4. EPDP Team Responses to Charter Questions & Preliminary Recommendations

The EPDP Team will not finalize its responses to the charter questions and recommendations to the GNSO Council until it has conducted a thorough review of the comments received during the public comment period on this Initial Report. Additionally, if ICANN Org receives further guidance from the European Data Protection Board ("EDPB"), the EPDP Team will consider this guidance in its Final Report.[1] At the time of publication of this Report, no formal consensus call has been taken on these responses and preliminary recommendations; however, this Initial Report did receive the support of the EPDP Team for publication for public comment.[2] Where applicable, differing positions have been reflected in the Report.

Note: During Phase 1 of the EPDP Team's work, the EPDP Team was tasked with reviewing the Temporary Specification. The Temporary Specification was established as a response to the GDPR[3]. Accordingly, the GDPR is the only law that is specifically referenced in this report. The EPDP team has extensively deliberated whether this Initial Report could be drafted in a way that is agnostic to any specific law, but it was determined that the report would benefit from explicit references to facilitate the implementation of the Team's recommendations. The GDPR is a regional law covering multiple jurisdictions and - given the strict criteria it contains - compliance with this law has a high probability of being compliant with other national data protection laws. The EPDP team fully endorses ICANN's aspiration to be globally inclusive, and nothing in this report shall overturn the basic principle that contracted parties can and must comply with locally applicable statutory laws and regulations.

4.1 System for Standardized Access/Disclosure to Non-Public Registration Data (SSAD)

In Annex A, further details are provided in relation to the approach and the materials that the EPDP Team reviewed in order to address the charter questions and develop the following preliminary recommendations.

As part of its deliberations, the EPDP Team considered various models but agreed to put the following SSAD model forward for public comment. This SSAD model is based on the following high level principles/concepts:

[1] See https://www.icann.org/en/system/files/correspondence/marby-to-jelinek-stevens-25oct19-en.pdf and https://www.icann.org/en/system/files/files/unified-access-model-gtld-registration-data-25oct19-en.pdf

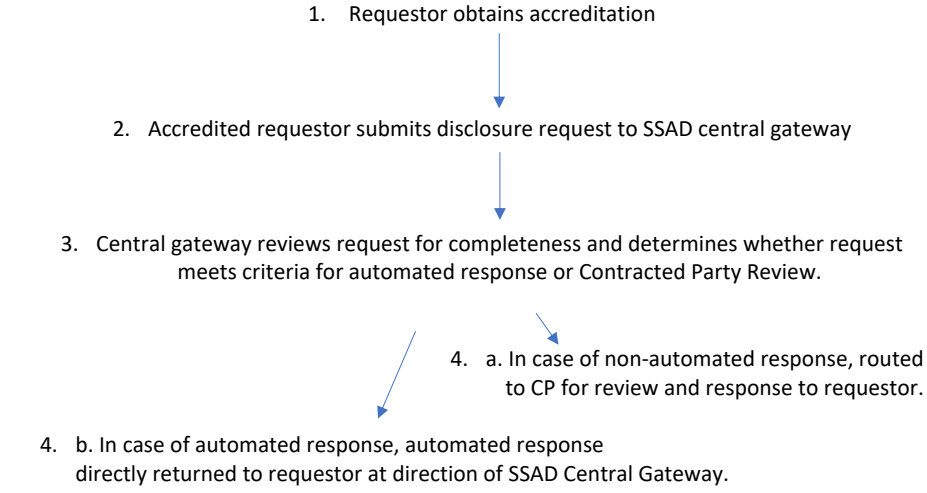
[2] Following a review of public comments, the EPDP Team will take a formal consensus call before producing its Final Report.

[3] "This Temporary Specification for gTLD Registration Data (Temporary Specification) establishes temporary requirements to allow ICANN and gTLD registry operators and registrars to continue to comply with existing ICANN contractual requirements and community-developed policies in light of the GDPR."

- Full automation[4] of the SSAD may not be possible, but the EPDP Team recommends that the SSAD must be automated where technically feasible AND legally permissible. Additionally, in areas where automation is not both technically feasible and legally permissible, standardization is the baseline objective.
- Experience gained over time with SSAD disclosure requests and responses must inform further streamlining and standardization of responses.
- In recognition of the expected evolving nature of SSAD and in an effort to avoid having to conduct a PDP every time a change needs to be made, a mechanism, which focuses solely on the implementation of the SSAD and does not contradict PDP and/or contractual requirements would need to be put in place to oversee and guide the continuous improvements of the SSAD.
- Meaningful SLAs need to be put in place, but these may need to be of an evolutionary nature to recognize that there will be a learning curve.
- Responses to disclosure requests, regardless of whether review is conducted manually or an automated responses is triggered, are returned from the relevant Contracted Party to the requestor, but appropriate logging mechanisms must be in place to allow for the SSAD to confirm that SLAs are met and responses are being processed according to the policy.

This model has been visually represented hereunder[5]; the diagram highlights which aspects of the roles and responsibilities are expected to change depending on the chosen model.

Commented [MK1]: To be replaced by detailed diagram, once developed



[4] See Automation Preliminary Recommendation for further details.
[5] For a standalone version, please see https://community.icann.org/x/BQZxBw.

Main SSAD Roles & Responsibilities:

- **Central Gateway Manager** – role performed by or overseen by ICANN Org. Responsible for managing intake and routing of SSAD requests that require manual review to responsible Contracted Parties. Responsible for managing and directing automated responses, consistent with the criteria established and agreed to in these policy recommendations.
- **Accreditation Authority** – role performed by or overseen by ICANN Org. A management entity who has been designated to have the formal authority to "accredit" users of SSAD, i.e., to confirm and Verify the identity of the user (represented by an Identifier Credential) and assertions (or claims) associated with the Identity Credential (represented by Authorization Credentials).
- **Identity Provider -** Responsible for 1) Verifying the identity of a requestor and managing an Identifier Credential associated with the requestor and 2) Verifying and managing Authorization Credentials associated with the Identifier Credential. For the purpose of the SSAD, the Identity Provider may be the Accreditation Authority itself or it may rely on zero or more 3rd parties.
- **Contracted Parties** – Responsible for responding to disclosure requests that do not meet the criteria for an automated response.
- **SSAD Advisory Group** – Group consisting of ICANN community representatives responsible for advising ICANN Org and Contracted Parties on 1) SLA matrix review; 2) categories of disclosure requests which should be automated; 3) other implementation improvements such as the identification of possible user categories and/or disclosure rationales. The Advisory Group may also make recommendations to the GNSO Council for any policy issues that may require further policy work.

It is the expectation that the different roles and responsibilities will be outlined in detail and confirmed in the applicable agreements.

Below is a detailed breakdown of the underlying assumptions and policy recommendations that the EPDP Team is putting forward for community input.

4.2 ICANN Board and ICANN Org Input

In order to help inform its deliberations, the EPDP Team reached out to both the ICANN Board and ICANN Org "to understand the Board's position on the scope of operational responsibility and level of liability (related to decision-making on disclosure of non-public registration data) they are willing to accept on behalf of the ICANN organization along with any prerequisites that may need to be met in order to do so".

