

Recommendation #2 – Accreditation of Governmental entities

Please note that the staff support team has reviewed all the input received and has applied changes as follows:

- Change applied as proposed
- Change applied but with modification
- Change not applied – rationale provided
- Need further guidance from EPDP Team to decide if / what change should be applied
- Response to question posed
- Request for further input from group that provided comment

Instructions: EPDP Team members are expected to review the last column ('how addressed') and indicate if any of the changes that have been applied or have not been applied have resulted in 'cannot live' with items. Please indicate your rationale for flagging an item and provide a proposal for how your concern can be addressed factoring in previous discussions.

Group	Change that has resulted in cannot live with status & Rationale	Proposed updated text	How Addressed
RySG	9) Use of “data controller” in this paragraph and through the recommendation may be confusing in implementation as the policy does not identify which parties are controllers. Change applied – updated ‘data controller’ to ‘Contracted Parties’ where deemed applicable.	Disagree - the term “data controller” was more appropriate in these cases. Change the text back to “data controller” from “contracted parties”.	Change applied based GAC update. (See version below.)
GAC	Use of term CERT - Isn't the correct term “CSIRT” as opposed to CERT (which I believe is a TM 'd term that has become somewhat genericized)?	Replace CERTs with CSIRTs	GAC disagreed with this change proposed by RySG, noting: CERT is more relevant to governmental entities.

<p>GAC</p>	<p>SSAD MUST ensure reasonable access to RDDS for entities that require access to this data for the exercise of their public policy tasks. In view of their obligations under applicable data protection rules, the final responsibility for granting access to RDDS data will remain with the party that is considered to be a controller for the processing of that RDDS data that constitutes personal data.</p> <p>The SSAD cannot “ensure” but it can be designed and created to “facilitate”.</p>	<p>Change to SSAD MUST facilitate reasonable access to...</p>	<p>GAC disagreed with this change, and provided, “SSAD MUST provide reasonable access”</p>
<p>ICANN org</p>	<p>“SSAD MUST provide reasonable access to non-public registration data for entities that require access to this data for the exercise of their public policy tasks.”</p> <p>ICANN org is unclear how this requirement should be implemented. There are several entities that make up the SSAD. How would each implement this requirement? ICANN org understands this statement as an objective. Is ICANN org expected to enforce a requirement of “reasonable access” and against which party?</p>		
<p>ICANN org</p>	<p>Use of “data controller” in this paragraph and through the recommendation may be confusing in implementation as it is not</p>	<p>ICANN org suggests replacing “data controller” throughout the recommendation with the relevant</p>	

	yet clear which party/parties will be deemed to be controllers.	Contracted Party or the Central Gateway Manager, as applicable.	
ICANN org	<p>“Consumer rights organizations granted a public policy task by law or delegation from a governmental entity”</p> <p>ICANN org is unclear how to enforce this requirement. May a government accredit a private entity within its jurisdiction? What about private entities outside its jurisdiction? What about private individuals within its jurisdiction? And private individuals outside its jurisdiction?</p>		
ICANN org	Footnote 2 says that any country that ratifies an IGO’s treaty may accredit that IGO. ICANN org understood from the team’s previous discussion that IGO accreditation would be conducted by the IGO’s host country. Can the EPDP team please clarify whether footnote 2 reflects the team’s agreement?		
ICANN org	Governmental Accreditation requirements MUST follow the requirements set out in Rec. 1.3.	ICANN org suggests the following minor edit for clarity: “Governmental Accreditation Authorities MUST follow the requirements set out in Recommendation 1, paragraph 1.3 of this report.”	
ICANN org	d. Data access		

	As there is no description, ICANN org suggests deleting this bullet.		
ICANN org	<p>Implementation Guidance: “Accredited users will be required to follow the safeguards as set by the policy. This is without prejudice for the entity to respect safeguards under its domestic law”</p> <p>Can the EPDP team please clarify to which safeguards does this guidance refer? Is it the Terms of Use and other policies as defined in Rec 10-13-14?</p>		
ICANN org	<p>“Accredited entities SHOULD provide details to aid the disclosure decision such as any applicable local law relating to the request.”</p> <p>Can the EPDP team please clarify to whom the details would be provided? Would it be included in the request that is sent to the Contracted Party?</p>		

Recommendation #2. Accreditation of governmental entities

1. Definitions

~~All definitions of the previous preliminary recommendation apply in addition to:~~

