RECOMMENDATION #6 - Contracted Party Authorization

Instructions: EPDP Team members are to review the updated recommendation #6 below and indicate if there are any aspects of this recommendation your group cannot live with. Please indicate your rationale for flagging an item and provide a proposal for how your concern can be addressed factoring in previous discussions.

Group	**Current text & rationale for cannot live with**	**Proposed updated text**
RrSG	"MUST NOT, absent any legal requirements to the contrary, deny a request 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 the disposition of a request 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. " Issues related to content on a website should NOT be addressed with the registrar or registry. (see: https://www.icann.org/resources/pages/spam-phishing-2017-06-20-en & Section 1.1.(c) of ICANN bylaws)	Delete "in content on a website associated"' *Staff support team: Change applied*
RrSG	This section should also be reworded to remove the negative requirement / double negative (may be difficult for non-native-English-speakers to understand; request that Staff assist with rewording)	*Staff support team: Input requested from IPC who originally drafted this paragraph 5*
RrSG**/IPC**	NOT A CANNOT LIVE WITH	*Staff support team: Change*

	ISSUE: The use of "prima facie" should be modified to plain English which would be understandable to the average person and does not require legal education to interpret	*applied - footnote added to clarify meaning.*
RySG	Footnote 4 For requests or jurisdictions where determination of a lawful basis is not required, a Contracted Party MUST at a minimum determine that it is legally permitted to process and disclose the data requested. this appears to be a type, the outcome of this evaluation isn't pre-determinted.	**Replace "that" with "if"** For requests or jurisdictions where determination of a lawful basis is not required, a Contracted Party MUST at a minimum determine if it is legally permitted to process and disclose the data requested. *Staff support team: Change applied but note that footnote has moved into main text and further changes have been applied as a result of other comments, but it is our understanding that those changes also address concerns expressed here.*
IPC/BC	"MUST conduct a prima facie review of the request's validity[1], i.e., is the request sufficient for the Contracted Party to ground a substantive review and process the associated underlying data;"	As a general matter, when the CP receives the request, its first step should be to disclose the data if the RDS data does not contain personal data. In the spirit of compromise, and as an attempt to address concerns raised by our CP colleagues, we may be able to live with some syntactical or other non-substantive preliminary

[1] 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 MAY request the requestor to provide further information prior to denying the request.

		review to ensure completeness. *Staff support team: Not clear if any specific changes are proposed. IPC/BC to clarify.*
IPC/BC	Footnote 3 "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 MAY request the requestor to provide further information prior to denying the request."	This MAY must be a MUST. If a request passes SSAD syntax check and is sent to the CP, but a CP claims that it is not valid on its face, the requestor must be able to address any claimed deficiency before a request may be denied. Also move this out of footnote. Normative language needs to be a policy recommendation, as opposed to a footnote. *Staff support team: Change applied*
BC/IPC	#3 - needs to be limited to personal data	Add at the end - "if the contact information includes personal data." *Staff support team: Change applied but with language suggested by ICANN org flagging the same issue (see below)*
BC/IPC	Footnote 5 includes a "MUST" and needs to be a policy recommendation	*Staff support team: Change applied*
BC/IPC	Footnote 8 needs to include denials where there is no personal data in the WHOIS record.	Add at the end of the first sentence: (v) denials where there is no personal data in the WHOIS Record *Staff support team: Change*

		applied but with wording consistent with terminology used elsewhere.
BC/IPC	Footnote 8: It is not appropriate for the EPDP to limit ICANN's ability to enforce the new policy based on current practices.	Footnote 8: Delete: 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. It's foreseeable that future legal guidance may make decision-making clearer, and Compliance may be able to ensure the decision was made correctly on the merits. We cannot enshrine permanently in policy the short-term inability of Compliance to enforce based on today's unknowns. *Staff support team: Change applied but with proposed alternative language limiting ICANN Compliance's role to these policy recommendations (and not opining about potential future changes).* ICANN org, NEW 24 June: This footnote should be updated to reflect the current recommendation language. For example, ICANN org notes that "content on a website" was deleted from paragraph 5. ICANN org also suggests revisiting the numbering within the footnote. For example, v) may be more appropriately labeled as e).

		Staff support team: Change applied
BC/IPC	#7 ICANN Compliance requests should not be limited to repeated failures only; It is not the EPDP's role to limit ICANN Compliance inquiries or processes.	Please add: If a requestor believes a Contracted Party is repeatedly and willfully engaging in the improper denial of requests, ADD: "or has wrongfully denied a properly supported request..." *Staff support team: Change applied but with language suggested by ICANN org flagging the same sentence (see below)*
ICANN org	General comment: For clarity in implementation, ICANN org suggests renumbering the paragraphs. For example, there are two paragraph 1's, two paragraphs 2's, etc.	*Staff support team: Change applied*
ICANN org	General Requirements, 1: "MUST review every request on its merits and MUST NOT disclose data on the basis of accredited user category alone." For clarity in implementation, ICANN org suggests incorporating the language from footnote 1 into General Requirements, paragraph 1.	General Requirements, 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." *Staff support team: Change applied*
ICANN org	General Requirements, 3: "MUST determine its own lawful basis for the processing related to the disclosure decision."	General Requirements, 3: "MUST determine its own lawful basis, if a lawful basis is required, for the processing related to the disclosure decision."