ICANN Org provided its response on 19 November 2019 noting in part that "ICANN org proposed that it could operate a gateway for authorized data to pass through. As noted above, the gateway operator does not make the decision to authorize disclosure. In the proposed model, the authorization provider would decide whether or not the criteria for disclosure are

met. If a request is authorized and authenticated, the gateway operator would request the data from the contracted party and disclose the relevant data set to the requestor".

The ICANN Board provided its response on 20 November 2019 noting in part that "the Board has consistently advocated for the development of an access model for non-public gTLD registration data. If the EPDP Phase 2 Team's work results in a consensus recommendation that ICANN org take on responsibility for one or more operational functions within a SSAD, the Board would adopt that recommendation unless the Board determined, by a vote of more than two-thirds, that such a policy would not be in the best interests of the ICANN community or ICANN. Given the Board's advocacy for the development of an access model, and support for ICANN org's dialogue with the EDPB on a proposed UAM, it is likely that the Board would adopt an EPDP recommendation to this effect".

The EPDP Team will consider this input together with the feedback from the EDPB, once received; the EPDP Team will also consider the input received during the public comment period, to make a final determination of the division of roles and responsibilities in the SSAD.

4.3 SSAD Underlying Assumptions

The EPDP Team used the following underlying assumptions to develop the following preliminary policy recommendations. These underlying assumptions do not necessarily create new requirements for contracted parties; instead, the assumptions are designed to assist both the readers of this Initial Report and the ultimate policy implementers in understanding the intent and underlying assumptions of the EPDP Team in putting forward the SSAD model and related recommendations.

- The objective of the SSAD is to provide a predictable, transparent, efficient and accountable mechanism for the access/disclosure of non-public registration data.
- The SSAD must be compliant with the GDPR and other applicable data protection legislations for all parties.
- SSAD must have the ability to adhere to these policy principles and recommendations.

Conventions Used in this Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 148 [RFC21199] [RFC817410].

Preliminary Recommendation #1. Accreditation[6]

Proposed working definitions used by the EPDP Team in its discussion of accreditation:

[6] Note that accreditation is not referring to accreditation/certification as discussed in GDPR Article 42/43.

- **Accreditation** - An administrative action by which the accreditation authority declares that a user is approved to gain access to SSAD in a particular security configuration with a prescribed set of safeguards.
- **Accreditation Authority** - A management entity who has been designated to have the formal authority to "accredit" users of SSAD, i.e., to confirm and Verify the identity of the user (represented by an Identifier Credential) and assertions (or claims) associated with the Identity Credential (represented by Authorization Credentials).
- **Accreditation Authority Auditor** - Independent entity that is contracted by ICANN org, or function that is carried out by ICANN Org itself if the Accreditation Authority function is outsourced to a third party, to carry out auditing requirements as outlined in auditing preliminary recommendation.
- **Authentication** - The process or action of Validating the Identity Credential and Authorization Credentials of a Requestor.
- **Authorization** - A process for approving or denying disclosure non-public registration data.
- **Credential**
    - **"Identifier Credential":** A data object that is a portable representation of the association between an identifier and a unit of authentication information, and that can be presented for use in Validating an identity claimed by an entity that attempts to access a system. Example: [Username/Password], [OpenID credential], X.509 public-key certificate.
    - **"Authorization Credential"**: A data object that is a portable representation of the association between an Identifier Credential and one or more access authorizations, and that can be presented for use in Validating those authorizations for an entity that attempts such access. Example: [OAuth credential], X.509 attribute certificate.
- **De-accreditation of Accreditation Authority –** An administrative action by which ICANN org revokes the agreement with the accreditation authority, if this function is outsourced to a third party, following which it is no longer approved to operate as the accreditation authority.
- **Identity Provider -** Responsible for 1) Verifying the identity of a requestor and managing an Identifier Credential associated with the requestor and 2) Verifying and managing Authorization Credentials associated with the Identifier Credential. For the purpose of the SSAD, the Identity Provider may be the Accreditation Authority itself or it may rely on zero or more 3rd parties.
- **Revocation of User Credentials-** The event that occurs when an Identity Provider declares that a previously valid credential has become invalid.
- **Validate -** To test or prove the soundness or correctness of a construct. (Example: The Discloser will Validate the Identity Credential and Authorization Credentials as part of its Authorization process.)
- **Validation -** Establish the soundness or correctness of a construct.
- **Verify -** To test or prove the truth or accuracy of a fact or value. (Example: Identity Providers Verify the identity of the requestor prior to issuing an Identity Credential.)

- **Verification -** The process of examining information to establish the truth of a claimed fact or value.

The EPDP Team recommends that a policy for accreditation of SSAD users is established.

The following principles underpin the accreditation policy:

a) SSAD must only accept requests for access/disclosure from accredited organizations or individuals. However, accreditation requirements must accommodate any intended user of the system, including an individual or organization who makes a single request. The accreditation requirements for regular users of the system and a one-time user of the system may differ.
b) Both legal persons and/or individuals are eligible for accreditation. An individual accessing SSAD using the credentials of an accredited entity warrants that the individual is acting on the authority of the accredited entity[7].
c) The accreditation policy defines a single Accreditation Authority, run and managed by ICANN org. This Accreditation Authority may work with external or third-party Identity Providers that could serve as clearinghouses to Verify identity and authorization information associated with those requesting accreditation.
d) The decision to authorize disclosure of registration data, based on Validation of the Identity Credential, Authentication Credentials, and data as required in preliminary recommendation concerning criteria and content of requests, will reside with the registrar, ICANN, or whatever authorization provider the EPDP Team ultimately agrees on.

Requirements

e) Verifying the Identity of the Requestor: The Accreditation Authority MUST verify the identity of the requestor, resulting in an Identity Credential.
f) Management of Authorization Credentials: The Accreditation Authority MUST verify and manage a set of dynamic assertions/claims associated with and bound to the Identity Credential of the requestor. This verification, performed by an Identity Provider, results in Authorization Credentials.
g) Authorization Credentials convey information such as:
    - Assertion as to the purpose(s) of the request
    - Assertion as to the legal basis of the requestor
    - Assertion that the user identified by the Identity Credential is affiliated with the Accreditation Authority
    - Assertion regarding compliance with laws (e.g., storage, protection and retention/disposal of data)
    - Assertion regarding agreement to use the disclosed data for the legitimate and lawful purposes stated

[7] Implementation guidance: The accredited entity is expected to develop appropriate policies and procedures to ensure appropriate use by an individual of its credentials.

- Assertion regarding adherence to safeguards and/or terms of service and to be subject to revocation if they are found to be in violation
- Assertions regarding prevention of abuse, auditing requirements, dispute resolution and complaints process, etc.
- Assertions specific to the requestor – trademark ownership/registration for example
- Power of Attorney statements, when/if applicable.

h) Validation of Identity Credentials and Authorization Credentials, in addition to the information contained in the request, facilitate the decision of the authorization provider to accept or reject the Authorization of an SSAD request. For the avoidance of doubt, the presence of these credentials alone DOES NOT result in or mandate an automatic access / disclosure authorization. However, the ability to automate access/disclosure authorization decision making is possible under certain circumstances where lawful.

i) Defines a base line "code of conduct" that establishes a set of rules that contribute to the proper application of data protection laws - including the GDPR - for the ICANN community, including:
   - A clear and concise explanatory statement.
   - A defined scope that determines the processing operations covered (the focus for SSAD would be on the Disclosure operation.)
   - Mechanism that allow for the monitoring of compliance with the provisions.
   - Identification of an Accreditation Body Auditor (a.k.a. monitoring body) and definition of mechanism(s) which enable that body to carry out its functions.
   - Description as to the extent a "consultation" with stakeholders has been carried out.
   - Etc.

