**Recommendation #8 - Contracted Party Authorization.**

*For clarity, this recommendation pertains to disclosure requests that are routed to the Contracted Party for review. These requirements DO NOT apply to disclosure requests that meet the criteria for automated processing of disclosure decisions as described in recommendation #9, regardless of whether automated processing of disclosure decisions is mandated or at the request of the Contracted Party.*

**General requirements**

The Contracted Party

8.1. MUST review every request individually and not in bulk, regardless of whether the review is done automatically or through meaningful review and MUST NOT disclose data on the basis of accredited user category alone.

8.2. 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.

8.3. MUST determine its own lawful basis for the processing related to the disclosure decision.[1] The Requestor will have the ability to identify the lawful basis under which it expects the Contracted Party to disclose the data requested; however, in all instances where the Contracted Party is responsible for making the decision to disclose, the Contracted Party MUST make the final determination of the appropriate lawful basis.

8.4. MUST support reexamination requests received from requests via the SSAD system and MUST consider them based on the rationale provided by the Requestor. For clarity, the resubmission of a disclosure request that is identical to the original request, without a supporting rationale as to why the request must be reconsidered, does not need to be reconsidered by the Contracted Party.

8.5. Absent any legal requirements to the contrary, disclosure MUST NOT 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.

**Authorization determination requirements**

Following receipt of a request from the Central Gateway Manager, the Contracted Party:

8.6. MUST conduct a prima facie[2] review of the request's validity, i.e., is the request sufficient for the Contracted Party to ground a substantive review and process the

[1] See also implementation guidance #17.
[2] Per the Cambridge Dictionary, at first sight (based on what seems to be the truth when first seen or heard).

associated underlying data. If the Contracted Party determines that the request is not valid, e.g. it does not provide sufficient ground for a substantive review of the underlying data, the Contracted Party MUST request the Requestor to provide further information prior to denying the request;

8.7. If the request is deemed valid based on the prima facie review, MUST conduct a substantive review of the request and the underlying data:

8.7.1. If, following the evaluation of the underlying data, the Contracted Party determines that disclosing the requested data elements would not result in the disclosure of personal data, the Contracted Party MUST disclose the data, unless the disclosure is expressly prohibited under applicable law.[3] For clarity, if the disclosure would not result in the disclosure of personal data, the Contracted Party does not have to further evaluate the request.

8.7.2. If following the evaluation of the underlying data, the Contracted Party determines that disclosing the requested data elements would result in the disclosure of personal data, the Contracted Party MUST determine, at a minimum, as part of its substantive review of the request and the underlying data:

8.7.2.1 whether the Contracted Party has a lawful basis for disclosure;[4]
8.7.2.2 whether all the requested data elements are necessary;[5]
8.7.2.3 whether balancing or review is required ~~under applicable law~~.

8.8. If the request is subject to balancing or review as per paragraph 8.7.2.3.:

8.8.1 MUST disclose the data if, based on its evaluation, 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 Contracted Party MUST document the rationale for its approval.

8.8.2 MUST deny the request, if, based on its evaluation, 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 Contracted Party MUST document the rationale for its denial and MUST communicate the reason for denial to the Central Gateway Manager, with care taken to ensure no personal data is included in the reason for denial.

8.9. If the request is not subject to balancing or review as per paragraph 8.7.2.3.:

8.9.1 MUST disclose if the Contracted Party determines it has a lawful basis or is not prohibited under applicable law to disclose the data. The Contracted Party MUST document the rationale for its approval.

---

[3] When considering the publication of non-public data of legal persons, particularly with respect to NGOs and parties engaged in human rights activities that may be protected by local law (e.g. Constitutional and Charter Rights law), the Contracted Party should consider the impact on individuals that could potentially be identified by disclosing the legal person data.

[4] See also implementation guidance #17

[5] For further context regarding the definition of necessary, please refer to p. 7 of the legal guidance the EPDP Team referenced when formulating this definition.

8.9.2 MUST deny the request if the Contracted Party determines it does not have a lawful basis or is prohibited under applicable law to disclose the data. The Contracted Party MUST document the rationale for its denial and MUST communicate the reason for denial to the Central Gateway Manager, with care taken to ensure no personal data is included in the reason for denial.

The Requestor:

8.10. MAY file a reexamination request if it believes its request was improperly denied.

8.11. MUST, within its reexamination request, provide a supporting rationale as to why its request must be reexamined. The supporting rationale should provide sufficient detail as to why the Requestor believes its request was improperly denied.

8.12. If a Requestor believes a Contracted Party is not complying with any of the requirements of this policy, the Requestor SHOULD notify ICANN Compliance further to the alert mechanism described in Recommendation #5 – Response Requirements.

