**Recommendation 13: Terms of Use**

Based on the staff support team review of the feedback provided by the different groups by the deadline on the discussion table, the following topics / issues are being put forward for discussion during Thursday’s meeting. The input on these topics / issues, as well as non-controversial changes identified or where responses were aligned in the discussion table, will be used to develop a next iteration of the recommendation text for EPDP Team review. Note, known concerns, which have been considered and discussed previously have not been included and will not be discussed again unless new information has been provided.

**Assumptions / Takeaways:**

* This recommendation should be coordinated with the references to the code of conduct in Rec. 1, query policy, data retention, acceptable use policy recommendations to avoid duplication.
* The principles and disclosures listed under “Policy for SSAD Users” should be mirrored and made clear to registrants in their registration agreements.
* The Privacy Policy for SSAD users says “The types of third parties with whom personal data is shared”; this should include the fact that data subjects will be provided with contact information for the parties that requested and received their data, according to applicable law.
* Based on yesterday’s discussion, we assume data subjects are not intended to be accredited users of the SSAD. Instead, they would go the registrar directly to confirm their data.

**Additional questions for EPDP Team:**

1. The EPDP team should clarify in the implementation guidance if the SSAD users are meant to be the Requestors, the Contracted Parties, or any party to the SSAD as a whole. Is it correct to assume in this context “SSAD users” was intended to mean “Requestors”?
2. The first paragraph notes that agreements are expected to be developed and negotiated by the parties involved in the SSAD. Is this intended to include ICANN, the Accreditation Authority, Identity Providers, Contracted Parties, users, and requestors? Note: some commenters expressed concerns with including requestors and data subjects in these negotiations. (Note: implementation guidance in the updated Rec. 11 provides: ICANN Org will develop the SSAD Privacy Policy for SSAD users, which it may publish for public comment to obtain input from potential SSAD users.)

**Privacy Policy**

1. Should “The EPDP recommends, at a minimum, the privacy policy **SHALL** include (…)” be changed to “The EPDP recommends, at a minimum, the privacy policy **SHOULD** include?
2. There is a proposal to add the following bullets to the list for the privacy policy for SSAD users:
   * Transparency requirements
   * Data security requirements
   * Accountability measures (privacy by design, by default, DPO above certain size, etc)

Does the EPDP Team agree to these additions?

1. “The EPDP recommends, at a minimum, the privacy policy SHALL include: Relevant data protection principles, for example,” This sentence appears to abruptly cut off - were there supposed to be particular examples listed here? If so, what should be included here, or should the “for example” be removed and this left to implementation?
2. “Further consideration should be given during implementation whether updates to the RAA are necessary to ensure compliance with these recommendations.” Should this sentence be removed? If not, can the EPDP team clarify which recommendations they are referring to here and if this is specific to the terms of use or a blanket recommendation?

**Terms of Use**

1. Should “The EPDP recommends, at a minimum, the terms of use **SHALL** include (…)” be changed to “The EPDP recommends, at a minimum, the terms of use **SHOULD** include?
2. The first bullet in this section states that the Terms of Use shall address indemnification of the controllers. The EPDP team should clarify which party is responsible to indemnify whom, as well as who is being referenced as the “controller.”
3. The bullets under the terms of use seem to be a mix of liability considerations and rules. Was this intended by the EPDP team?

**Disclosure Agreement**

1. Can the EPDP team confirm and clarify if the last 4 bullets of this recommendation are requirements for Contracted Parties or requestors?

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 for SSAD Users

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 for SSAD users

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

* Indemnification of the controllers based on the following principles:
  + Requestors are responsible for damages or costs related to third party claims arising from (i) their misrepresentations in the accreditation or request process; or (ii) misuse of the requested data in violation of the applicable terms of use or applicable law(s).
  + Nothing in these terms limits any parties’ liability or rights of recovery under applicable laws (i.e. requestors are not precluded from seeking recovery from controllers where those rights are provided under law).
  + Nothing in these terms shall be construed to create indemnification obligations for public authority requestors who lack the legal authority to enter into such indemnification clauses. Further, nothing in this clause shall alter potentially existing government liability as a recourse for the operators of the SSAD.
* Data request requirements
* Logging requirements
* Ability to demonstrate compliance
* Applicable prohibitions

Disclosure agreements for SSAD users

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