The accreditation authority:

j) MUST have a uniform baseline application procedure and accompanying requirements for all applicants requesting accreditation, including:
   - Definition eligibility requirements for accredited users
   - Identity Validation, Procedures
   - Identity Credential Management Policies: lifetime/expiration, renewal frequency, security properties (password or key policies/strength), etc.
   - Identity Credential Revocation Procedures: circumstances for revocation, revocation mechanism(s), etc. [see also "Accredited User Revocation & abuse section below]
   - Authorization Credential Management: lifetime/expiration, renewal frequency, etc.
   - NOTE: requirements beyond the baseline listed above may be necessary for certain classes of requestors.

k) MUST define a dispute resolution and complaints process to challenge actions taken by the Accreditation Authority.

l) MUST be audited by an auditor on a regular basis. Should the Accreditation Authority be found in breach of the accreditation policy and requirements, it will be given an opportunity to address the breach, but in cases of repeated failure, a new Accreditation Authority must be identified or created. Additionally, accredited entities MUST be audited for compliance with the accreditation policy and requirements on a regular basis; (Note: detailed information regarding auditing requirements can be found in the Auditing preliminary recommendation).

m) MAY develop user groups / categories to facilitate the accreditation process as all requestors will need to be accredited, and accreditation will include identity verification.

n) MUST report publicly and on a regular basis on the number of accreditation requests received, accreditation requests approved/renewed, accreditations denied, accreditations revoked and information about the identity providers it is working with.

Accredited User Revocation & Abuse:

o) Revocation, within the context of the SSAD, means the Accreditation Authority can revoke the accredited user's status as an accredited user of the SSAD. A non-exhaustive list of examples where revocation may apply include 1) the accredited user's violation of the code of conduct, 2) the accredited user's abuse of the system, 3) a change in affiliation of the accredited user, or 4) where prerequisites for accreditation no longer exist.

p) A mechanism to report abuse committed by an accredited user must be provided by SSAD. Reports must be relayed to the Accreditation Authority for handling.

q) The revocation policy for individuals/entities should include graduated penalties. In other words, not every violation of the system will result in Revocation; however, Revocation may occur if the Accreditation Authority determines that the accredited individual or entity has materially breached the conditions of its accreditation and failed to cure based on: a) a third-party complaint received; b) results of an audit or investigation by the Accreditation Authority or auditor; c) any misuse or abuse of privileges afforded; d) repeated violations of the accreditation policy. In the event there is a pattern or practice of abusive behavior within an entity, the credential for the entity could be suspended or revoked as part of a graduated sanction.

r) Revocation will prevent re-accreditation in the future absent special circumstances presented to the satisfaction of the Accreditation Authority.

De-authorization of Identity Providers

s) The authorization policy for Identity providers should include graduated penalties. In other words, not every violation of the policy will result in De-authorization; however, De-authorization may occur if it has been determined that the Identity Provider has materially breached the conditions of its contract and failed to cure based on: a) a third-party complaint received; b) results of an audit or investigation by the Accreditation Auditor or auditor; c) any misuse or abuse of privileges afforded; d) repeated violations of the accreditation policy. Depending upon the nature and circumstances leading to the

de-authorization of an Identity Provider, some or all of its outstanding credentials may be revoked or transitioned to a different Identity Provider.

Accredited entities or individuals:

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

u) Will not be restricted in the number of SSAD requests that can be submitted during a specific period of time, except where the accredited entity poses a demonstrable threat to the SSAD. It is understood that possible limitations in SSAD's response capacity and speed may apply. For further details see the response requirements preliminary recommendation.

Fees:
The accreditation service will be a service that is financially sustainable. For further details, see the financial sustainability preliminary recommendation.

Implementation Guidance

In relation to accreditation, the EPDP Team provides the following implementation guidance:

a) Recognized, applicable, and well-established organizations could support the Accreditation Authority as an Identity Provider and/or Verify information. Proper vetting must take place if any such reputable and well-established organizations are to collaborate with the Accreditation Authority.
b) Examples of additional information the Accreditation Authority or Identity Provider may require an applicant for accreditation to provide could include:
   - a business registration number and the name of the authority that issued this number (if the entity applying for accreditation is a legal person);
   - information asserting trademark ownership.

Auditing / logging by Accreditation Authority and Identity Providers

c) The accreditation/verification activity (such as accreditation request, information on the basis of which the decision to accredit or verify identity was made) will be logged by the Accreditation Authority and Identity Providers.
d) Logged data shall only be disclosed, or otherwise made available for review, by the Accreditation Authority or Identity Provider, where disclosure is considered necessary to a) fulfill or meet an applicable legal obligation of the Accreditation Authority or Identity Provider; b) carry out an audit under this policy or; c) to support the reasonable functioning of SSAD and the accreditation policy.

See also auditing and logging preliminary recommendations for further details.

Preliminary Recommendation #2. Accreditation of governmental entities

1. <u>Definitions</u>

- Accreditation - An administrative action by which the accreditation authority declares that a party/entity user is approved to gain access to SSAD in a particular security configuration with a prescribed set of safeguards.
- Eligible entity: an entity that is considered by its government (including local government) to require access to RDDS data for the exercise of a public policy task.
- Accredited party/entity: an entity that has been accredited by an accreditation authority.
- Accreditation Authority - A management entity who has been designated to have the formal authority to "accredit" users of SSAD, i.e., to confirm and verify the identity of the user (represented by an “Identifier Credential”) and assertions (or claims) associated with the Identity Credential (represented by “Authorization Credentials”).
- Authentication - The process or action of verifying the Identity Credential and Authorization Credentials of a Requestor.
- Credentials
    - "Identifier Credential": A data object that is a portable representation of the association between an identifier and a unit of authentication information, and that can be presented for use in verifying an identity claimed by an entity that attempts to access a system. Example: [Username/Password], [OpenID credential], X.509 public-key certificate.
    - "Authorization Credential": A data object that is a portable representation of the association between an Identifier Credential and one or more access authorizations, and that can be presented for use in verifying those authorizations for an entity that attempts such access. Example: [OAuth credential], X.509 attribute certificate.
- Identity Provider - Responsible for 1) verifying the identity of a requestor and managing an Identifier Credential associated with the requestor and 2) verifying and managing Authorization Credentials associated with the Identifier Credential. For the purpose of

the SSAD, the Identity Provider may be the Accreditation Authority itself or it may rely on one or more trusted 3rd parties.

