester to notify/request, this is a matter for the central gateway to discern and apply where confirmed and necessary. • If there are jurisdictional issues that would justify consideration of the request by the gTLD Registry Operator. In this specific case, the Central Gateway Manager MUST provide the response of the Registrar of Record to the gTLD Registry Operator as well as identify the jurisdictional issues that resulted in submitting this request to the gTLD Registry Operator. This is unclear. The implication here is that one party is legally not permitted to disclose, but the registry may not be so directly encumbered. This is the very embodiment of forum shopping, and ignores the rights of the data subject, bypassing them in favour of the requester. Should the primary disclosing party be legally prevented from disclosure, the SSAD should not be facilitating the circumvention of any such restrictions.		
10. BC/IPC	Original comment: NCSG Rec #5, paragraph 4, 3rd bullet:	This bullet should be removed altogether.	Change applied as a result of changes made in response to previous comment.

	"If there are jurisdictional issues that would justify consideration of the request by the gTLD Registry Operator. In this specific case, the Central Gateway Manager MUST provide the response of the Registrar of Record to the gTLD Registry Operator as well as identify the jurisdictional issues that resulted in submitting this request to the gTLD Registry Operator." If jurisdictional issues exist for the Registrar, which is the Data Controller with which the Registrant/Data Subject interacts and holds a contract with, then whatever legal restrictions preventing disclosure of the data by the Registrar should not be circumvented by seeking disclosure via the applicable Registry. This could result in infringement on the rights of the Registrant, as well as create legal liability issues for the Registrar, and other Data Controllers with which the Registrar has signed a Data Processing Agreement.		**Flagged for discussion**: IPC/BC: We agreed that a requestor could elect to direct a request to the Registry Operator, at the requestor's option. Revert to original language. *Discussed during 16/6 meeting: Leave as is.*

"If a requestor is of the view that its request was denied erroneously, a complaint MAY be filed with ICANN Compliance.

[…]

ICANN Compliance MUST make available an alert mechanism by which requestors as well as data subjects whose data has been disclosed can alert ICANN Compliance if they are of the view that disclosure or non-disclosure is the result of systemic abuse by a Contracted Party. This alert

mechanism is not an appeal mechanism – to contest disclosure or non-disclosure affected parties are expected to use available dispute resolution mechanisms such as courts or Data Protection Authorities – but it should help inform ICANN Compliance of potential systemic abuse which should trigger appropriate action. **Information resulting from the alert mechanism is also expected to be included in the SSAD Implementation Status Report (see recommendation #19) to allow for further consideration of potential remedies to address abusive behavior**.

11. BC	Original comment: RySG Rec #8	Delete: Information resulting from the alert mechanism is also expected to be included in the SSAD Implementation Status Report (see recommendation #19) to allow for further consideration of potential remedies to address abusive behavior.	RySG to explain why text should be deleted. **Flagged for discussion**: BC: Do not delete the verbiage RySG: Consideration of potential remedies to address abusive behavior is not currently contemplated as in scope for the evolutionary mechanism described in Rec #19. The contents of the implementation status report and the scope of the evolutionary mechanism should be described ONLY in Rec #19 to avoid confusion.
12. BC/IPC	Original comment: ICANN org Rec #8, "If a requestor is of the view that its request was denied erroneously, a complaint MAY be filed with ICANN Compliance." Can the team please clarify what is meant by "denied erroneously?" ICANN org interprets this to mean, ""was denied in violation of the procedural requirements of this		Change applied. **Flagged for discussion:** BC/IPC No, requestors cannot be limited to reporting only procedural violations. Substantive complaints must also be permitted. *Staff support team note: the language does not limit the ability of requestors to submit complaints but as outlined in footnote 29: ICANN org would review compliance with the following: a) response adhered to established SLAs; b) response included all required content (i.e. denial communicated without disclosure of personal data, rationale for*

	policy." Is this accurate? If yes, suggest editing the language.		*the decision, and (if applicable) how the Contracted Party applied the balancing test); c) request was reviewed based on its individual merits; and, d) absent any legal requirements to the contrary, disclosure was not refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; or solely based on the fact that the request is founded on alleged intellectual property infringement in content on a website associated with the domain name (absent any legal requirements to the contrary). 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.*

Recommendation #NEW – Priority Levels
(…)
Implementation Guidance

Examples of circumstances in which an Urgent SSAD request may be warranted include, but are not limited to:

- Imminent threat to life: [To be completed]
- Serious bodily injury: [To be completed]
- Critical infrastructure (online and offline): [To be completed]
- Child exploitation: [To be completed]

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
13. RySG	Urgent • Imminent threat to life:	Address the to be completed language	GAC Team to provide examples as previously agreed

	[To be completed] • Serious bodily injury: [To be completed] • Critical infrastructure (online and offline): [To be completed] Child exploitation: [To be completed]		
14. GAC		Per the ongoing Action Item regarding examples of SSAD urgent requests, after review of the revised text of Rec. 8 and the new recommendation on Urgent SSAD Disclosure Requests • GAC Reps believe there is no need to further illustrate the categories listed, be it "imminent threat to life", "serious bodily injury" and "child exploitation". For reference, the Framework for Registry Operator to Respond to Security Threats refers to these as such: *Initial judgment of a request being "High Priority" should be self-evident and require no unique skills in order to determine a public safety nexus. "High Priority" should be considered an imminent threat to human life, critical infrastructure or child exploitation.*	Is there any concern about the GAC proposed approach (not to provide any examples but consider including a reference to the Framework for Registry Operator to respond to security threats? Is there any concern about adding the following definition for critical infrastructure: "Critical infrastructure means the physical and cyber systems that are vital that their incapacity or destruction would have a major detrimental impact on the physical or economic security or public health or safety."