	As a lawful basis is not always required for a disclosure decision, ICANN org suggests editing the requirement to make this clear.	*Staff support team: Change applied*
ICANN org	Authorization Determination Requirements, 2.2: "If 2.1 does not apply, the Contracted Party MUST determine, at a minimum, as part of its substantive review of the request and the underlying data: " This wording may be confusing in implementation. For clarity, ICANN org suggests the updated text.	Authorization Determination Requirements, 2.2. "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:" *Staff support team: Change applied*
ICANN org	Authorization Determination Requirements, 2.1: There is no requirement to document the rationale for approval in 2.1. However, in 3.1, the Contracted Party MUST document a rationale for approval for a request. Shouldn't the rationale for approval in 2.1 also be documented? Similarly, in paragraphs 4.1 and 4.2, there is no requirement to document the rationale. In all instances where a request is approved or denied, does the EPDP team intend for the rationale to be documented and communicated to the Gateway? If yes, ICANN org suggests adding that	

	requirement to this language, as well as ensuring this consistency elsewhere in Rec #6.	
ICANN org	Authorization Determination Requirements, 2.2.1, Footnote 4: "For requests or jurisdictions where determination of a lawful basis is not required, a Contracted Party MUST at a minimum determine that it is legally permitted to process and disclose the data requested." ICANN org notes that it would be challenging to determine what could be explicitly legally permitted with regard to processing and disclosing data.	Footnote 4: Suggested edit for clarity, "For requests or jurisdictions where determination of a lawful basis is not required, a Contracted Party MUST at a minimum determine that it is not legally prohibited from processing and disclosing the data requested." *Staff support team: Change applied* ICANN org, NEW 24 June, ICANN org suggests revising this language to "..determine whether or not it is legally prohibited.." instead of being required to "determine that it is not legally prohibited.." *Staff support team: Change applied*
ICANN org	Authorization Determination Requirements, 2.2.1., Footnote 4: "For requests or jurisdictions where determination of a lawful basis is not required, a Contracted Party MUST at a minimum determine that it is legally permitted to process and disclose the data requested." This footnote reads as a policy requirement for Contracted Parties. ICANN	*Staff support team: Change applied*

	org suggests moving it into the body of the recommendation. In addition, the footnote seems to be the same requirement referenced in Authorization Determination Requirements, paragraph 4. ICANN org suggests the EPDP team consider revising Rec #6 to clarify how paragraph 4 and footnote 4 are expected to interact.	
ICANN org	Authorization Determination Requirements, 2.2.2: "whether all the requested data elements are necessary;" Could the EPDP Team please clarify what action a Contracted Party must take if it believes some or all of the requested data elements are not necessary? ICANN org thinks the EPDP team did not intend for the Contracted Party to deny the entire disclosure request.	Based on the EPDP team's language in Rec #8, d. and Rec #11, b., ICANN org understands the team's intent with this paragraph to be: If a Contracted Party determines that a requested data element is unnecessary, it MUST deny the request for that element, and continue to evaluate the request for any other requested elements that the Contracted Party deems necessary.
ICANN org	Authorization Determination Requirements, 2.2.3: Can the EPDP team please clarify what is meant by "whether further balancing or review is required" in 2.2.3? On what basis would a Contracted Party make this determination? Would "further balancing or review" be conducted in addition to the "substantive review of the request" in Authorization	

	Determination Requirements, paragraph 2? In addition, ICANN org is unclear how to enforce Authorization Determination Requirements 3.1 and 3.2 without further clarification on the intent of 2.2.3. ICANN org notes that depending on the EPDP Team's explanation of how 2.2.3 applies, it may require reviewing the language in Authorization Determination Requirements, paragraphs 3 and 4.	
ICANN org	Authorization Determination Requirements, 3.2: "MUST deny the request, 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." Should the language, "based on consideration of the above factors," match the language of 3.1 "based on its evaluation", as the language in 3.2 appears to refer to factors which no longer appear in the revised language?	*Staff support team: Change applied*
ICANN org	Authorization Determination Requirements, 6: "MUST, within its reexamination request, provide a supporting rationale as to why its	*Staff support team: Change applied*