- Requestors: the entities submitting queries, the results of which gain them access to non-public gTLD registration data.
- Access Authorization – A process where an accredited entity provides its legal basis and applicable safeguards for processing personal data to meet its purpose against its identifier credential.
- Disclosing Decision - A process for approving or denying disclosure non-public registration data.
- RDDS - Registration Data Directory Services, the services that each contracted party use to collect and store domain name registration data that can be provided to access and disclosure systems such as via a System for Standardized Access/Disclosure) and WHOIS.
- Revocation of Accredited party/entity - An administrative action by which the accreditation authority revokes the credentials of an accredited party/entity who is no longer approved to operate in a particular security configuration with a prescribed set of safeguards.
- De-accreditation of Accreditation Authority – An administrative action by which ICANN org revokes the agreement with the accreditation authority following which it is no longer approved to operate as the accreditation authority.
- SSAD – System for Standardized Access/Disclosure – a system that ensures reasonable access to the non-public RDDS data for parties/entities that require legitimate access to this data.

2. Objective of accreditation

SSAD should ensure reasonable access to RDDS for entities that require access to this data for the exercise of their public policy task. 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 as the controller for the processing of that RDDS data that constitutes personal data.

Notwithstanding these obligations, the decisions that these data controllers will need to make before granting access to RDDS data to a particular entity, can be greatly facilitated by means of the development and implementation of an accreditation procedure. The 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 countries'/territories' government body or its authorized body would be available to various eligible entities that require access to non-public registration data for the exercise of their public policy task, including, but not limited to:

- Law enforcement authorities,
- Judicial authorities,

- Consumer right's organizations,
- Cybersecurity authorities, including national Computer Emergency Response Teams (CERTs),
- Data protection authorities,

4. Determining eligibility

Eligible entities are those that governments consider 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, without prejudice to the final responsibility of a disclosing party for the processing of personal data following a request for RDDS data.

5. Accreditation requirements:

In order to ensure that the accreditation procedure can provide useful information for the data controller to decide whether the RDDS data should be disclosed on the basis of a request from an accredited entity, the accreditation process should take account of a number of requirements.

The requirements shall be listed and made available to eligible entities.

Compliance of accredited entities with these requirements needs to be assured by the accreditation authority. On that basis, accredited parties can be authorized to participate in the SSAD system and receive the necessary access/authentication credentials. In particular, the accreditation authority needs to ensure that an accredited entity respects the following conditions.

- Have a specific and delineated purpose for their access to and use of non-public RDDS data.
- Represent that access to and use of non-public data is for a lawful purpose and its processing will not be incompatible with the purpose for which it is sought.
- Have appropriate procedures in place to ensure appropriate identity and access management for individual users in its internal organization.
- Comply with applicable laws and terms of service to prevent abuse of data accessed.
- Be subject to, ultimately, de-accreditation if they are found to fall short or in violation of any of these requirements.
- In cases of violation of any of these requirements, be subject to penalties under applicable laws.

6. Accreditation procedure

Accreditation would be provided by an approved accreditation authority. This authority may be

either a countries'/territories' 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 entities.

- Accreditation emphasizes the responsibilities of the data requestor (recipient), who is responsible for complying with the law.
- Accreditation will focus on the requirements of the law, such as requirements regarding data retention length, secure storage, organizational data controls, and breach notifications.
- Renewals will incorporate updated terms of service or other obligations imposed by the accreditation authority.
- Accredited parties must provide updated accreditation materials with validity dates covering the period of accreditation.
- The accreditation authority reserves the right to update what credentials or other material are required for accreditation.

a. Renewal

Accredited/authenticated parties must renew their accreditation/authentication periodically. Each authentication authority should determine an appropriate time limit.

b. Logging

The accreditation authority must log all contact details for the accredited entities and must keep a record of any abuse by the accredited entity. This is without prejudice to any obligation the accreditation authority or the accredited entities may already have to document their use of the system.

c. Auditing

Audits should be conducted by either the data protection authority or by the country/territory designated auditor. This is without prejudice to audits that may carried out by relevant data protection authorities.

d. Complaints

Complaints regarding unauthorized access to, or improper use of, data should be handled by the accreditation authority, for which appropriate procedures should be in place. This is without prejudice to other obligations they may already have under applicable data protection laws to ensure rights of individuals are respected.

e. 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 process the personal data that it needs to process in order to achieve its processing purposes. They will be obligated to minimize the number of queries they make to those that are reasonably necessary to achieve the purpose.
- Accredited entities will be required to follow the safeguards as set by the disclosing system.
- Disclosure of RDDS data to the type of third parties must be made clear to the data subject. Upon a request from a data subject inquiring about the exact processing activities of their data within the SSAD, [relevant information] should be disclosed as soon as reasonably feasible. However the nature of legal investigations or procedures may require SSAD and/or the disclosing entity keep the nature or existence of these requests confidential from the data subject. Confidential requests can be disclosed to data subjects in cooperation with the requesting authority, and in accordance with the data subject's rights under applicable law.
- 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.

f. De-Accreditation

- Accredited entities will be subject to graduated penalties, and ultimately de-accreditation if they are found to abuse the system.
- De-Accreditation will occur when the accreditation authority determines that the Accredited entity has materially breached the conditions of its Accreditation based upon either; a) a third-party complaint received; b) results of an audit or investigation; or c) otherwise for any misuse or abuse of the privileges afforded.
- De-accreditation will prevent re-accreditation in the future absent special circumstances. De-accreditation procedures will be on reasonable notice to the Accredited party/entity who shall have the right to an appeal.
- De-accreditation does not prevent the requestor from submitting future requests under the access method provisioned in Recommendation 18 of the EPDP Phase 1 Report, but that they will not be accredited, and thus will be subject to delays, and manual processing.

Preliminary Recommendation #3. Criteria and Content of Requests

The EPDP Team recommends that each SSAD request must include, at a minimum, the following information:

a) Domain name pertaining to the request for access/disclosure;
b) Identification of and information about the requestor (including, requestor's accreditation status, if applicable, the nature/type of business entity or individual, Power of Attorney statements, where applicable and relevant);
c) Information about the legal rights of the requestor specific to the request and specific rationale and/or justification for the request, (e.g., What is the basis or reason for the request; Why is it necessary for the requestor to ask for this data?);
d) Affirmation that the request is being made in good faith and that data received (if any) will be processed lawfully and only in accordance with the justification specified in (c);
e) A list of data elements requested by the requestor, and why the data elements requested are adequate, relevant and limited to what is necessary.

The objective of this recommendation is to allow for the standardized submission of requested data elements, including any supporting documentation.

Preliminary Recommendation #4. Third Party Purposes/Justifications

[As identified in the preliminary recommendation relating to criteria and content of requests, each request must include information about the legal rights of the requestor specific to the request and/or specific rationale and/or justification for the request, e.g. What is the basis or reason for the request; Why is it necessary for the requestor to ask for this data? The EPDP Team expects that over time, the entity responsible for receiving requests will be able to identify certain patterns that could result in the development of a preset list of rationales and/or justifications that a requestor can select from, while always maintaining the option for the requestor to provide this information in free form.]

Preliminary Recommendation #5. Acknowledgement of receipt

The EPDP Team recommends that the response time for acknowledging receipt of a SSAD request by the Central Gateway Manager must be without undue delay, but not more than two (2) hours from receipt.

The Central Gateway Manager MUST confirm that all required information as per preliminary recommendation #3, criteria and content of request, is provided. Should the Central Gateway Manager determine that the request is incomplete, the Central Gateway Manager must reply to the requestor with an incomplete request response, detailing which required data is missing, and provide an opportunity for the requestor to amend its request.