- ~~1. — Eligible government entity: a government entity (including local government) that has a purpose to access RDDS data for the exercise of a public policy task within its mandate.~~

12. Objective of accreditation

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

~~Notwithstanding these obligations, t~~The development and implementation of an accreditation procedure that specifically applies to governmental entities will facilitate decisions that ~~these data controllers~~ ~~Contracted Parties~~ ^[LC2] will need to make before granting access to ~~non-public registration data~~ ~~RDDS data~~ to a particular entity or automated disclosure decisions, if applicable. This accreditation procedure can provide data controllers with information necessary to allow them to assess and decide about the disclosure of data.

23. Eligibility

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

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

34. Determining eligibility

Eligible government entities are those that require access to ~~non-public RDDS~~ [registration](#) data for the exercise of their public policy task, in compliance with applicable data protection laws. Whether an entity should be eligible is determined by a country/territory-~~nominated~~ [designated](#) Accreditation Authority. ~~This eligibility determination does not affect the final responsibility of the data controller~~ [Contracted Party](#) ^[LC4] to determine whether or not to disclose personal data following a request for ~~RDDS non-public~~ [registration](#) data.

45. Requirements of the Governmental Accreditation [Authority](#) requirements

Governmental Accreditation requirements ~~will~~ [MUST](#) follow the requirements set out in Rec. 1.3.

Additionally, the requirements ~~SHALL~~ [MUST](#) be listed and made available to eligible government entities. [Failure to abide by these requirements may result in de-accreditation of the Accreditation Authority by ICANN Org.](#)

56. Accreditation procedure

Accreditation ~~would~~ [MUST](#) be provided by an approved accreditation authority. ^[3] This authority may be either a country's/territory's governmental agency (e.g. a Ministry) or delegated to an intergovernmental ~~agency~~ [organization](#). This authority SHOULD publish the requirements for accreditation and carry out the accreditation procedure for eligible government entities.

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

[Implementation Guidance:](#)

- Accreditation is required for a party-governmental entity to participate in the access-system (SSAD). Unaccredited governmental entities ~~parties~~ can make data requests outside the system SSAD, and Contracted Parties should have procedures in place to provide reasonable access.
 - ~~Accreditation does not guarantee disclosure of the data. The final responsibility for the decision to disclose data lies with the data controller. [MOU7]~~
 - ~~Any accredited user will be expected to only request the personal data that it needs to process in order to achieve its processing purposes. An accredited user will be obligated to minimize the number of queries they make to those that are reasonably necessary to achieve the purpose. [MK8] [MOU9]~~
- Accredited users will be required to follow the safeguards as set by the policy. This is without prejudice for the entity to respect safeguards under its domestic law
 - ~~The possibility of disclosure of RDDS data to accredited governmental entities including law enforcement MUST be made clear to the data subject. Upon a request from a data subject inquiring about the exact processing activities of their data within the SSAD, relevant information SHOULD be disclosed as soon as reasonably feasible. However, if there is a risk that the applicable investigation or legal procedure could be compromised if the request for data were disclosed to the data subject, then the SSAD and/or the disclosing entity MAY keep the nature or existence of these requests confidential from the data subject. Confidential requests MAY be disclosed to data subjects in cooperation with the requesting authority, and in accordance with the data subject's rights under applicable law. [MOU10]~~
 - ~~Accredited entities SHOULD indicate the requirement for confidentiality for any requests where applicable.~~
- Accredited entities SHOULD provide details to aid the disclosure decision such as any applicable local law relating to the request.

[1] Implementation consideration: such a body could be an International Governmental Organization.

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

[3] ~~For clarity, an entity could not serve as both an accreditation authority and an identity provider.~~

CANNOT LIVE WITH

Group	Text & Rationale	Proposed updated text	How Addressed
-------	------------------	-----------------------	---------------

1. ICANN Org	Upon review of the recommendation, ICANN org is unsure how to implement or enforce this recommendation as it is unclear what requirements are expected of governments, ICANN org, or the Central Gateway Manager.		EPDP Team to provide further clarity on the expectations for implementation and enforcement.
--------------	---	--	--

