Recommendation #11 – Disclosure Requirements

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 to factor into updated recommendation:

- This recommendation describes how disclosure happens once the decider has performed its review – it is not about compelling disclosure.
- Logging requirements are dealt with in the logging recommendation.
- Requirements in relation to disclosure of non-personal data will be aligned with how this is addressed in recommendation #6 – note that the EPDP Phase 1 recommendations allow, but do not require CP to distinguish between legal and natural persons. Note that bullet e) does specify that 'where required by applicable law'.
- It is not the EPDP Team's role to determine what applicable law is – that will be up to the parties involved in SSAD.
- In f) the reference to applicable law covers requests that are to be treated confidentially such as LEA requests or other non-LEA requests.
- Right to erasure does not overwrite data retention requirements that CPs have.

Additional questions for EPDP Team:

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.

1. The introduction paragraph notes that the disclosure requirements "are applicable to Contracted Parties and subject to ICANN Compliance enforcement, as well as any automated responses provided by SSAD." Does this mean that all parties to the SSAD must comply with disclosure requirements if approved for automated disclosure?
2. Should it be clarified who can trigger the enforcement mechanism and what the enforcement mechanism should look like, or is this an implementation question?

a) MUST only disclose the data requested by the requestor;

3. There is support for the following changes, but clarification has been asked about whether the first option implies that the CP may include additional data which was not requested?
   Option 1: ~~MUST~~ **MAY** ~~only~~ disclose the data requested by the requestor**, adding data at the Contracted Party's discretion or omitting data. (as stated above, with a reason for the omission).**
   Option 2: ~~MUST~~ **MAY** ~~only disclose the~~ **return current** data ~~requested by the requestor~~ **or a subset thereof; if data are omitted, a reason MUST be provided. Contracted Party need not provide a reason for returning additional data.**

b) MUST return current data or a subset thereof in response to a request (no historic data);

4. Has the EPDP team considered what should happen if registration data changes between the time a request for disclosure is received and when a request is evaluated? Would the changed data be considered historic data if returned once the data changed? Could this be addressed if the Contracted Party were to notify the requestor that the data has changed since the request was filed? Has the EPDP team considered how to address domain names that have expired or transferred since submitting the request? Note that the following additional text was put forward by another commenter to avoid potential changes: "**The domain name that is the subject of a disclosure request shall be locked (using the UDRP definition) during the pendency of a disclosure request.**".

   - Note: EPDP Team Members registered no objections to the following text: Update b) MUST return current data or a subset thereof **which is current at the time a request is processed** ~~in response to a request~~ (no historic data); (note, original edit also deleted 'no historic data' but there was no support for that change).
     Does this need to be updated in light of the above discussion?

Contracted Parties and SSAD
e) Where required by applicable law, MUST perform a balancing test before processing the data;

5. Stating that Contracted Parties and SSAD "[w]here required by law, MUST perform a balancing test before processing the data" rules out any automation requiring a 6(1)(f) balancing. A strict reading of this would mean that any automation of a disclosure requiring a balancing test would violate the disclosure requirements and be subject to ICANN Compliance enforcement. How can this be clarified?

Contracted Parties and SSAD
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;

6. The following edit was put forward "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. **The CP may not pro-actively inform, or offer to pro-actively inform, registrants of disclosure requests once it has received them. The CP may not condition its approval of a disclosure request to the registrant's consent, or absence of objection, to the request.**" but some noted that this addition might prevent a contracted party from following applicable law. Should this change be considered or not?

7. The following edit was put forward "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 **without disclosing the identity of the requestor**" but some noted that this addition might prevent a contracted party from following applicable law. Should this change be considered or not?
8. Is there a need for a requirement to notify parties whose data has been disclosed or is this only upon request?

Contracted Parties and SSAD
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;

9. A commenter noted that this is a redundant restatement of what the law actually states. Additionally, the SSAD and the rules surrounding it, should not even attempt to dictate the manner in which a controller meets their legal obligations. This serves nothing but to greatly increase the liability of that body that is tasked with enforcement of this policy. Is this requirement necessary or can it be deleted?

Contracted Parties and SSAD
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. Notwithstanding obligations on the Contracted Parties under applicable law, ICANN and the Contracted Parties will draft and agree upon a privacy policy for the SSAD and standard language (relating to the SSAD) to inform data subjects according to Art. 13 and 14 GDPR (or any other relevant obligations), to be presented to data subjects by the Registrars. This will contain information on potential recipients of non-public registration data including, but not limited to the recipients listed in Preliminary Recommendation #4 Third Party Purposes / Justifications, as legally permissible. Information duties according to applicable laws may apply additionally, but the information referenced above must be contained as a minimum.

10. Some commenters suggested that all SSAD stakeholders should be involved in drafting and agreeing up on a privacy policy for the SSAD and standard language to inform data subjects, but others pointed out that contract language is determined by the parties in the contract. Could a possible compromise be 'ICANN and the Contracted Parties will **solicit and factor in input from all SSAD stakeholders when** draft**ing** and agree**ing** upon a privacy policy for the SSAD and standard language (relating to the SSAD) to inform data subjects (…)'?
11. The EPDP team should clarify who the privacy policy is intended to cover (registrants, requestors, others)?

Contracted Parties and SSAD
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.

12. The following edit was proposed, but some expressed concern that it will be nearly impossible to expand this language to include other types of investigations that could be subject to confidentiality, so limiting to governmental agencies is the only way to address at this time.
    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 **in accordance with applicable law** ~~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 **entity** ~~authority~~, [and] [or] in accordance with the data subject's rights under applicable law. **Note, the nature of legal investigations or procedures:**
    - **are not limited to criminal investigations or to other investigations (e.g. many civil investigations require confidentiality);**
    - **are not limited to investigations by governmental agencies (most civil investigations are conducted by private parties.**
13. A commenter expressed concern that this is in direct contravention to applicable law. "For example, the GDPR requires disclosure without the data subject's explicit request in the event that third parties have received a data subject's personal data. In addition, confidentiality of requests may be reasonable and may be granted but must be reviewed in each case, similar to the review of a disclosure request itself. Where the Contracted Party determines that the confidentiality request is not valid or is being abused (AUP might help here), the Contracted Party may be required by local law to disclose to the data subject as usual, regardless of whether or not the requestor agrees". Should a reference be added that this is subject to applicable law?
14. There is still bracketed language in this section. How should it be updated?

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. Notwithstanding obligations on the Contracted Parties under applicable law, ICANN and the Contracted Parties will draft and agree upon a privacy policy for the SSAD and standard language (relating to the SSAD) to inform data subjects according to Art. 13 and 14 GDPR (or any other relevant obligations), to be presented to data subjects by the Registrars. This will contain information on potential recipients of non-public registration data including, but not limited to the recipients listed in Preliminary Recommendation #4 Third Party Purposes / Justifications, as legally permissible. Information duties according to applicable laws may apply additionally, but the information referenced above must be contained as a minimum.
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.[18]