The response provided by the Central Gateway Manager should also include information about the subsequent steps as well as the timeline consistent with the recommendations outlined below.

Preliminary Recommendation #6. Contracted Party Authorization

1. The Contracted Party to which the disclosure request has been routed MUST review every request on its merits and MUST NOT disclose data on the basis of accredited user category alone. For the avoidance of doubt, automated review is not explicitly prohibited where it is both legally and technically permissible.
2. If deemed desirable, the Contracted Party may outsource the authorization responsibility to a third-party provider, but the Contracted Party will remain ultimately responsible for ensuring that the applicable requirements are met.
3. While the requestor will have the ability to identify the lawful basis under which it expects the Contracted Party to disclose the data requested, the Contracted Party must make the final determination of the appropriate lawful basis for the Contracted Party to disclose the requested information.
4. The Contracted Party should make a threshold determination (without processing the underlying data) about whether the requestor has established an interest in the disclosure of personal data. The determination should consider the elements:
    - Is the identity of the requestor clear/verified?
    - Has the requestor provided a legitimate interest or other lawful basis in processing the data?
    - Are the data elements requested necessary to the requestor's stated purpose?
        - Necessary means more than desirable but less than indispensable or absolutely necessary.
    - The Contracted Party should determine whether the data elements requested are limited and reasonable to achieve the requestor's stated purpose?
        - Each request should be evaluated individually (i.e. each submission should contain a request for data related to a single domain. If a submission relates to multiple domains, each must be evaluated individually.).
        - In addition, each data element in a request should be evaluated individually.

    If the answer to any of the above questions is no, the Contracted Party may deny the request, or require further information from the requestor before proceeding to paragraph 6 below.
    Absent any legal requirements to the contrary, disclosure cannot be 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; nor can refusal to disclose 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.
5. The Contracted Party may evaluate the underlying data requested once the validity of the request is determined under paragraph 4 above. The purpose of paragraph 5 is to determine whether the paragraph 6 [meaningful human review] is required. The Contracted Party's review of the underlying data should assess at least:
    - Does the data requested contain personal data?

- If no personal data, no further balancing required.

- The applicable lawful basis and whether the requested data contains personal data the authorization provider to determine if the balancing test, similar to the requirements under GDPR's 6.1.f, as described in paragraph 6 below is applicable and proceed accordingly.
- The Contracted Party should evaluate at least the following factors to determine whether the legitimate interest of the requestor is not outweighed by the interests or fundamental rights and freedoms of the data subject. No single factor is determinative; instead the authorization provider should consider the totality of the circumstances outlined below:
- **Assessment of impact**. Consider the direct impact on data subjects as well as any broader possible consequences of the data processing (e.g., triggering legal proceedings). Whenever the circumstances of the disclosure request or the nature of the data to be disclosed suggest an increased risk[8] for the data subject affected, this shall be taken into account during the decision-making.
- ***Nature of the data***. Consider the level of sensitivity of the data as well as whether the data is already publicly available.
- ***Status of the data subject***. Consider whether the data subject's status increases their vulnerability (e.g., children, other protected classes)
- ***Scope of processing***. Consider information from the disclosure request or other relevant circumstances that indicates whether data will be [securely] held (lower risk) versus publicly disclosed, made accessible to a large number of persons, or combined with other data (higher risk), .[provided that this is not intended to prohibit public disclosures for legal actions or administrative dispute resolution proceedings such as the UDRP or URS].
- ***Reasonable expectations of the data subject***. Consider whether the data subject would reasonably expect their data to be processed/disclosed in this manner.
- ***Status of the controller and data subject***. Consider negotiating power and any imbalances in authority between the controller and the data subject.
- ***Legal frameworks involved***. Consider the jurisdictional legal frameworks of the requestor, Contracted Party/Parties, and the data subject, and how this may affect potential disclosures.

If, based on consideration of the above factors, 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 data **shall** be disclosed. The rationale for the approval should be documented.

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

[8] [include reference to relevant GDPR provision]

6. The application of the balancing test and factors considered in paragraph 6 should be revised as appropriate to address applicable case law interpreting GDPR, guidelines issued by the EDPB or revisions to GDPR that may occur in the future.

Implementation Guidance

1. As noted in paragraph 4 above, in situations where the requestor has provided a legitimate interest for its request for access/disclosure, the Contracted Party should consider the following:
    - Interest must be specific, real, and present rather than vague and speculative.
    - An interest is generally legitimate so long as it can be pursued consistent with data protection and other laws.
    - Examples of legitimate interests include: (i) enforcement of legal claims; (ii) prevention of fraud and misuse of services; and (iii) physical, IT, and network security.

Preliminary Recommendation #7. Authorization for automated disclosure requests

For disclosure requests for which it has been determined that these can be responded to in an automatic fashion (i.e. no human intervention required) the following requirements will apply:

1. The Central Gateway Manager MUST confirm that all required information as per preliminary recommendation #3 'criteria and content of requests' is provided and that the request meets the criteria established in these policy recommendations (and is confirmed during the implementation phase) to qualify as an automated disclosure request.
2. Should the Central Gateway Manager determine that the request is incomplete, the Central Gateway Manager must reply to the requestor with an incomplete request response, detailing which required data is missing, and provide an opportunity for the requestor to amend its request.
3. Responses to SSAD requests MUST be provided consistent with the SLAs outlined in preliminary recommendation #8.

With respect to disclosure requests sent to a Contracted Party, a Contracted Party MAY request the Central Gateway to fully automate all, or certain types of, disclosure requests, irrespective of the ultimate policy requirements. A Contracted Party MAY retract or revise a request for automation that is not required by these policy recommendations at any time.

Implementation Guidance

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

- Law Enforcement in jurisdiction requests;
- Responses to UDRP Providers for registrant information verification.

The EPDP Team will further consider if other types of disclosure requests can be fully automated. Over time, based on experience gained and/or further legal guidance, the SSAD Advisory Group is expected to provide further guidance on which types of disclosure requests can be fully automated.

Preliminary Recommendation #8. Response Requirements

For the Central Gateway Manager:

a) Following receipt of a disclosure request, the Central Gateway Manager must confirm[9] that all required information as per the preliminary recommendation 'criteria and content of requests' is provided (see also preliminary recommendation #5 Acknowledgement of Receipt). Should the Central Gateway Manager establish that the request is incomplete, the Central Gateway Manager must provide an opportunity for the requestor to amend and resubmit its request.
b) Following confirmation that the request is syntactically correct and that all required information has been provided, the Central Gateway Manager must immediately and synchronously respond with an acknowledgement response and relay the disclosure request to the responsible Contracted Party, if it does not concern a request that meets the criteria for automatic disclosure.
c) As part of its relay to the responsible Contracted Party, the Central Gateway Manager MUST provide a recommendation to the Contracted Party whether to disclose or not. The Contracted Party MAY follow this recommendation. If the Contracted Party decides not to follow the recommendation of the Central Gateway Manager, the Contracted Party SHOULD communicate its reasons for not following the Central Gateway Manager recommendation so the Central Gateway Manager can learn and improve on future response recommendations.

