**Preliminary Recommendation #2. Accreditation of governmental entities**

**1. Definitions**

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

### 2. Objective of accreditation

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.

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

### 3. Eligibility

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

* Civil and criminal law enforcement 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 Emergency Response Teams (CERTs),
* Data protection authorities,

### 4. Determining eligibility

Eligible government entities are those that require access to non-public RDDS 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 Accreditation Authority. This eligibility determination does not affect the final responsibility of the data controller to determine whether or not to disclose personal data following a request for RDDS data.

### 5. Requirements of the Governmental Accreditation requirements

Governmental Accreditation requirements will follow the requirements set out in Rec. 1.3

Additionally the requirements SHALL be listed and made available to eligible government entities.

### 6. Accreditation procedure

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. This authority SHOULD publish the requirements for accreditation and carry out the accreditation procedure for eligible government entities.

1. Accreditation emphasizes the responsibilities of the data requestor (recipient), who is responsible for complying with the law.
2. Accreditation will focus on the requirements of the law, such as requirements regarding data retention length, secure storage, organizational data controls, and breach notifications.

### Renewal, Logging, Auditing, Complaint and De-accreditation will be handle as per Rec. 1

###

### Data access

* Accreditation is required for a party to participate in the access system (SSAD). Unaccredited parties can make data requests outside the system, and contracted parties should have procedures in place to provide reasonable access.
* Accreditation does not guarantee disclosure of the data. The final responsibility for the decision to disclose data lies with the data controller.
* 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.
* 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.
* 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 Organisation [↑](#footnote-ref-1)