Recommendation #8 – Response 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.

For the Central Gateway Manager:

a) *Following receipt of a disclosure request, the Central Gateway Manager MUST confirm[1] 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.*

Takeaways to factor into updated recommendation:

- Many commenters noted these requirements should be folded into Recommendation 5, as they deal with the acknowledgement of receipt.
- Acknowledgement of receipt should include a ticket number for reference – should be included in updated Rec. 5.

Additional questions for EPDP Team:

1. Regarding "relay the disclosure request to the responsible Contracted Party," the EPDP Team needs to discuss further whether the disclosure request is only relayed to the registrar and/or in which circumstances it may be related to the registry. It has been suggested that the request must always be forwarded to the REGISTRAR, and if the registrar does not respond by the SLA or there are specific circumstances that make it impossible to relay the request to the registrar, the request could be forwarded to the Registry by the Central Gateway Manager. However, if the Registrar denies the request, the requestor cannot forward the request to the registry.

---

[1] 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.

2. Paragraph b) states that the "the Central Gateway Manager MUST...relay the disclosure request to the responsible Contracted Party, if it does not concern a request that meets the criteria for automatic disclosure." ICANN org understands that all requests that meet the criteria for automatic disclosure must also be relayed to the responsible Contracted Party in a similar manner to non-automated requests – is this understanding correct? If so, should it also include a confirmation / check of how the criteria were met? In addition, what, specifically, must be relayed to the Contracted Party? Is this all information included in a request, or some subset of that information? Is the same information required to be relayed for automated and non-automated requests?

For the Central Gateway Manager:

c) *As part of its relay to the responsible Contracted Party, the Central Gateway Manager MAY 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 MUST communicate its reasons for not following the Central Gateway Manager recommendation so the Central Gateway Manager can learn and improve on future response recommendations.*

Takeaways to factor into updated recommendation:

- Any recommendation from the Central Gateway Manager is optional for the Contracted Party to follow

Questions and Considerations for the EPDP Team:

3. Many commenters were confused about the utility of the Central Gateway Manager's recommendation:
   o Is the recommendation envisioned to be automatic or manual?
   o How would the Central Gateway Manager go about making a recommendation?
   o There is disagreement about if the Contracted Party should be required to send its rationale for denying the request to the Central Gateway Manager – note, that this is a compromise that was previously agreed by the EPDP Team to allow the Central Gateway Manager to learn and improve its 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 MUST 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 access/disclosure request MUST include information on how public registration data can be obtained.***

Takeaways for drafting updated recommendation:

- References to SLA should be handled separately within the SLA recommendation. There is still confusion regarding how SLAs will be enforced and how these will be developed. The EPDP Team can discuss Rec. 9 further, following updated guidance from Volker and Mark SV.
- For the purposes of evolving the SSAD, as well as to ensure centralized logging, all decisions (i.e. at a minimum whether or not the Contracted Party discloses) should be logged with the Central Gateway Manager. (to be included in the Logging Recommendation)
- There is disagreement regarding the following sentence in d): *Such exceptional circumstances MAY include the overall number of requests received if the number far exceeds the established SLAs.* Note, there is language in other recommendations that addresses potential abuse of SSAD. Consider adding a footnote/explanatory text and discussing abusive use of SSAD in Recommendation 12 (query policy).

Further discussion needed on:

4. Is an appeals mechanism necessary for requestors who would like to appeal the decision of a contracted party? Or are existing mechanisms, such as filing a complaint with the relevant data protection authority or via other relevant legal process/existing dispute mechanisms sufficient? If an appeals mechanism is deemed necessary, who would be the decider?
5. If a disclosure request is rejected by a Contracted Party, should ICANN Compliance be notified about this rejection? If yes, what information would be required to be provided?
6. There is disagreement on the following text in e): "including, for example, an analysis and explanation of how the balancing test was applied (if applicable)." Some commenters believe this should be removed because the determination should be lightweight to avoid including personal information, while others agree it should remain. Note, this sentence included 'for example' and (if applicable) to make clear that this is not a requirement but could be the type of information that may help the requestor understand the rationale for the decision.
7. Regarding the text, "Additionally, in its response, the entity receiving the access/disclosure request MUST include information on how public registration data can