Contracted Parties:

d) must provide a disclosure response without undue delay, unless there are exceptional circumstances. Such exceptional circumstances may include the overall number of requests received if the number far exceeds the established SLAs. SSAD requests that meet the automatic response criteria must receive an automatic disclosure response. For requests that do not meet the automatic response criteria, a response must be received in line with the SLAs outlined below.
e) Responses where disclosure of data (in whole or in part) has been denied should include: rationale sufficient for the requestor to understand the reasons for the decision, including, for example, an analysis and explanation of how the balancing test was applied (if applicable). Additionally, in its response, the entity receiving the

[9] It is the expectation that the initial review of the completeness of requests is done automatically with the system not accepting the request until all requested data has been provided.

access/disclosure request must include information on how public registration data can be obtained.

f) A separate accelerated timeline has been recommended for the response to 'Urgent' SSAD Requests, those Requests for which evidence is supplied to show an immediate need for disclosure (see below). The criteria to determine whether it concerns an urgent request are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation.

g) Must maintain a dedicated contact for dealing with Urgent SSAD requests which can be stored and used by the Central Gateway Manager, in circumstances where an SSAD request has been flagged as Urgent. Additionally, the EPDP Team recommends that Contracted Parties MUST publish their standard business hours and accompanying time zone on the homepage of their website (or in another standardized place that may be designated by ICANN from time to time).

The EPDP Team recommends that 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).

If a requestor is of the view that its request was denied erroneously, a complaint should be filed with ICANN Compliance. ICANN Compliance must either compel disclosure or confirm that the denial was appropriate. ICANN Compliance should be prepared to investigate complaints regarding disclosure requests under its standard enforcement processes.

Implementation Guidance:

a) The Central Gateway Manager MUST confirm that the request is syntactically correct, including proper and valid Authentication and Authorization Credentials. Should the Central Gateway Manager establish that the request is syntactically incorrect, the Central Gateway Manager MUST reply with an error response to the requestor detailing the errors that have been detected.

b) Should the Central Gateway Manager establish that the request is incomplete, Central Gateway Manager MUST reply with an incomplete request response to the requestor detailing which data required by policy is missing, providing an opportunity for the requestor to amend its request.

c) Typically the acknowledgement response will include a "ticket number" or unique identifier to allow for future interactions with the SSAD.

d) An example of online critical infrastructure includes root servers; an example of offline critical infrastructure includes bridges.

Preliminary Recommendation #9. Determining Variable SLAs for SSAD

How is priority defined?

Priority is a code assigned to requests for disclosure that contain agreed to, best effort target response times. The spectrum of codes is defined by urgency and corresponding impacts to match market conditions. It is assumed that the SSAD will contain an application to process disclosure requests and can manage a feature to set attributes for an inbound request in the SSAD.

Who sets the priority?

The initial priority of a disclosure request is set by the Central Gateway Manager based on the criteria outlined below.

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 Central Gateway Manager and/or 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 SHALL be communicated to the Requestor. The disclosing entity shall provide the requested information or provide a reason why it cannot disclose the information under the below-defined SLAs. It is expected that the process and procedures based on best practices such as incident or problem management will ultimately govern the processing of disclosure requests and in particular the assignments and subsequent management of the assigned priority. An appeal mechanism will likely be required.

If a Contracted Party is of the view that the priority designation is not assigned by the Central Gateway Manager in a manner consistent with the conditions established by EPDP Team, the Contracted Party can raise an appeal with the SSAD Steering Committee.

Priority Matrix for non-automated disclosure requests

Request Type	Priority	Proposed SLA[10] (for discussion) / Compliance at 6 months / 12 months / 18 months
Urgent Requests "The criteria to determine whether it concerns an urgent request are limited to circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure (online and offline) or child exploitation."	1	1 business day / 85% / 90% / 95%
Court orders, administrative proceedings (response to UDRP or URS filing, for example), etc.	2	2 business days / 85% / 90% / 95% *Note: this SLA is a current contractual obligation for registrars under the UDRP Rules (UDRP Rule 4(b))*
All other requests*	3	5 business days / 85% / 90% / 95%

*Note: Nothing in these policy recommendations explicitly prohibits the development of new categories and defined SLAs.

SLAs for disclosure requests that meet the criteria for fully-automated responses are expected to be further developed during the implementation phase, but these are expected to be under 60 seconds.

In the event the SSAD Advisory Panel identifies additional categories of requests that could be fully automated, the SSAD MUST allow for automation of the processing of well-formed, valid, complete, properly-identified requests from accredited users with some limited and specific set of legal basis and data processing purposes which are yet to be determined. These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention.

The "SSAD Advisory Panel" refers to the group whose membership has been tasked with reviewing and revising, as appropriate, the above-defined SLA matrix (see preliminary recommendation #18 for further details).

Preliminary Recommendation #10. Acceptable Use Policy

[10] 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.

The EPDP Team recommends that the following requirements are applicable to the requestor and must be confirmed by the Central Gateway Manager and subject to an enforcement mechanism. For the avoidance of doubt, every request does not have to go through an enforcement procedure; the enforcement mechanism may, however, be triggered in the event of apparent misuse.

The requestor:

a) Must only request data from the current RDS data set (no historic data);
b) Must, for each request for RDS data, provide representations of the corresponding purpose and lawful basis for the processing, which will be subject to auditing (see the auditing preliminary recommendation for further details);
c) MAY request data from the SSAD for multiple purposes per request, for the same set of data requested;
d) For each stated purpose must provide (i) representation regarding the intended use of the requested data and (ii) representation that the requestor will only process the data for the stated purpose(s). These representations will be subject to auditing (see auditing preliminary recommendation further details);
e) Must handle the data subject's personal data in compliance with applicable law (see auditing preliminary recommendation for further details).

Preliminary Recommendation #11. Disclosure Requirement

The EPDP Team recommends that the following requirements are applicable to Contracted Parties and subject to ICANN Compliance enforcement, as well as any automated responses provided by SSAD. For the avoidance of doubt, every response does not have to go through an enforcement procedure; the enforcement mechanism may, however, be triggered in the event of apparent misuse.

Contracted Parties and SSAD:

a) Must only disclose the data requested by the requestor;
b) Must return current data or a subset thereof in response to a request (no historic data);
c) Must process data in compliance with applicable law;
d) Must log requests;
e) Where required by applicable law, must perform a balancing test before processing the data;
f) Must disclose to the Registered Name Holder (data subject), on reasonable request, confirmation of the processing of personal data relating to them, per applicable law;
g) Where required by applicable law, must provide mechanism under which the data subject may exercise its right to erasure and any other applicable rights;

h) 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.
i) Confidentiality of disclosure requests – Upon a request from a data subject the exact processing activities of their data within the SSAD, should be disclosed as soon as reasonably feasible. However the nature of legal investigations or procedures may require SSAD and/or the disclosing entity keep the nature or existence of these requests confidential from the data subject. Confidential requests can be disclosed to data subjects in cooperation with the requesting authority, [and] [or] in accordance with the data subject's rights under applicable law.[11]

Preliminary Recommendation #12. Query Policy

The EPDP Team recommends that the Central Gateway Manager:

a) Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system;
b) May take measures to limit the number of requests that are submitted by the same requestor if it is demonstrated that the requests are of an abusive* nature;

*"Abusive" use of SSAD may include (but is not limited to) the detection of one or more of the following behaviors/practices:

1. High volume automated submissions of malformed or incomplete requests.
2. High volume automated duplicate requests that are frivolous or vexatious.
3. Use of false, stolen or counterfeit credentials to access the system.
4. Storing/delaying and sending high-volume requests causing the SSAD or other parties to fail SLA performance. When investigating abuse based on this specific behavior, the concept of proportionality should be considered.

As with other access policy violations, abusive behavior can ultimately result in suspension or termination of access to the SSAD. In the event the entity receiving requests makes a determination based on abuse to limit the number of requests a requestor, further to point b, the requestor may seek redress via ICANN org if it believes the determination is unjustified. For the avoidance of doubt, if the entity receiving requests receives a high volume of requests from the same requestor, the volume alone must not result in a de facto determination of system abuse.

c) MUST respond only to requests for a specific domain name for which non-public registration data is requested to be disclosed and MUST examine each request on its own merits.

[11] The EPDP Team may reconsider this requirement once there is clarity on who will be the entity disclosing the data.

The EPDP Team recommends the SSAD, in whatever form it eventually takes, MUST:

a) Unless otherwise required or permitted, not allow bulk access, wildcard requests, nor boolean search capabilities.
b) Have the capacity to handle the expected number of requests in alignment with the SLAs established
c) Only return current data (no data about the domain name registration's history);
d) Receive a specific request for every individual domain name (no bulk access);
e) Direct requests at the entity that is determined through this policy process to be responsible for the disclosure of the requested data.

Requests must only refer to current registration data (historical registration data will not be made available via this mechanism).

See also the preliminary recommendation #9 (Acceptable Use Policy).

Preliminary Recommendation #13. Terms of use

The EPDP Team recommends that appropriate agreements, such as terms of use for the SSAD, a privacy policy and a disclosure agreement are put in place that take into account the recommendations from the other preliminary recommendations. These agreements are expected to be developed and negotiated by the parties involved in SSAD, taking the below implementation guidance into account.

Implementation guidance:

Privacy Policy

The EPDP recommends, at a minimum, the privacy policy shall include:

- Relevant data protection principles, for example,
- The type(s) of personal data processed
- How and why the personal data is processed, for example,
    - verifying identity
    - communicating service notices
- How long personal data will be retained
- The types of third parties with whom personal data is shared
- Where applicable, details of any international data transfers/requirements thereof
- Information about the data subject rights and the method by which they can exercise these rights
- Notification of how changes to the privacy policy will be communicated

Further consideration should be given during implementation whether updates to the RAA are necessary to ensure compliance with these recommendations.

Terms of Use

The EPDP recommends, at a minimum, the terms of use shall address:

- Indemnification of the disclosing party and ICANN.
- Data request requirements
- Logging requirements
- Ability to demonstrate compliance
- Applicable prohibitions

Disclosure agreements

The EPDP recommends, at a minimum, disclosure agreements shall address:

- Use of the data for the purpose indicated in the request
- Requirements for use of data for a new purpose other than the one indicated in the request
- Retention of data
- Lawful use of data

Preliminary Recommendation #14. Retention and Destruction of Data

The EPDP Team recommends that requestors must confirm that they will store, protect and dispose of the gTLD registration data in accordance with applicable law. Requestors must retain only the gTLD registration data for as long as necessary to achieve the purpose stated in the disclosure request.

Preliminary Recommendation #15. Financial Sustainability

The EPDP Team recommends that, in considering the costs and financial sustainability of SSAD, one needs to distinguish between the development and operationalization of the system and the subsequent running of the system.

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. 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.

The subsequent running of the system is expected to happen on a cost recovery basis whereby historic costs may be considered. For example, if the SSAD includes an accreditation framework under which users of the SSAD could become accredited, the costs associated with becoming accredited would be borne by those seeking accreditation. Similarly, some of the cost of running the SSAD may be offset by charging fees to the users of the SSAD.

When implementing and operating the SSAD, a disproportionately high burden on smaller operators should be avoided.

The EPDP Team recognizes that the fees associated with using the SSAD may differ for users based on [cost causation].

[Under no circumstances should data subjects be expected to foot the bill for having their data disclosed to third parties; beneficiaries and users of the SSAD should bear the costs of maintaining this system.] <<

The SSAD should not be considered a profit-generating platform for ICANN or the contracted parties. Funding for the SSAD should be sufficient to cover costs, including for subcontractors at market cost and to establish a legal risk fund. It is crucial to ensure that any payments in the SSAD are related to operational costs and are not simply an exchange of money for non-public registration data.

In relation to the accreditation framework:

a) Accreditation applicants may be charged a to-be-determined non-refundable fee proportional to the cost of validating an application.
b) Rejected applicants may re-apply, but the new application(s) may be subject to the application fee.
c) Fees are to be established by the accreditation authority.
d) Accredited users and organizations must renew their accreditation periodically.

Implementation guidance: (associated with disclosure requests):
[Given the number of policy options implicit in the various models, 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 fee structure as well as the renewal period is to be determined in the implementation phase, following the principles outlined above. The EPDP Team recognizes that it may not be possible to set the exact fees until the actual costs are known. The EPDP Team also recognizes that the SSAD fee structure may need to be reviewed over time.

Placeholders

The EPDP Team will further consider whether the resubmission of a request will be treated as a new request from a cost/fee perspective.

The EPDP Team has requested input from ICANN Org concerning the expected costs of developing, operationalizing and maintaining the three different models. Based on the feedback received, the EPDP Team may develop further guidance in relation to the financial sustainability of SSAD.

Commented [MK2]: [awaiting proposed footnote from Brian K.]

Commented [MK3]: Homework: (Amr, Brian, Stephanie & Franck) to clarify intent of statement; the statement intent is on-going maintenance/cost of the system; not to infer a blanket prohibition; (due Monday Jan 20)

Commented [MK4]: Suggestion by Stephanie

Preliminary Recommendation #16. Automation

The EPDP Team acknowledges that full automation of the SSAD may not be possible, but recommends that the SSAD must be automated where technically feasible and legally permissible[12]. Additionally, in areas where automation is not both technically feasible and legally permissible, the EPDP Team recommends standardization as the baseline objective.

For example, the EPDP Team expects that aspects of the SSAD such as intake of requests, credential check, request submission validation (format & completeness, not content) could be automated, while it may not be possible to completely automate all request review and disclosure.

The SSAD must allow for the automation of syntax checking of incoming requests, resulting in an automatic response that indicates the errors to the requestor. This automation addresses the risk of filling up the request queues of the discloser with malformed requests.

The SSAD must allow for the automation of checking that the contents of a request is complete, per policy, resulting in an automatic response that provides details explaining what elements are incomplete. This automation allows for the discloser to indicate - without human intervention - if any additional information is required per policy and enables the requestor to address the error.

The SSAD must allow for the automation of an immediate and synchronous response that indicates the receipt of a valid request and some indication that it will be processed. Typically, such responses include a "ticket number" or some kind of unique ID to allow for future queries (status, updates, deletion, etc.). This automation allows for efficient queue management on the discloser's side and assists in ensuring the principal of "predictability" is met.

The SSAD must allow for automation of the processing of well-formed, valid, complete, properly-identified requests from accredited users with some limited and specific set of legal basis and data processing purposes which are yet to be determined. These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention.