MINOR EDITS

Group	Text & Rationale	Proposed updated text	How Addressed
2. RySG	<p>SSAD MUST ensure reasonable access to RDDS for entities that require access to this data for the exercise of their public policy tasks. In view of their obligations under applicable data protection rules, the final responsibility for granting access to RDDS data will remain with the party that is considered to be a controller for the processing of that RDDS data that constitutes personal data.</p> <p>The SSAD cannot “ensure” but it can be designed and created to “facilitate”.</p>	Change to SSAD MUST facilitate reasonable access to...	Change applied
3. RySG	Use of term CERT - Isn't the correct term “CSIRT” as opposed to CERT (which I believe is a TM 'd term that has become somewhat genericized)?	Replace CERTs with CSIRTs	Change applied

4. RySG	Use of RDDS is confusing in some places - RDDS is short for Registration Data Directory Services.	Make sure use of RDDS is as intended (rather than for example non-public registration data)	Change applied – changed references to RDDS to non-public registration data. EPDP Team, and especially GAC Team, to indicate if there are concerns about this change.
5. RySG	<p>“Accredited entities SHOULD indicate the requirement for confidentiality for any requests where applicable.”</p> <p>To be clear if the requirement for confidentiality is not noted, then such requests will be releasable. If the requirement of confidentiality is essential, then for clarity, this should be a ‘MUST’ to prevent any weakening of this requirement.</p>	“Accredited entities MUST indicate the requirement for confidentiality for any requests where applicable.	Change applied
6. ICANN org	First bullet: “All definitions of the previous preliminary recommendation apply in addition to:”	Delete as definitions have been removed from Rec #1 and now apply to the full report.	Change applied
7. ICANN org	<p>1. Eligible government entity: a government entity (including local government) that has a purpose to access RDDS data for the exercise of a public policy task within its mandate.</p> <p>Can the EPDP team please clarify if this recommendation is also intended to cover accreditation for intergovernmental organizations (IGOs)? We understand from 3. Eligibility that an IGO may serve as the</p>		EPDP Team to clarify whether eligible government entity also includes accreditation for intergovernmental organizations (IGOs).

	Accreditation Authority for a national government. May it also be accredited as an Accreditation Authority for its members?		
8. ICANN org	<p>2. "SSAD MUST ensure reasonable access to RDDS..."</p> <p>2. ICANN org is concerned that this sentence will cause confusion during implementation because it's written as a requirement but we understand it as an objective. Can the EPDP team please clarify whether this is an obligation (MUST) for CPs or the Gateway to provide access? Or is this an objective? Is this intended to be an enforceable obligation? This recommendation may ensure a mechanism for accrediting governmental entities, however, it does not ensure access in any given case.</p>		Note this language has been clarified per comment #3. ICANN org to review whether this addresses the concern expressed.
9. ICANN org	2. Use of "data controller" in this paragraph and through the recommendation may be confusing in implementation as the policy does not identify which parties are controllers.	ICANN org suggests replacing "data controller" throughout the recommendation with the relevant Contracted Party or the Central Gateway Manager, as applicable.	Change applied – updated 'data controller' to 'Contracted Parties' where deemed applicable.
10. ICANN org	<p>2. "Notwithstanding these obligations.."</p> <p>It's unclear to which obligations this phrase is referencing.</p>	Suggest deleting "Notwithstanding these obligations."	Change applied

<p>11. ICANN org</p>	<p>1. Eligibility</p> <p>Does the EPDP team intend that government entities are restricted to accreditation under Rec #2? Or may they be accredited per Rec #1?</p> <p>Further the first paragraph under 3 contemplates that accreditation under Rec #2 is limited to “government entities.” Does the EPDP team intend for this accreditation to be limited to government entities only as the third bullet under 3. implies that governmental entities can grant tasks to non-governmental entities.</p>		<p>EPDP Team to clarify whether governmental entities are restricted to accreditation under rec #2 or may they also be accredited per #1.</p> <p>Does the EPDP intend for this accreditation to be limited only to government entities as bullet 3 implies that governmental entities can grant tasks to non-governmental entities?</p>
<p>12. ICANN org</p>	<p>1. “... Whether an entity should be eligible is determined by a country/territory nominated Accreditation Authority.:</p> <p>Should “nominated” in this paragraph be changed to "designated" since it is presumed that the entity put forth by a governmental agency would be confirmed (as opposed to only nominated) as that government's accreditation authority?</p>		<p>Change applied</p>
<p>13. ICANN org</p>	<p>Requirements of the Governmental Accreditation requirements</p>	<p>Suggest rewording to: “Governmental Accreditation Authority requirements”</p>	<p>Change applied</p>