	request must be reconsidered." As this is a reexamination request and not a reconsideration request, suggest revising "reconsidered" to "reexamined."	
ICANN org	Authorization Determination Requirements, 7: "If a requestor believes a Contracted Party is repeatedly and willfully engaging in the improper denial of requests, the requestor MAY notify ICANN Compliance further to the alert mechanism described in Recommendation 8." ICANN Contractual Compliance will enforce all of the above requirements. Requestors should file a complaint with ICANN org if a Contracted Party is failing to comply with any of the requirements in this policy. It is unclear why the Contracted Party must "repeatedly and willfully engag(e) in the improper denial of requests" for a complaint to be filed.	"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 8." *Staff support team: Change applied*
ICANN org	Implementation Guidance, paragraph 2 references paragraph 5(b), but ICANN org does not see a paragraph 5(b) in Rec #6. Can the team please clarify? Is this a reference to a previous version of Rec #6?	*Staff support team: Change applied - reference included to footnote 3*

ICANN org	Implementation Guidance, 3: "In situations where the requestor has provided a legitimate interest for its request for access/disclosure, the Contracted Party SHOULD consider the following:" In order for this guidance to be consistent with paragraph 3 of the Authorization Determination Requirements, ICANN org suggests editing the text.	"In situations where the Contracted Party is evaluating the legitimate interest of the requestor, the Contracted Party SHOULD consider the following:" *Staff support team: Change applied*
ICANN org	Implementation Guidance, "4.1. Has the requestor reasonably demonstrated/substantiated a legitimate interest or other lawful basis in its request?" If the Contracted Party, under 2.2.1. must determine whether it has a lawful basis to disclose the data, it seems that Implementation Guidance 4.1 is no longer necessary and has been subsumed in the requirement detailed in Authorization Determination Requirements, 2.2.1.	ICANN org suggests deleting Implementation Guidance 4.1. *Staff support team: Change applied*
ICANN org	Implementation Guidance, 4.2: "Are the data elements requested necessary to the requestor's stated purpose? Necessary means more than desirable but less than indispensable or absolutely necessary." Implementation Guidance, 4.2.2: "In addition, the	ICANN org suggests deleting Implementation Guidance 4.2 and 4.2.2. *Staff support team: Change applied*

	necessity of each data element in a request SHOULD be evaluated individually." This Implementation Guidance no longer seems necessary as it has been subsumed by the requirement detailed in Authorization Determination Requirements, 2.2.2.	
ICANN org	Implementation Guidance, 4.2.1: "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.)." This guidance no longer seems necessary as it seems to have been subsumed by General Requirements, 1: "MUST review every request on its merits and MUST NOT disclose data on the basis of accredited user category alone."	ICANN org suggests deleting Implementation Guidance 4.2.1. *Staff support team: Change applied*
ICANN org	Implementation Guidance, 5.1: "The applicable lawful basis and whether, based on the applicable lawful basis, further balancing or review is required." This Implementation Guidance no longer seems necessary as it is captured in Authorization Determination Requirements 2.2.1 and	ICANN org suggests deleting Implementation Guidance 5.1. *Staff support team: Change applied*

	2.2.3.	
ICANN org	Implementation Guidance 5.2: "Where applicable, 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." Minor edit: This appears to be a sentence fragment.	"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." *Staff support team: Change applied*
ICANN org (NEW - 24/6)	To align with the change to the language proposed for 7.2.1, suggest revising 9.1 9.2 from "is legally permitted to disclose the data" to read: "is not legally prohibited from disclosing the data."	*Staff support team: Change applied*

Redline version

Recommendation #6: 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 #16, regardless of whether automated processing of disclosure decisions is mandated or at the request of the Contracted Party.

General requirements

The Contracted Party

1. MUST review every request individually and not in bulk, regardless of whether the review is done automatically or through meaningful review ~~on its merits~~ [1] and MUST NOT disclose data on the basis of accredited user category alone.

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.

3. MUST determine its own lawful basis, if a lawful basis is required, for the processing related to the disclosure decision. 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.

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.

5. MUST NOT, absent any legal requirements to the contrary, deny a request 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 the disposition of a request 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.

Authorization determination requirements

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

6. MUST conduct a prima facie[2] review of the request's validity[3], i.e., is the request sufficient for the Contracted Party to ground a substantive review and process the associated underlying data;

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:

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.[4] 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.

7.2. If following the evaluation of the underlying data, the ~~2.1 does not apply, the~~ Contracted Party ~~MUST~~ 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:

2.2.1 whether the Contracted Party has a lawful basis[5] for disclosure. For requests or jurisdictions where determination of a lawful basis is not required, a Contracted Party MUST at a minimum determine that it is not legally prohibited from processing and disclosing the data requested;

27.2.2 whether all the requested data elements are necessary[6];

72.2.3 whether further balancing or review is required.