Preliminary Recommendation #17. Logging

The EPDP Team expects that the appropriate logging procedures are put in place to facilitate the auditing procedures outlined in these recommendations. These logging requirements will cover the following:

- Accreditation authority

[12] EPDP Team to revisit this language once the decision of who will be the authorization provider is made.

- Central Gateway Manager
- Identity provider
- Activity of accredited users such as login attempts, queries
- What queries and disclosure decision(s) are made[13]

The EPDP Team recommends:

a) The activity of all SSAD entities will be logged. (for further details, please see the implementation guidance below).
b) Logs will include a record of all queries and all items necessary to audit any decisions made in the context of SSAD.
c) Logs must be retained for a period sufficient for auditing and complaint resolution purposes, taking into account statutory limits related to complaints against the controller.
d) Logs must be retained in a commonly used, structured, machine-readable format accompanied by an intelligible description of all variables.
e) Logged data will remain confidential and must be disclosed in the following circumstances:
    i. In the event of a claim of misuse, logs may be requested for examination by an accreditation authority or dispute resolution provider.
    ii. Logs should be further available to data protection authorities, ICANN, and the auditing body.[14]
    iii. When mandated as a result of due legal process, including relevant supervisory authorities, as applicable.
    iv. General technical operation to ensure proper running of the system.

Implementation guidance:

At a minimum, the following events must be logged

- Logging related to the Identity Provider
- Logging related to the accreditation provider
    - 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 Authorization Credentials have been Validated.
- Logging related to the Central Gateway Manager

[13] Note, EPDP Team to review at a later stage as the ability for SSAD to log this information depends on who is the entity that makes the disclosure decision

[14] Note, EPDP Team to review at a later stage as there is a question of the set up of the system of whether or not the Ry and RR as Controllers (where liability remains with them) may require access to the logs for them to engage in audit, or answer Data Subject requests.

- 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)

- Logging related to the entity Authorizing the request
  - Request Response details, e.g., Reason for denial, Notice of approval and data elements released.

Preliminary Recommendation #18. Audits

The EPDP Team expects that the appropriate auditing processes and procedures are put in place to ensure appropriate monitoring and compliance with the requirements outlined in these recommendations.

As part of any audit, the auditor MUST be subject to reasonable confidentiality obligations with respect to proprietary processes and personal information disclosed during the audit.

More specifically:

Audits of the Accrediting Authority

If ICANN outsources the accreditation authority function to a qualified third party, the accrediting authority MUST be audited periodically to ensure compliance with the policy requirements as defined in the accreditation preliminary recommendation. Should the accreditation authority be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure, a new accreditation authority must be identified or created.

Any audit of the accreditation authority shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data, and other information requested.

As part of such audits, the accreditation authority shall provide to the auditor in a timely manner all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

If ICANN serves as the accreditation authority, existing accountability mechanisms are expected to address any [policy] breaches, noting that in such an extreme case, requirements for other entities involved in SSAD may be temporarily lifted until a confirmed breach has been addressed.

[If ICANN serves as the accreditation authority, existing accountability mechanisms are expected to address any breaches of the accreditation policy, noting that in such an extreme

case, the credentials issued during the time of the breach will be reviewed. Modalities of this review should be established in the implementation phase.]

[…that any SSAD users accredited during the period of the breach need to have their access to SSAD temporarily suspended until the breach is addressed.]

[There needs to be a concept of causality and proportionality between the breach (eg size, how bad) and the consequences.] << Franck suggestion

Audits of Identity Provider(s)

Identity Providers MUST be audited periodically to ensure compliance with the policy requirements as defined in the accreditation preliminary recommendation. Should the Identity Provider be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure, a new Identity Provider must be identified.

Any audit of an Identity Provider shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested.

As part of such audits, the Identity Provider shall provide to the auditor in a timely manner all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

Audits of Accredited Entities/Individuals

Appropriate mechanisms must be developed in the implementation phase to ensure accredited entities' and individuals' compliance with the policy requirements as defined in the accreditation preliminary recommendation. These could include, for example, audits triggered by complaints, random audits, or audits in response to a self-certification or self-assessment. Should the accredited entity or individual be found in breach of the accreditation policy and requirements, it will be given an opportunity to cure the breach, but in cases of repeated non-compliance or audit failure the matter should be referred back to the Accreditation Authority and/or Identity Provider, if applicable, for action.

Any audit of accredited entities/individuals shall be tailored for the purpose of assessing compliance, and the auditor MUST give reasonable advance notice of any such audit, which notice shall specify in reasonable detail the categories of documents, data and other information requested.

As part of such audits, the accredited entity/individual shall, in a timely manner, provide to the auditor all responsive documents, data, and any other information necessary to demonstrate its compliance with the accreditation policy.

Commented [MK5]: Janis proposal

Commented [MK6]: Amr suggestion to proposal

Commented [MK7]: Franck suggestion

Audits of the Central Gateway Manager & Contracted Parties

The EPDP Team will further consider these requirements once the EPDP Team has decided on the roles and responsibilities of the different parties in the SSAD.

NOTE: Depending on the ultimate SSAD model the EPDP Team recommends, there may be other relevant parties that would be subject to auditing. This will be revisited when the ultimate SSAD model is recommended.

[If ICANN serves as the accreditation authority, existing accountability mechanisms are expected to address any breaches of Registration Data held by ICANN in the SSAD. If such a breach is confirmed, Contracted Parties may withhold Registration Data from the SSAD until the Office of the Chief Technology Officer (OCTO) has confirmed that the breach has been remediated. In the event that such a breach has not been remediated, or is not expected by OCTO to be remediated within seven (7) days, a new SSAD provider should be brought online as quickly as possible but not longer than thirty (30) days from the date of identification of the breach.]

Commented [MK8]: Suggestion from Brian

Preliminary Recommendation #19. SSAD Advisory Group

In conjunction with the implementation of these recommendations, the EPDP recommends the creation of an SSAD Advisory Group (the "Advisory Group"). The Advisory Group will have the responsibility to provide advice to ICANN Org and Contracted Parties on the following topics:

a) SLA matrix review;
b) Categories of disclosure requests which should be automated;
c) Other implementation improvements such as the identification of possible user categories and/or disclosure rationales.

Upon receipt of the advice from the Advisory Group, ICANN Org and Contracted Parties will meet virtually to review the advice and discuss if/how this advice can be implemented. ICANN Org and Contracted Parties will report back to both the Advisory Group and the GNSO Council on how the advice was considered and what next steps, if any, are expected to be taken in response to the advice.

The Advisory Group may also make recommendations to the GNSO Council for any policy issues that may require further policy work.

The members of the Advisory Group commit to working in good faith towards the goals outlined in these policy recommendations.

A detailed charter for the SSAD Advisory Group is expected to be developed during the implementation phase of these policy recommendations.

To begin, the EPDP Team recommends the Advisory Group to meet virtually at least every six months for the first two years following the implementation of the SSAD.

SSAD Implementation Guidance

Implementation Guidance #i.
The EPDP Team recommends that, consistent with the preliminary recommendation that an SSAD request must be received for each domain name registration for which non-public registration is requested to be disclosed, it must be possible for requestors to submit multiple requests at the same time, for example, by entering multiple domain name registrations in the same request form if the same request information applies.