		• Regarding "Critical Infrastructure", they believe it should be understood as discussed by the GAC reps in the Phase 1 IRT to be along the lines of generally accept definition: Critical infrastructure means the physical and cyber systems that are vital that their incapacity or destruction would have a major detrimental impact on the physical or economic security or public health or safety.	
15. RySG	Urgent (Recommendation NEW) c) 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	Remove "or in another standardized place that may be designated by ICANN from time to time."	Note, this language has been there from the Initial Report to provide flexibility in case the SSAD would not allow for storing of this information. RySG to provide further details on why this is now a 'cannot live with item'. **Input provided:** RySG: The point of the recommendation is to mandate CPs provide urgent contact info, business hours and time zone to the SSAD… not "another standardized place that may be designated by ICANN from time to time". That language is way to open ended, which could allow for ICANN org to insist that info be published on company home pages as recently happened in the phase 1 IRT. Remove "or in another standardized place that may be designated by ICANN from time to time.

	hours and accompanying time zone in the SSAD portal (or in another standardized place that may be designated by ICANN from time to time). Remove or in another standardized place that may be designated by ICANN from time to time.		

"The Contracted Party:

- MAY reassign the priority level during the review of the request. For example, as a request is manually reviewed, the Contracted Party MAY note that although the priority is set as priority 2 (ICANN Administrative Proceeding), the request shows no evidence documenting an ICANN Administrative Proceeding such as a filed UDRP case, and accordingly, the request should be recategorized as Priority 3."

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
16. ICANN org	ICANN org notes that this paragraph adds complexity to both contracted parties' and the Central Gateway's systems and may be challenging to implement. Would the EPDP team consider instead that a request that does not meet the requirements for Priority 1 or 2 may be rejected and may be refiled? In addition, should the recommendation remain as is written, ICANN org suggests	"MAY reassign the priority level during the review of the request, in accordance with the requirements above."	

	a minor edit for clarification during implementation.		

- Priority 2 - ICANN Administrative Proceedings – disclosure requests that are the result of administrative proceedings under ICANN's contractual requirements or existing Consensus Policies, such as UDRP and URS verification requests.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
17. ICANN org	In Rec #NEW, Priority 2, can the EPDP team please clarify if this priority is intended to be available only to ICANN-approved dispute resolution service providers, or should it also be available to parties and potential parties in administrative proceedings?		

For Priority 3 requests, requestors MUST have the ability to indicate that the disclosure request concerns a consumer protection issue (phishing, malware or fraud), in which case the Contracted Party MAY prioritize the request over other Priority 3 requests. Persistent abuse of this indication can result in the requestor's de-accreditation.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
18. ICANN org	In Rec #NEW, Priority 3 seems to contemplate a bifurcation within this priority level resulting in 4 priority levels. For implementation purposes, the system would require a fourth category, even if the contracted party were to choose to treat the two priority levels the same. Would it make more sense to create a fourth priority level to allow for this?		

a. Abuse of urgent requests: Violations of the use of Urgent SSAD Requests will result in a response from the Central Gateway Manager to ensure that the requirements for Urgent SSAD Requests are known and met in the first instance, but repeated violations may result in the Central Gateway Manager suspending the ability to make urgent requests via the SSAD.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
19. ICANN org	In Rec #NEW, a. Abuse of urgent requests: For clarity during implementation, does the EPDP team contemplate any recommendations regarding abuse of the use of other priority levels? For example, what if a requester regularly incorrectly cites Priority 2, and those requests are downgraded. Would that be considered abuse?		

Recommendation #4 – Requestor Purposes

(iii) consumer protection, abuse prevention, digital service provision and network security. Requestors MAY also submit data disclosure requests on the basis of Registered name holder (RNH) consent that has been obtained by the requestor, for example to validate the RNH's claim of ownership of a domain name registration, or contract with the requestor.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
20. IPC / RySG	Original comment: RySG "Digital service provider (DSP)" isn't a purpose, it seems to be a type of requestor?	Either delete "Digital service provider (DSP)" or clarify what the intended purpose is.	Change applied – changed 'digital service provider' to 'digital service provision'. **Flagged for discussion**: IPC: 4. Fine to correct for sentence syntax, but DSP is a term of art (i.e. under NIS EU law)

			and needs to stay. "obligations applicable to digital service providers (DSP)" RySG: still not sure what this means. What is a "digital service provision" requestor purpose?

Recommendation #6 – CP Authorization

a) MUST disclose the data if, following the evaluation of the underlying data, the Contracted Party determines disclosing the requested data elements would not result in the disclosure of personal data, unless the disclosure is expressly prohibited under applicable law.[2] If the disclosure would not result in the disclosure of personal data, the Contracted Party does not have to further evaluate the request under paragraph 9.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
21. ALAC	Unclear that the reference to Paragraph 9 is appropriate. If there is no personal data involved (and not otherwise prohibited by law), the requested data must be disclosed		*Note, no update was made to this paragraph in response to input provided, the only change was made in response to input from BC/IPC/ALAC was to move this paragraph up as #1.*
22. RySG	Original comment: BC/IPC/ALAC 7: The first determination in the balancing test should be whether the contact data contains personal data.	Move 7 to #1	Change applied **Flagged for discussion**: RySG: Changing the order of the steps taken to make a determination on if to disclose the data is in this case substantive

[2] When considering the publication of non-public data of legal persons, particularly with respect to NGOs and parties engaged in human rights activities that may be protected by local law (e.g. Constitutional and Charter Rights law), the Contracted Party should consider the impact on individuals that could potentially be identified by disclosing the legal person data.

			and materially changes the recommendation. Revert to previous text

5(a) MUST make a threshold determination ~~without reviewing the underlying data~~ about whether the requestor has established a prima facie valid request for the disclosure of personal data. In other words, would the Contracted Party have a lawful basis for disclosure and are all the data elements necessary. The determination SHOULD consider these factors: (…)

7. For disclosure requests that are not subject to the automated processing of the disclosure decision, MUST evaluate the ~~underlying data~~ request once the validity of the request is determined under paragraph 5a.