be obtained," a Contracted Party may be unaware of every source where the specifically-requested public data is available. Could this be changed to a MAY? Or, alternatively, could the CGM provide a message to requestors, noting how to access public information via RDAP? Additionally, if a requestor is repeatedly using the SSAD to obtain information that is available elsewhere, is that abusive behavior?

Urgent SSAD Requests

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. Note that the use of 'Urgent' SSAD Requests is not limited to LEA.*

g. *Abuse of urgent requests: Violations of the use of Urgent SSAD Requests will result in a response from the Central Gateway Manager to ensure that the requirements for Urgent SSAD Requests are known and met in the first instance, but repeated violations may result in the Central Gateway Manager suspending the ability to make urgent requests via the SSAD. Contracted Parties 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 in the SSAD portal (or in another standardized place that may be designated by ICANN from time to time).*

Takeaways for drafting updated recommendation:

- Urgent requests should be included in a separate recommendation to avoid confusion
- Contracted parties should have the ability to challenge a requestor's assertion of an urgent request – note: this was previously addressed in Rec. 9 (SLA discussion).
- Following the discussion on Rec. 9, it has been suggested that urgent requests (Priority 1) would be limited to approved governmental authorities; accordingly, the following sentence would need to be removed, if the suggestion is followed: *Note that the use of 'Urgent' SSAD Requests is not limited to LEA.* For reference, the relevant section of Rec. 9 current reads: This priority code can only be used by accredited governmental entities. If an accredited non-governmental requestor believes its disclosure request(s) that meets these criteria, it MAY contact the accredited governmental entity within its jurisdiction, who would have the authority to submit the disclosure request(s), should it choose to do so. Persistent abuse of this priority code can result in the requestor's de-accreditation.

Further discussion needed on:

8. The Team struggled to draft an agreeable definition of urgent request. Could the Team consider keeping the current definition and providing a non-exhaustive list of examples to assist policy implementation and contracted parties and requestors who are closely involved with the EPDP's work? (To be discussed in conjunction with implementation guidance d, which provides comments examples of critical infrastructure – see comment oo.)

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 MAY be filed with ICANN Compliance. ICANN Compliance should be prepared to investigate complaints regarding disclosure requests under its enforcement processes.

Takeaways for drafting updated recommendation:

- Consider moving the first paragraph to the Contracted Parties section, as it appears out of place as a standalone paragraph.
- Requestors MAY file complaints if they believe responses were denied erroneously, and ICANN org MUST investigate complaints regarding disclosure requests, not just be prepared to investigate.
- ICANN org has noted the following it anticipates reviewing compliance with the following:
  - response adhered to established SLAs;
  - response included all required content (i.e. denial communicated without disclosure of personal data, rationale for the decision, and (if applicable) how the Contracted Party applied the balancing test);
  - request was reviewed based on its individual merits; and
  - disclosure was not 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; or 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 (absent any legal requirements to the contrary);
- ICANN Compliance will not be in a position to address the merits of the request itself or the legal discretion of the Contracted Party making the determination.

Implementation Guidance:
a) The Central Gateway Manager MUST confirm that the request is syntactically correct, including proper and valid Authentication and Signed Assertions. 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[2] includes, amongst others, root servers; examples of offline critical infrastructure includes, amongst others, utilities, transportation and banking.*

Takeaways for drafting updated recommendation:
- Implementation guidance a and b are duplicative, as they are already covered in Rec. 5 – Acknowledgement of Receipt.
- c) will be addressed in updated Rec. 5, as referenced in the comments discussed in 8(a) and 8(b). The word "typically" will be removed in the addition.

---

[2] For further information, see for example https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC