Recommendation #6 – Contracted Party Authorization

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:

- Where further detail is requested on specific provisions that overlap with other recommendations, the details will be covered in the most appropriate recommendation. Specifically, further details on automation will be covered in Rec. 16, the concept of trusted notifiers will be covered in Rec. 8, and further details on contracted party routing was covered in discussions on Rec. 8.
- CPs are NOT preemptively judging a legal claim in their assessment on whether to disclose or not.
- Non-personal data is not protected and should be disclosed – if a CP confirms a request concerns non-personal data, there is no need to examine the lawful basis and legitimate interest of the requestor.
- Change '*The Contracted Party ~~MAY~~ **MUST** evaluate the underlying data requested' and* '*The Contracted Part ~~SHOULD~~ **MUST** make a threshold determination'.* Also consider whether re-ordering is helpful because if CP makes a determination that it concerns non-personal data, the different steps do not need to be followed.
- Support Staff will apply proposed edits to which no concerns were expressed.

Additional questions for EPDP Team:

1. *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.*

1. Should the policy recommendation contain further information about which third-party providers that may be used and which criteria they should meet, or is this left for implementation and/or Contracted Party determination?

2. *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.*

3. The Contracted Party SHOULD make a threshold determination (without considering the underlying data) about whether the requestor has established an interest in the disclosure of personal data. The determination SHOULD consider the elements:

- *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.*
    - *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.*

2. Re. #3, should Contracted Party be changed to 'Controller'? If updates are made, should this apply to the whole recommendation? Alternatively, would 'Contracted Party Controller' work? Do note that the recommendation itself is titled Contracted Party Authorization.
3. Should 'provided' be changed to 'demonstrated' in the first bullet under #4 so it would read 'has the requestor ~~provided~~ **demonstrated** a legitimate interest or other lawful basis in processing the data?
4. 'The determination SHOULD consider the elements' – how can inconsistent interpretations be avoided of what requestors must provide? Is there any further guidance that can be provided here?
5. *'Necessary means more than desirable but less than indispensable or absolutely necessary'* – can further details be provided on how this would be enforced from a compliance perspective?

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 bullet #5 below.

6. If the Contracted Party denies the request, should there be an ability for the requestor to appeal? If yes, what would such an appeal look like and who would be the arbiter?
7. Should requestors first have the opportunity to provide further information before the CP may deny the request?
8. What implementation guidance should be provided in relation to questions such as 'must Contracted Parties go back to the Central Gateway to request more information' or 'must the Contracted Parties directly interact with the requestor? Additionally, how would such an interaction take place if the Contracted Parties have not already established a relationship with the requestor? Does the EPDP team envision there would be an open ticket with the requestor at the gateway?

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.

9. Some commenters have suggested that this text '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', may limit the CP's discretion and deals with content which should not be addressed by the Registrar/Registry – how can this concern be addressed?

4. The Contracted Party MAY evaluate the underlying data requested once the validity of the request is determined under bullet point #4 above. 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 is required, and the non-personal data MUST be disclosed.

10. Some commenters are of the view that the requirement to disclose non-personal data conflicts with the EPDP Phase 1 recommendation which allowed Contracted Parties to decide whether or not to distinguish between natural and legal persons. Should 'MUST' be changed to 'MAY'?

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. Whenever the circumstances of the disclosure request or the nature of the data to be disclosed suggest an increased risk 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.*

11. Should the list also include: "the controller MUST consider whether the data is covered by applicable law"?
12. Scope of processing: Unclear on how combination with other data presents a higher risk. The EPDP team should clarify.
13. Status of the data subject: it is unclear whether minors can register domain names. Even if so, further examples of "other protected classes" should be presented. This information would not necessarily be available to the Contracted Party. Consider whether further clarifications can be provided if/when this criteria would be applicable?
14. Status of the controller and data subject: Could the EPDP team clarify if this is referring to the relationship between a contracted party and registrant, the data subject and requestor, or another relationship?
15. Should further details be provided under what is covered as part of assessment of impact, such as human rights impact, or would that require the inclusion of all possible impacts?

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 MUST 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.

16. Should the recommendation be clearer on the specific criteria that must be applied when this test is conducted, so that any dispute regarding a contracted party's application of this test can be objectively evaluated?
17. Should this text be clarified as follows: '*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~~* ***should*** *be denied'?*

5. The application of the balancing test and factors considered in bullet point #5 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.

18. Should the Mechanism for the Evolution of SSAD develop, and suggest to requestors, model language for each of the elements of a SSAD request*?*

19. It would be helpful to understand the expected process for such revisions to occur. Is this intended as a task for Contracted Parties, as this is the "Contracted Party Authorization" recommendation? Would such revisions be limited to how Contracted Parties apply the test, or would ICANN org or the GNSO be expected to change the policy to account for these? ICANN org understands the use of SHOULD to mean that no revisions would be required based on case law or guidelines issued by data protection authorities. If this is not the intention, this section could be clarified.

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.*

20. Would it be acceptable to change 'an interest is generally legitimate' to 'an interest is generally **deemed** legitimate? Some expressed support for adding deemed while others noted their interest in retaining the word 'generally'.
21. Should '(iv) IP infringements' be added to examples of legitimate interests? Some have indicated that this is already covered under (i). Could a compromise be to change this to '(i) enforcement of legal claims, **including IP infringements**'?
22. A commenter noted that 'an interest is generally legitimate so long as it can be pursued consistent with data protection and other laws: this presumes legitimacy rather than allowing the determination to rest upon the merits. Where personal data are concerned, privacy should be the presumption and only if the legitimate legal purpose in violating that privacy is sufficient should disclosure be made. The Preliminary Recommendation has this backwards'. Are any updates necessary to address this comment?

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 considering the underlying data) about whether the requestor has established an interest in the disclosure of personal data. The determination SHOULD consider the elements:*
   - *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.*
     - *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 bullet #5 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 bullet point #4 above. 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 is required, and the non-personal data MUST be disclosed.*
   - *The applicable lawful basis and whether the requested data contains personal data for the Contracted Party to determine if the balancing test, similar to the requirements under GDPR's 6.1.f, and as described in the paragraph 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. Whenever the circumstances of the disclosure request or the nature of the data to be disclosed suggest an increased risk 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 MUST 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.

6. *The application of the balancing test and factors considered in bullet point #5 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

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.*