23. RySG	Original comment: BC/ALAC In 4(a): unclear why "without reviewing the underlying data" is required;	Delete "without reviewing the underlying data"	Change applied – up to the CP to determine whether or not it can make such a threshold decision with or without reviewing the underlying data. NOTE: As underlying data was removed from 4(a), it was also removed from paragraph 7. Flagged for discussion: RySG: This change defeats the purpose of a threshold determination. Further, the now modified paragraph 7 doesn't make sense anymore. Change back to previous text.
24. ICANN org			Can the EPDP team please explain what is the purpose of making a threshold determination? The paragraph used to require a Contracted Party to "make a threshold determination without

			reviewing the underlying data." Paragraph 5a) no longer includes this language. Further, Paragraph 7 no longer indicates whether the registration data ought to be evaluated together with the request, rather it only requires the Contracted Party to "evaluate the request." It is unclear how Paragraphs 5a) and 7 are distinct. Can the EPDP team please clarify? Paragraph 7: ICANN org notes that there do not appear to be any mandatory requirements specifying what it means to "evaluate the request." Accordingly ICANN Contractual Compliance would only be able to assess whether the CP has conducted "an evaluation". Can the EPDP team please confirm there are no mandatory requirements specified for this evaluation?

(….)
5(b) If the Contracted Party has established that it lacks a lawful basis to process the data or the Contracted Party does not believe a requested data element(s) is necessary for the requestor's stated purpose, **the Contracted Party MUST allow the requestor to provide further information prior to denying the request**.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
25. ICANN org	Is this notification or opportunity to provide more information on the request also applicable following the evaluation referenced in paragraph 6, should the		EPDP Team to confirm whether 5b ("the CP MUST allow the requestor to provided further information prior to denying the request" is still accurate or whether a requestor can provide additional

	Contracted Party determine that it is likely to deny the request?		information on these as part of reexamination. For clarity, a CP can at any point request a requestor for further information to help inform its evaluation of its request.

26. RrSG / RySG	Original comment: ICANN org 4.b) "(b) If the request lacks a lawful basis to process the data or the Contracted Party does not believe a requested data element(s) is necessary for the requestor's stated purpose, the Contracted Party MUST allow the requestor to provide further information prior to denying the request." Can the EPDP team please clarify what it means by "If the request lacks a lawful basis?" Can the EPDP explain if this means that the requestor did not specify a lawful basis for its request? Or that the Contracted Party does not judge the lawful basis to be appropriate? Further, it is unclear how this comports with paragraph 3 above, which notes the Contracted Party MUST determine a legal basis? In addition, this paragraph implies that the Contracted Party or the Central Gateway Manager must notify the requestor of its intent to deny the request. Is this a correct understanding?		Change applied to clarify that it is the staff support team's understanding that this refers to the CP not having identified a lawful basis under which it (the CP) can process the data. If this is an incorrect understanding, EPDP Team to indicate this **Flagged for discussion**: RrSG: Not accurate (MUST Is problematic) RySG: As a point of clarification - any material change to a request must also be assessed. The emphasis MUST be on a properly created, and carefully crafted and individualized request, that is intended to be a full request upon 1st submission. The change of a claimed legal basis is considered material. These requests must be careful and considered, and barring genuine error or mistake, the lack of care in making a request, as demonstrated by misapplying legal basis or other vital elements, then a subsequent change of such a request to "better suit disclosure", must be a consideration in the decision.

	Must the Contracted Party also document its rationale in this instance?		Privacy rights are not simply something to be negotiated and horse traded in the back and forth between a disclosing party and a requestor. A requester should of course be allowed to modify a request, but the conduct of the requester in doing so is a factor that must be considered in the decision to disclose or not. We further caution that at some point a "No" must be a "No". This supports the fact that multiple material changes in a request to 'achieve; disclosure, builds up a stronger likelihood of denial.

6. (…) nor can the disposition of a request be solely based on the fact that the request is founded on alleged intellectual property infringement in content on a website associated with the domain name. (…)

27. BC / IPC	Original comment: IPC 5. "the disposition of a request" conflicts with our agreement in L.A. that requests could not be denied solely because they relate to IP on a website, and it also conflicts with the Rec 16 ability for CPs to automate if they wish to do so	Change back to "requests cannot be denied solely" Improve clarity, "Contracted Parties MUST NOT deny requests solely…"	No change made – the updated language was the result of a lengthy discussion within the EPDP Team and has not changed the intent of the agreement in LA. **Flagged for discussion**: BC/IPC: Cannot live with this. This significantly changes the intent of our agreement in LA, and it also conflicts with Rec 7 which allows CPs to automated (voluntarily) specific types of requests. We did not and do not agree to change the language we agreed on in LA. This language mirrors an identical requirement in the Privacy/Proxy

			policy. To be clearer, this should be a standalone statement.

28. BC	Original comment: RySG Consideration will need to be given by all parties involved in SSAD to the requirements that may apply to cross-border data transfers. Moved from Rec #3	Add a new subsection to #8 second bullet: Consideration needs to be given to the requirements that may apply to cross-border data transfers	RySG to clarify what is meant with 'second bullet' – this sentence has currently been added to the implementation guidance section. **Flagged for discussion**: BC: This new language has significant potential policy impact to multiple Recommendations and should not be accepted as a Minor Edit without discussion. *Staff Support team note: the original edit (adding reference to cross-border data transfers) was agreed during meeting #58 on 19 May.*

(…)

9. **If the request is subject to meaningful review**, MUST disclose the data if, based on its evaluation, 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 Contracted Party MUST document the rationale for its approval.** If the request is not subject to meaningful review, MUST disclose if the Contracted Party determines it has a lawful basis to disclose the data.

10. **If the request is subject to meaningful review**, SHOULD deny the request, 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 Contracted Party MUST document the rationale for its denial and MUST communicate the rationale to the Central Gateway Manager, with care taken to ensure no personal data is revealed in the rationale explanation. If the request is not subject to meaningful review, MUST deny the request if the Contracted Party determines it does not have a lawful basis to disclose the data.

(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
29. ICANN org	Further, does the second sentence of the paragraph imply that the Contracted Party must only document its rationale for approval only in this circumstance or in every circumstance for which it approves a request? In addition, ICANN org suggests the Contracted Party share its rationale for approval with the Central Gateway Manager, so that it may learn which requests are approved, should the Contracted Party's decision conflict with a possible Central Gateway recommendation.		EPDP Team to confirm whether a CP must only document its rationale for approval only if meaningful review is required or in every circumstance for which it approves a request. Are there any concerns about requiring CPs to share its rationale for approval with the CGM so that it may learn which requests are approved, should the CPs decision conflict with a possible CGM recommendation. Input received: • RrSG: Agree only for meaningful review. Concern with implementing sharing of rationale.
30. RySG	Imbalance between section 9 and 10 Section 9 ia a MUST but section 10 is a SHOULD creating an imbalance in favor of the requestor, at the expense of the Data Subject, that seems hard to justify. They should either both be SHOULD or MUST.	Change the first MUST in section 9 to SHOULD. -alternative- Change the first SHOULD in section 10 to MUST	No change applied - note that the change in 10 was made by the EPDP Team in response to public comment (See Question 17 in the discussion issues list.) **Flagged for discussion**: RySG: Whereas we appreciate that a discussion ensued post a public comment, this should not preclude revisiting such a matter, when the discussed changes are presented in the clean document, and an issue that was not apparent at the time becomes clear. The team, when considering the data privacy rights of registrants, should not knowingly present an imbalance in the language that favours

			unconnected 3rd parties. The RYSG is merely pointing out this inconsistency as one that should be rectified to ensure that the policy is focused on vindicating all rights and not favouring those of the 3rd party requester. Either there are 2 MUSTS in 9/10 (now 10/11) or 2 SHOULDS - not one of either.
31. RySG	Original comment: IPC/BC 9. "evaluation," implies that each request will be 6.1.f	"If the request is subject to a balancing test, MUST…"	Change applied – note that 'balancing test' has been changed to 'meaningful review' as that is the language that the EPDP Team has used in other recommendations. Note – text also added to paragraphs 9 and 10 for disclosure decisions that do not relate to 6(1)(f) as it seemed this situation was not covered under the current language; however, please review to ensure Support Staff's understanding is correct. **Flagged for discussion:** RySG: These changes don't make sense in the overall context of Rec 6 Revert to previous text ICANN org: Paragraph 9: Can the EPDP team please define "meaningful review" and clarify how a Contracted Party is to determine whether a request is subject to "meaningful review?"

			Further, the sentence: "If the request is not subject to meaningful review, MUST disclose if the Contracted Party determines it has a lawful basis to disclose the data." seems to be based on the idea that every request requires a lawful basis. That is a GDPR concept that will not apply in every instance. ICANN org proposes revising the language to ensure the policy is globally applicable.
32. RySG	Original comment: IPC/BC 10. also implies that each request will be 6.1.f	"If the request is subject to a balancing test, SHOULD…"	Change applied – note that 'balancing test' has been changed to 'meaningful review' as that is the language that the EPDP Team has used in other recommendations. Note – text also added to paragraphs 9 and 10 for disclosure decisions that do not relate to 6(1)(f) as it seemed this situation was not covered under the current language; however, please review to ensure Support Staff's understanding is correct. **Flagged for discussion:** RySG: These changes don't make sense in the overall context of Rec 6 Revert to previous text ICANN Org: Paragraph 10: Can the EPDP team please explain why the policy should permit registrars to approve disclosure

			requests if the registrar determines that the data subject's interests or fundamental rights and freedoms outweigh the interests of the requestor? Such a disclosure arguably would violate the GDPR and therefore this may raise issues in implementation.

(…)
8. SHOULD[3], in its evaluation, assess at least:
(…)

33. RySG	Consideration will need to be given by all parties involved in SSAD to the requirements that may apply to cross-border data transfers. Moved from Rec #3	Add a new subsection to #8 second bullet: Consideration needs to be given to the requirements that may apply to cross-border data transfers	RySG to clarify what is meant with 'second bullet' – this sentence has currently been added to the implementation guidance section. **Input provided:** RySG: move to section 8 - create a new viii) IPC: Should this be tackled with the SSAD acceptable use policy/terms?

Footnote 38**:** ICANN org would review compliance with the following: a) response adhered to established SLAs; b) response included all required content (i.e. denial communicated without disclosure of personal data, rationale for the decision, **and (if applicable) how the Contracted Party applied the balancing test**); c) request was reviewed based on its individual merits; and, d) absent any legal requirements to the contrary, disclosure was not refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; or solely based on the fact that the request is founded on alleged intellectual property infringement in content on a website

[3] ICANN org would review compliance with the following: a) response adhered to established SLAs; b) response included all required content (i.e. denial communicated without disclosure of personal data, rationale for the decision, and (if applicable) how the Contracted Party applied the balancing test); c) request was reviewed based on its individual merits; and, d) absent any legal requirements to the contrary, disclosure was not refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; or (iv) a UDRP or URS proceeding; or solely based on the fact that the request is founded on alleged intellectual property infringement in content on a website associated with the domain name (absent any legal requirements to the contrary). 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.

associated with the domain name (absent any legal requirements to the contrary). 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.

34. RySG	Original comment: ICANN Org 8. ICANN org notes the use of the word "SHOULD" as opposed to "MUST" in this recommendation. To be clear, as noted in Rec #8 footnote 9, ICANN Contractual Compliance will not be able to enforce anything in this paragraph. For clarity in implementation, the EPDP team may consider adding that footnote to this paragraph.		Change applied – footnote added **Flagged for discussion:** RySG: We support the effort to provide additional clarity regarding the enforcement role for ICANN Compliance. However, "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" seems to conflict with the language earlier in the footnote stating that Compliance would review "how the Contracted Party applied the balancing test." Remove the language regarding Contracted Party application of the balancing test from the footnote.

Recommendation #16/7 Automation

The SSAD MUST allow for the automated disclosure of data in response to well-formed, valid, complete, properly identified requests from accredited users as described in Recommendation #7.

Deleted: automation of the processing of

Deleted: ¶

35. RySG	Original comment: IPC/BC/ALAC "The SSAD MUST allow for automation of the processing"	The SSAD MUST allow for the automated disclosure of data in response to…"	Change applied **Flagged for discussion:**

			RySG: "automation of the processing" seems appropriately broader than "automated disclosure of data" in the revised version. The latter risks confusion for implementers about what is an isn't the actual "disclosure" the data (e.g., is this only referring to the functional step where the CP discloses to the CGM? Where the CGM discloses to the requestor? Using "processing" captures the entirety of the processing involved with a disclosure request. "The SSAD MUST allow for automation of the processing"

Automated processing of disclosure decisions

Contracted Parties MUST automatically process disclosure decisions for any categories of requests for which automation is determined (pursuant to the implementation guidance below and the processes detailed in recommendation #19) to be technically and commercially feasible[4] and legally permissible.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
36. RrSG / RySG	Several changes below to the text of Rec 7/16 have led to text that is not acceptable. Specifically the language: 'Contracted Parties MUST automatically process disclosure decisions for any categories of requests for which	Instead of the quoted text shown here, say "Where a Contracted Party has determined it is technically and commercially feasible and legally permissible to do so, they MUST	

[4] 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 evolution of SSAD, as applicable.

	automation is determined (pursuant to the implementation guidance below and the processes detailed in recommendation #19) to be technically and commercially feasible1 and legally permissible'	automatically process disclosure decisions…"	
1. NCSG	Rec#7, paragraph 1: "The EPDP team recommends that disclosure decisions MUST SHOULD be automated where technically and commercially feasible and legally permissible." The "MUST" in this recommendation should be changed back to "SHOULD", and should apply to disclosure requests, which may meet the threshold for automated decisions to disclose registration data. This should be left to the discretion of the applicable Contracted Party, and take into account the reasonable expectations of the Registrant/Data Subject on how his/her registration data will be processed, and at a minimum, give the Registrant the right to object to automated decisions to disclose his/her registration data. • The same objection applies to the implementation guidance on this recommendation.	The EPDP team recommends that disclosure decisions SHOULD be automated where technically and commercially feasible and legally permissible.	No change applied – a number of safeguards have been put in place to ensure that automation only happens when legally permissible. In addition, CPs can notify ICANN Compliance (and stop automated processing) if a risk that was not previously recognized, is identified through a DPIA. Note, the implementation guidance section has been updated per comment #9. **Flagged for discussion:** NCSG - The measures/safeguards taken to address the NCSG concern in #12 are not sufficient, nor is the step of a Contracted Party flagging a possible issue of potential conflict with law to ICANN Compliance. Registrars will always be Controllers, and likely the ones that need to be most accountable to the Data Subject/Registrants. If a decision is made to fully automate a disclosure request with the CGM, this decision should remain with the Registrar (not the Registry Operator). Currently, the recommendation still reads: *"The EPDP team recommends that disclosure decisions **MUST** be automated*

			where technically and commercially feasible and legally permissible." Changing MUST to SHOULD here would address the NCSG's concern, and keep the decision to automate disclosure requests with the Registrar. Registrars may also provide rationale on why they've refused to automate a disclosure request on a category of use cases that have been found to be legally permissible. Proposed updated text: "The EPDP team recommends that disclosure decisions SHOULD be automated where technically and commercially feasible and legally permissible." Possible Implementation Guidance: The determination of how legally permissible automation of decisions to disclose registration data in a certain category of use cases should ultimately remain with the Registrar.

Footnote 43:
For clarity, if a Contracted Party demonstrates that automated processing of disclosure decisions for the use cases specified in this recommendation or through the processes detailed in Recommendation #19 is not legally permissible or brings with it a significant risk that was not recognized in the legal guidance obtained by the EPDP Team but has been subsequently identified through a Data Protection Impact Assessment (DPIA), the Contracted Party can notify ICANN Compliance of an exemption from automated processing of disclosure decisions of a specific use case. As soon ICANN compliance has been notified, automated processing of disclosure decisions for the use cases specified by the

Deleted: request

Deleted: by petitioning ICANN Compliance

Deleted: for

Contracted Party making the submission will be halted, and the Contracted Party MUST review the requests further to the requirements in Recommendation 6. Unreasonable exemption notifications MAY be subject to review by ICANN Compliance.

Per the legal guidance obtained (see here), the EPDP Team recommends that the following types of disclosure requests are legally permissible under GDPR for full automation (in-take as well as processing of disclosure decision) from the start:

Deleted: at least the following types of disclosure requests MUST be fully automated (

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
37. BC	The changes to #5, #9, and #10 potentially put the entire system of MfE at risk. All of the concerns expressed here should be discussed within the MfE Recommendation 19.	Revert to previous verbiage.	Consider proposal to revert to previous verbiage
38. RySG	5) The RYSG agrees with the RRSG. Please note that the WHOIS Conflicts procedure itself pre dated the GDPR, and probably would not have survived DPA review (pre or post GDPR) therefore is not a solid comparator . e.g. For all those parties who demonstrated that an exemption was necessary to not breach the law, and yet somehow that provision continued to apply to all those other parties, who had to, in turn', 'prove' that the law (in this instance Data Protection Directives 1995 & 2003) also applied to them, was always legally dubious. No party should have been compelled by ICANN to breach the law. Once ICANN becomes aware of such an incompatibility, this should trigger a full review, and not continue to expect parties to 'ask for permission' to not break that	Change footnote For clarity, if a Contracted Party determines that automated processing of disclosure decisions for the use cases specified in this recommendation or through the processes detailed in Recommendation #19 is not legally permissible or brings with it a significant risk ~~that was not recognized in the legal guidance obtained by the EPDP Team but has been subsequently identified through a Data Protection Impact Assessment (DPIA)~~, the Contracted Party MAY cease automated processing of disclosure decisions. To:	Consider proposed change

	law, but continue doing so until the 'request' was 'granted'. The EPDP team should not try to model our policy recommendations on a procedure that expected the blind enforcement of contractual obligations in the face of actual notice of illegality of that provision. In this instance, whereas ICANN may, of course, require explanation from any CP who believes that they had no choice but to cease adherence to a contractual provision for legal incompatibilities, we should however be clear that there be no expectation that such a party continue to willfully ignore their legal obligations. ICANN, retains no legal standing or authority to overturn or interpret such laws. The bias in this process should rest with adhering to legislative obligations over contractual. Should the relevant CP, who has ceased to follow such contractual obligations citing legal incompatibility, be proven incorrect in their assertion, then, ICANN may consider it's options for contractual enforcement and censure. The language in the footnote says "demonstrates" which implies some sort of burden of proof for Contracted	The Contracted Party MUST notify ICANN Compliance once it ceases automated processing of any disclosure decision. The Contracted Party MUST then review those disclosure decisions further to the requirements in Recommendation 6. Unreasonable exemption notifications MAY be subject to review by ICANN Compliance.	

	Parties. That should instead say "determines" for the reasons stated above. We should consider how the CGM is appropriately notified as well that automation has been stopped.		
39. ICANN org	Footnote 43 seems to contemplate exemptions to the requirements of this recommendation. For clarity in implementation, ICANN org suggests incorporating the proposed language into the recommendation.		Can the EPDP team please clarify how this language is intended to be implemented? How does the EPDP Team contemplate ICANN Compliance may be involved in this process? Would Compliance be able to overrule the Contracted Party's request? The footnote indicates that ICANN Contractual Compliance may review these "unreasonable exemptions." Who determines whether an exemption is unreasonable? What would ICANN Contractual Compliance be empowered to review? Would ICANN Contractual Compliance be empowered to challenge a Contracted Party's request? Further, the footnote notes that the Contracted Party "demonstrates that automated processing… is not legally permissible." How would a Contracted Party demonstrate this? To who? Would it be considered legally impermissible only in their jurisdiction or globally? What does it mean for that processing to "bring with it a significant risk?" Is it only possible to identify these concerns via a DPIA? The footnote also indicates that upon the

			Contracted Party's request, the automation must be halted. Is it the Central Gateway that would take that action?

(…)
Similarly, the Central Gateway MAY request the Contracted Party for further information that may help the Central Gateway Manager in determining whether or not the criteria for an automated processing of disclosure decisions have been met. A Contracted Party MAY provide such further information, if requested.
(…)

Group	**Text & Rationale**	**Proposed updated text**	**For EPDP Team Consideration**
40. RySG	4) If the CGM needs to requests additional information from the Contracted Party about the registrant in order to determine whether a request is automatable then either (1) the requestor has not provided sufficient information and it should be sent back to the requestor; or (2) the request isn't automatable and should be forwarded to the CP. We should avoid adding additional processing of registrant data (data minimization) in order to respond to requests from third-parties.	Delete addition	Consider proposed deletion

(…)
Requests from Law Enforcement in local or otherwise applicable jurisdictions with a confirmed 6(1)e lawful basis or processing is to be carried out under an Article 2 exemption;
(…)

41. RySG	Original comment: GAC Requests from Law Enforcement in local or otherwise applicable jurisdictions with a confirmed 6(1)e lawful basis;	Requests from Law Enforcement in local or otherwise applicable jurisdictions with a confirmed 6(1)e lawful basis or processing is to be carried out under an Article 2 exemption;	Change applied **Flagged for discussion**: RySG - Request further explanation from GAC on the applicability of Article 2 exemptions in this context. We don't recall discussing this as a plenary.

Recommendation #9 SLAs

See draft Final Report language

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
42. IPC/BC	Priority Matrix should not be *entirely* Implementation Guidance.	The EPDP Team recommends that the SLAs established in the Priority Matrix MUST be applicable during Phase 1 and thereafter MAY be adjusted according to the Mechanism described in Recommendation 19.	Does the EPDP Team agree with this? If so, Staff Support needs further guidance as to which specific text belongs in the policy recommendation. Our previous understanding was the EPDP Team did not wish to include specific numbers in the text of the policy recommendation. **Input received:** • RrSG - agree

The EPDP Team recommends that Contracted Parties MUST abide by Service Level Agreements (SLAs) that are developed, implemented, and enforced, and as updated from time to time per Recommendation #19, in accordance with the implementation guidance provided below.
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
43. ICANN org	Original comment: ICANN org	If the team intends for the SLAs to be binding, ICANN org suggests the	Change applied as proposed

	"The EPDP Team recommends that Service Level Agreements (SLAs) are developed, implemented, and enforced in accordance with the implementation guidance provided below. " Can the EPDP team please clarify how SLAs are meant to be binding, whether as policy requirements outlined in this recommendation or does the team expect that SLAs will be entered into as contract amendments to be negotiated with the Contracted Parties? Further, the policy seems to recommend it be implemented "in accordance with" the guidance below. Can the EPDP team clarify what that means? Does that mean the guidance should be considered policy recommendations? Or should the guidance be used to develop the SLAs during implementation?	following language: "The EPDP Team recommends that Contracted Parties MUST abide by Service Level Agreements (SLAs) as developed, implemented, and enforced, and as updated from time to time per recommendation 19."	**Flagged for discussion:** ICANN org - Can the EPDP team please clarify who they intend to have the final say on the specifics of the Service Level Agreements? Are they being determined as a matter of policy here in Rec #9? Or will it be an implementation matter to be determined by the IRT and ICANN org? Or will this be determined in contractual negotiations between ICANN org and the Contracted Parties? Further, can the team please clarify what "in accordance with" means? Does that mean it must be in exact accordance with the Implementation Guidance or does it mean that the SLAs would be along the lines of the Implementation Guidance?

Request Type	Priority	Proposed SLA[5] (for discussion) / Compliance at 6 months / 12 months / 18 months
Urgent Requests	1	1 business day/ 85% / 90% / 95%
ICANN Administrative proceedings	2	Max. 2 business days / 85% / 90% / 95%
All other requests*	3	See below

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration

[5] Note, the business days referenced in the table are from the moment of Contracted Party receipt of the disclosure request from the Central Gateway Manager.

44. ICANN org	Priority Matrix, " Proposed SLA (for discussion) / Compliance at 6 months / 12 months / 18 months" Can the EPDP team please confirm whether the SLAs described in this table will be the required SLAs or if these are still subject to discussion during the implementation phase, as indicated in the heading noted here?		EPDP to provide further guidance / confirm if below understanding is correct. The Team agreed to the SLAs defined in the table, and these times are not subject to further discussion in implementation. Because of the uncertainty of how many requests the SSAD would receive, the Team provided guidance as to how Priority 3 SLAs should be enforced in the first year of SSAD operations. EPDP Team to confirm if the Phase 1 and Phase 2 approach do not apply to Priority 1 and Priority 2 requests, and also if the percentages still apply, or if this is a holdover from a previous version of the recommendation.
45. ICANN org	Priority Matrix: "24 hours 1 business day / 85% / 90% / 95%" Could the EPDP team please clarify to what these percentages refer? Does it mean that the Contracted Party would meet the 24 hour target for responding to 85% of its requests within the first 6 months of the policy taking effect, while it would be acceptable for 15% to take much longer?		EPDP Team to clarify. **Input received**: • RrSG – Agree with understanding

46. ICANN org	Priority Matrix: Max. 2 business days / 85% / 90% / 95% Can the EPDP team please confirm that as it has defined business days to be those of the Contracted Party, how would the team define business days? For example, some Contracted Parties may have longer holiday periods than others, limiting their business schedule.		EPDP to confirm it meant business days as defined in CP's jurisdiction. **Input received**: • RrSG – Agree with understanding
47. ICANN org	Original comment: RrSG 24-hour response time for Urgent requests should instead be 1 Business Day Urgent request SLA - change 24 hours back to 1 business day		Change applied **Flagged for discussion:** ICANN org notes the complexity of determining, defining and tracking business days in a global setting. Both the RAA and the RA reference calendar days and not business days, given the complexity in calculating business days.

A reexamination request or a requestor response with more information would be considered the start of a new request for SLA calculation purposes.
(…)
The impact on the SLA regarding any back-and-forth between the requestor and Contracted Party should be further considered in implementation, taking into consideration best practices from ICANN policies or other relevant industries.
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
48. RySG	new text: "The impact on the SLA regarding any back-and-forth between the requestor and Contracted Party should be further considered	Delete	**Flagged for discussion**:

	in implementation, taking into consideration best practices from ICANN policies or other relevant industries."		Unsure where this new text came from, but it seems to be redundant with the new 2nd paragraph in Rec #9. *Staff support team note: This was originally added in response to a comment on rec 3-5-8 but it does indeed seem duplicative with paragraph 2 language.*

(…)
Contracted Party response time requirements for SSAD requests will occur over two phases:

- Phase 1 begins **six (6) months** following the SSAD Policy Effective Date.
- Phase 2 begins **one (1) year** following the SSAD Policy Effective Date.

(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
49. ICANN org	"Phase 1 begins six (6) months following the SSAD Policy Effective Date. Phase 2 begins one (1) year following the SSAD Policy Effective Date." Can the EPDP team please clarify that Phase 1 and Phase 2 only apply to Priority 3 requests? Priority 1 and 2 requests will have the same SLAs as indicated in the table?		EPDP Team to confirm that Phase 1 and Phase 2 compliance targets only apply to Priority 3 requests. (Similar to Question in 24.) **Input received**: • RrSG – Don't agree

Phase 1
(…)
The Central Gateway Manager MUST measure response targets using a Mean Response Time, not on a per-response basis.
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
50. ICANN org	"The Central Gateway Manager SHALL measure response targets using a Mean Response Time, not on a per-response basis." Could the team explain how the Mean Response Time and Response Target Value correspond to the priority max and the SLAs identified within that table?		EPDP Team to clarify if the Mean Response Times and Response Target Values correspond to Priority 1 and Priority 2 requests. **Input received**: • RrSG – Yes they do correspond

The SSAD MUST also measure the Response Target Value of the ongoing rolling average at the end of the Response Target Evaluation Interval.

Deleted: SHALL

Deleted: sample

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
51. BC	Original comment: ICANN org "The SSAD SHALL also sample the Response Target Value of the ongoing rolling average at the end of the Response Target Evaluation Interval." Can the EPDP team please clarify what it means by "sample"? Did the team mean "measure"?		"Sample" changed to "measure". **Flagged for discussion:** BC: #27: "Sample" would be the mathematical term, but "examine" could be substituted. Response times are "measured"; the mean response time is "computed" every day; on any given day, the current value of the mean response time can be "sampled" or "examined"; when the mean response time value is examined on the closing day of the target evaluation interval, that value is also known as the Response Target Value.

Phase 1
(…)
For the avoidance of doubt, the intent of the SSAD providing the Contracted Party with the Response Target Value is to provide a warning to the Contracted Party that there may be an issue with its response times and to allow the Contracted Party to remedy the issue in a cooperative manner. During Phase 1, if the Contracted Party's Response Target Value exceeds five (5) business days, this MUST NOT result in a policy breach.
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
52. ICANN org	"For the avoidance of doubt, the intent of the SSAD providing the Contracted Party with the Response Target Value is to provide a warning to the Contracted Party that there may be an issue with its response times and to allow the Contracted Party to remedy the issue in a cooperative manner." Can the EPDP team clarify whether "Response Target Value" ought to reference "Mean Response Time?"		EPDP Team to clarify whether "Response Target Value" ought to reference "Mean Response Time". **Input received**: • RrSG – Agree to change

Phase 1
(…)
The Contracted Party MUST respond to the ICANN's response target failure notice within five (5) business days.
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
53. ICANN org	"The Contracted Party MUST respond to the ICANN's response target failure notice within five (5) business days."		EPDP team to clarify to whose business days this requirement is referencing. **Input received**: • RrSG – CP business day

	Can the EPDP team please clarify to whose business days this requirement is referencing?		

(…)
How is priority defined?
Priority is a code assigned to requests for disclosure that contain agreed to, best effort target response times.
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
54. ICANN org	Implementation Guidance, questions regarding how priorities are defined		Given the addition of Rec #NEW, would the team consider moving this guidance either to Rec #NEW or deleting entirely if it is now duplicative?