**Implementation Guidance**

8.13. The EPDP Team envisions the Contracted Party having the ability to communicate with the Requestor via a dedicated ticket in the SSAD. The EPDP Team also envisions the SSAD offering encryption to protect the transmission of personal data.

8.14. The EPDP Team notes the specifics of how the communication in paragraph 8.6 will be assessed in the policy implementation phase; however, the EPDP Team provides this additional guidance to assist. The EPDP Team envisions the Contracted Party sending a notice to the Requestor, via the relevant SSAD ticket, noting its decision to deny the request. The Requestor would then have (x) amount of days to provide updated information to the Contracted Party. Upon the Requestor's provision of updated information, the SLA response time would reset. For example, the Contracted Party would have 1 business day to respond to the updated urgent request. If the Requestor chooses not to provide the information, the SLA would be counted when the Contracted Party sends the "intent to deny" notice to the Requestor. If the Requestor decides not to respond, the request is denied as soon as the time period has expired.

8.15. In situations where the Contracted Party is evaluating the legitimate interest of the Requestor, the Contracted Party SHOULD consider the following:

8.15.1 Interest must be specific, real, and present rather than vague and speculative.

8.15.2 An interest is generally deemed legitimate so long as it can be pursued consistent with data protection and other laws.

8.15.3 Examples of legitimate interests include: (i) enforcement, exercise, or defense of legal claims, including IP infringement; (ii) prevention of fraud and misuse of services; (iii) physical, IT, and network security.

8.16. The Contracted Party SHOULD[6], as part of its substantive review, assess at least:

8.16.1 Where applicable, the following factors should be used 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 Contracted Party SHOULD consider the totality of the circumstances outlined below:

8.16.1.1 *Assessment of impact*. Consider the direct impact on data subjects as well as any broader possible consequences of the data processing. Consider the public interest and legitimate interests pursued by the Requestor to, for example, maintain the security and stability of the DNS. 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.

8.16.1.2 *Nature of the data.* Consider the level of sensitivity of the data as well as whether the data is already publicly available.

8.16.1.3 *Status of the data subject.* Consider whether the data subject's status increases their vulnerability (e.g., children, asylum seekers, other protected classes)

8.16.1.4 *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),[7] provided that this is not intended to prohibit public disclosures for legal actions or administrative dispute resolution proceedings such as the UDRP or URS.

8.16.1.5 *Reasonable expectations of the data subject.* Consider whether the data subject would reasonably expect their data to be processed/disclosed in this manner.

8.16.1.6 *Status of the controller and data subject.* Consider negotiating power and any imbalances in authority between the controller and the data subject.[8]

---

[6] ICANN org would review compliance with the following: a) response adhered to established SLAs; b) response included all required content (i.e. denial communicated without disclosure of personal data, rationale for the decision, and (if applicable) whether the Contracted Party applied the balancing test); c) request was reviewed based on its individual merits; and, d) absent any legal requirements to the contrary, disclosure was not refused solely for lack of any of the following: (i) a court order; (ii) a subpoena; (iii) a pending civil action; (iv) a UDRP or URS proceeding; or (e) denials where the registration data does not include personal information. Note, (e) shall neither predetermine nor contradict any outcome of the legal / natural discussion, the result of which shall prevail this clause. Typically, ICANN Org will not be in a position to address the merits of the request itself or the Contracted Party's conclusions, if applicable, in balancing the rights of the data subject with the legitimate interests of the requester. For avoidance of doubt, this does not preclude ICANN Org from addressing complaints related to allegations of unreasonable denials of requests to disclose data, especially where there is evidence of widespread and unjustified denials of disclosure requests. the legal discretion of the Contracted Party making the determination based on these policy recommendations.

[7] For further context regarding the higher risk when data is combined, please refer to p. 5 of the legal guidance the EPDP Team referenced when considering these factors.

[8] In the context of Contracted Party authorization, the relevant parties are the Contracted Party (controller) and the registrant (data subject); however, the roles and responsibilities of the parties will be further discussed in implementation.

8.16.1.7 *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.
8.16.1.8 *Cross-border data transfers.* Consider the requirements that may apply to cross-border data transfers.

8.17. A lawful basis may be based on either the presence of a lawful basis under applicable law~~;~~ or on the absence of a prohibition on the processing and disclosure of the data requested under applicable law.

The application of the balancing test and factors considered in this section SHOULD be revised, as appropriate, to address applicable case law interpreting GDPR, guidelines issued by the EDPB or revisions to GDPR or other applicable privacy laws that may occur in the future.