<p>14. ICANN org</p>	<p>5. “Additionally the requirements SHALL be listed and made available to eligible government entities.”</p> <p>Can the EPDP team please clarify to which requirements it is referring? Is it the requirements as listed in 1.3? Also, where must these requirements be listed and made available to the eligible government entities? Further, it is unclear how this requirement would be enforced or by whom. Could the team provide further clarity on these points?</p>		<p>EPDP team to clarify to which requirements section 5 is referring (“Additionally the requirements SHALL be listed and made available to eligible government entities”)? Is it the requirements as listed in 1.3? Also, where must these requirements be listed and made available to the eligible government entities? Further, it is unclear how this requirement would be enforced or by whom. Could the team provide further clarity on these points?</p>
<p>15. ICANN org</p>	<p>1. “Accreditation would be provided by an approved accreditation authority. This authority may be either a country’s/territory’s governmental agency (e.g. a Ministry) or delegated to an intergovernmental agency.”</p> <p>Can the EPDP team please clarify whether “would” in this sentence ought to be a “SHOULD” or “MUST?” Further, the sentence seems to contemplate approval of an accreditation authority. Does the use of “approved” here mean one that has been “designated” by a government? Finally, is “intergovernmental agency” as referenced here meant to be an “intergovernmental organization (IGO)”?</p>		<p>EPDP team to clarify whether “would” in this sentence ought to be a “SHOULD” or “MUST?” Further, the sentence seems to contemplate approval of an accreditation authority. Does the use of “approved” here mean one that has been “designated” by a government? Finally, is “intergovernmental agency” as referenced here meant to be an “intergovernmental organization (IGO)”?</p>

<p>16. ICANN org</p>	<p>6. Bullets a)-d)</p> <p>Can the EPDP team please clarify whether bullets a) and b) are intended to serve as guidance for governmental agencies or are they intended as requirements? Further, it's unclear if the remaining bullets in this section are intended as a required procedure for accreditation. Can the team please clarify?</p>		<p>EPDP team to clarify whether bullets a) and b) are intended to serve as guidance for governmental agencies or are they intended as requirements? Further, it's unclear if the remaining bullets in this section are intended as a required procedure for accreditation. Can the team please clarify?</p>
<p>17. ICANN org</p>	<p>6. Bullet d) is labeled as "Data access," but it's unclear what that is meant to encompass. Can the team please clarify?</p> <p>Further, the first bullet under d) may be made clearer if it specified who must do what.</p> <p>Bullets 3 and 4 under d) include the phrases "will be expected," "will be obligated," and "will be required." Can the team clarify whether these statements are intended to be requirements and thus should use "MUST" in place of those phrases?</p> <p>Bullet 4 under d) notes "the safeguards as set by the policy." Can the EPDP team please clarify to which safeguards it is referring? Is this intended to be the</p>	<p>Suggested edit for d), first bullet: "Parties MUST be accredited to participate in the SSAD."</p>	<p>EPDP Team to clarify:</p> <p>6. Bullet d) is labeled as "Data access," but it's unclear what that is meant to encompass. Can the team please clarify?</p> <p>Further, the first bullet under d) may be made clearer if it specified who must do what.</p> <p>Bullets 3 and 4 under d) include the phrases "will be expected," "will be obligated," and "will be required." Can the team clarify whether these statements are intended to be requirements and thus should use "MUST" in place of those phrases?</p> <p>Bullet 4 under d) notes "the safeguards as set by the policy." Can the EPDP team please clarify to which safeguards it is referring? Is this intended to be the</p>

	<p>policies outlined in the combined Rec 10-13-14?</p> <p>Bullet 5 under d) in the first and last sentences seem to include requirements directed at a registrar's privacy policy and does not appear to be a part of the accreditation procedure for governmental agencies. ICANN org suggests this requirement be addressed elsewhere in the report.</p>		<p>policies outlined in the combined Rec 10-13-14?</p>
18. ICANN org	<p>Footnote 1: Is this intended as implementation guidance for ICANN org or is it intended for governmental accreditation authorities?</p>		<p>EPDP Team to clarify: is footnote 1 (Implementation consideration: such a body could be an International Governmental Organization.) intended for ICANN org or governmental accreditation authorities?</p>