(…)
What happens if priority needs to be shifted?
It is possible that the initially-set priority may need to be reassigned during the review of the request. For example, as a request is manually reviewed, the Contracted Party MAY note that although the priority is set as 2 (UDRP/URS), the request shows no evidence documenting a filed UDRP case, and accordingly, the request should be recategorized as Priority 3. Any recategorization MUST be communicated to the Central Gateway Manager and Requestor. 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 above-defined response times, the Contracted Party MUST respond to the request.
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
55. ICANN org	What happens if priority needs to be shifted?		EPDP Team to confirm if requests are improperly categorized if the CP can reject the request rather than recategorize.

	ICANN org notes that this paragraph add complexity to both contracted parties' and the Central Gateway's systems and may be challenging to implement. Would the EPDP team consider instead that a request that does not meet the requirements for Priority 1 or 2 may be rejected?		**Input received**: • RrSG – Yes (MAY is correct)

Recommendation #10 – 12 – 14 – Terms and Conditions

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
56. RySG	Original comment: BC The SSAD Terms and Conditions may need to be updated as GDPR is interpreted and other privacy laws apply that require compliance.	Add: The SSAD Terms and Conditions may be updated as appropriate through the MFE to address applicable law and practices.	Change applied – note this recommendation would also need to be included in recommendation #19. **Flagged for discussion**: RySG - Unsure if Rec #19 is the right place for these to change, though that comment that they may need to change makes sense. Further discussion? Should ICANN org or the entity operating the SSAD be able to make those updates? Maybe the mechanism in Rec #19 can make suggestions for updates to the operator.

Recommendation #11 – Disclosure Requirements

Contracted Parties and SSAD (…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration

57. ICANN org			Rec #11 indicates that SSAD must comply with the requirements in c, d, e and f. Does the EPDP Team mean that these requirements are expected of the Central Gateway Manager? Can the EPDP team please clarify which requirements apply to the Contracted Parties and which to the Central Gateway Manager, Accreditation Authority, or the Identity Provider?

d. (…) Confidential requests ~~can~~ **MUST NOT** be disclosed to data subjects except ~~in~~ **without** cooperation **from** ~~with~~ the requesting entity, and in accordance with the data subject's rights under applicable law; (…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
58. IPC/BC	i) "Confidential requests can be disclosed to data subjects in cooperation with the requesting **entity** ~~authority~~, ~~[~~and~~]~~ ~~[or]~~ in accordance with the data subject's rights under applicable law." has no normative language.	"Confidential requests MUST NOT be disclosed to data subjects without cooperation from the requesting **entity** ~~authority~~, ~~[~~and~~]~~ ~~[or]~~ in accordance with the data subject's rights under applicable law.	Change applied as proposed Flagged for discussion: RySG - This change materially alters the meaning resulting in cannot live with text. revert to previous text

Contracted Parties and SSAD:
(…)
f. MUST, in a concise, transparent, intelligible and easily accessible form, using clear and plain language, provide notice to data subjects, of the types of entities/third parties which may process their data.[6] (…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration

[6] Implementation guidance: ICANN Org will develop the SSAD Privacy Policy for SSAD users, which it may publish for public comment to obtain input from potential SSAD users.

59. IPC/BC	Footnote 3. Covered by another Rec, and not applicable here.	Strike	Is there any concern from the EPDP Team concerning this deletion? (footnote: "Implementation guidance: ICANN Org will develop the SSAD Privacy Policy for SSAD users, which it may publish for public comment to obtain input from potential SSAD users"). **Input received**: • RrSG – No concern

Contracted Parties and SSAD:
(…)
e. Where required by applicable law, MUST provide mechanism under which the data subject may exercise its right to erasure, to object to automated processing of its personal information should this processing have a legal or similarly significant effect, and any other applicable rights
(…)

60. ALAC	This is not a can't live with, but a question of how this could be implemented?	

Recommendation #12 – Query Policy

The EPDP Team recommends that the Central Gateway Manager:
(…)
In the event the Central Gateway Manager makes a determination based on abuse to limit the number of requests from a requestor, further to point b, the requestor MAY seek redress via ICANN org if it believes the determination is unjustified.
(…)

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
61. ICANN org	b) "In the event the entity receiving requests makes a determination based on abuse to limit		EPDP Team to clarify what is expected in relation to 'redress' – is this similar to a

	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." Could the EPDP team also please clarify what "redress" would entail? If it's a reexamination request as referenced in Rec #6, perhaps that can be referenced here?		reexamination? So that the SSAD/CGM would be requested to reexamine whether the submission by the requestor are indeed abusive. Feedback RrSG: Agree it's similar to reexamination

"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
62. 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.

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
63. 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

Recommendation #15 – Financial Sustainability

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
64. 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

"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."

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
65. 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.

(…)
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

66. 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.

Footnote 60: 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".

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration
67. ICANN Org	Original Comment: ALAC	Add a footnote to "ICANN MAY contribute to the (partial) covering of	ICANN org:

	The ALAC agrees with "ICANN MAY contribute to the (partial) covering of costs for maintaining the Central Gateway." but it needs a footnote to 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	costs for maintaining the Central Gateway." saying "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".	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 "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."

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.

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration

68. 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?

(…)
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.[7]
(…)

[7] 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".

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

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
71. 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

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
72. 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."	The intent of use of "cost distribution" needs to be clarified.	EPDP Team to clarify intent of use of "cost distribution"

	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 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

Group	Text & Rationale	Proposed updated text	For EPDP Team Consideration

73. ICANN org	74. 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."
75. ICANN org	a. The activity of all SSAD entities MUST be logged. (for further details, please see the implementation guidance below).		Can the EPDP team please clarify who is expected to do the logging?

76. 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? d) "These logs shall not contain any personal data."		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? 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." 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 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?

	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.		
77. 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 (surely this would merely a listing in their individual accounts) and contracted parties, rather the data in those logs	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 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.

(…)
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
78. 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

79. 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
80. 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 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.		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 related to capturing rationales either in this recommendation or in Rec #6?
81. BC	Original comment: RySG • Disclosure decisions including a written rationale must be stored.	Change to: Disclosure decisions including a rationale must be stored; access	Change applied **Flagged for discussion:**

	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	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.	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”).