8. If the request is subject to further balancing or review as per paragraph 7.2.3:
   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.
   8.2 MUST deny the request, if, based on consideration of the above factorsits 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 rationale to the Central Gateway Manager, with care taken to ensure no personal data is revealed in the rationale explanation.

9. If the request is not subject to further balancing or review as per paragraph 7.2.3:
   9.1 MUST disclose if the Contracted Party determines it has a lawful basis or is legally permitted to disclose the data.
   9.2 MUST deny the request if the Contracted Party determines it does not have a lawful basis or is not legally permitted to disclose the data.

The Requestor:

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

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

12. If a requestor believes a Contracted Party is repeatedly and willfully engaging in the improper denial of requestsnot complying with any of the requirements of this policy, the requestor MAY SHOULD notify ICANN Compliance further to the alert mechanism described in Recommendation 8.

Implementation Guidance

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.

14. The EPDP Team notes the specifics of how the communication in ~~Paragraph 5(b)~~footnote 3 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.

15. In situations where the Contracted Party is evaluating ~~requestor has provided a~~ the legitimate interest of the requestor ~~for its request for access/disclosure~~, the Contracted Party SHOULD consider the following:

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

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

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.

~~1. As part of the substantive review in 2.2, the Contracted Party SHOULD consider these factors:~~

~~16.1Has the requestor reasonably demonstrated/substantiated a legitimate interest or other lawful basis in its request?~~[7]

~~16.1Are the data elements requested necessary to the requestor's stated purpose? Necessary means more than desirable but less than indispensable or absolutely necessary.~~[8]

~~16.1.1Each 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.).~~

~~16.1.1In addition, the necessity of each data element in a request SHOULD be evaluated individually.~~

16. The Contracted Party SHOULD[9], as part of its substantive review, assess at least:

~~5.1The applicable lawful basis and whether, based on the applicable lawful basis, further balancing or review is required.~~

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:

16.2.1 *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.

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

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

16.2.4 *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),[10] provided that this is not intended to prohibit public disclosures for legal actions or administrative dispute resolution proceedings such as the UDRP or URS.

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

16.2.6 *Status of the controller and data subject.* Consider negotiating power and any imbalances in authority between the controller and the data subject.[11]

16.2.7 *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.

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

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.

~~[1] For clarity, "on its merits" means that requests cannot be considered in bulk but must be considered individually, regardless of whether the consideration is done automatically or through meaningful review.~~

[2] Per the Cambridge Dictionary, at first sight (= based on what seems to be the truth when first seen or heard)

[3] 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 ~~MAY~~ MUST request the requestor to provide further information prior to denying the request

[4] 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.

~~[5] For requests or jurisdictions where determination of a lawful basis is not required, a Contracted Party MUST at a minimum determine that it is legally permitted to process and disclose the data requested.~~

[6] 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.

~~[7] For the avoidance of doubt, the Contracted Party's threshold determination of the lawful basis or legitimate interest is meant to assess the provision of a lawful basis or legitimate interest, rather than the merits of a potential legal claim.~~

~~[8] 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.~~

[9] 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; ~~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); or (v) denials where the registration data does not include personal information. 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 based on these policy recommendations.

[10] 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.

[11] 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.

Previous version

Recommendation #6: 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 #16, regardless of whether automated processing of disclosure decisions is mandated or at the request of the Contracted Party.

General requirements

The Contracted Party

1. MUST review every request on its merits[2] and MUST NOT disclose data on the basis of accredited user category alone.

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.

3. MUST determine its own lawful basis for the processing related to the disclosure decision. 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.

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.

5. MUST NOT, absent any legal requirements to the contrary, deny a request 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 the disposition of a request 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.

Authorization determination requirements

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

[2] For clarity, "on its merits" means that requests cannot be considered in bulk but must be considered individually, regardless of whether the consideration is done automatically or through meaningful review.

1. MUST conduct a prima facie review of the request's validity[3], i.e., is the request sufficient for the Contracted Party to ground a substantive review and process the associated underlying data;

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

    2.1 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.[4] 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.

    2.2. If 2.1 does not apply, the Contracted Party MUST determine, at a minimum, as part of its substantive review of the request and the underlying data:
    2.2.1 whether the Contracted Party has a lawful basis[5] for disclosure;
    2.2.2 whether all the requested data elements are necessary;
    2.2.3 whether further balancing or review is required.

3. If the request is subject to further balancing or review as per paragraph 2.2.3:
    3.1 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.
    3.2 MUST deny the request, 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 Contracted Party MUST document the rationale for its denial and MUST communicate the rationale to the Central Gateway Manager, with care taken to ensure no personal data is revealed in the rationale explanation.

4. If the request is not subject to further balancing or review as per paragraph 2.2.3:
    4.1 MUST disclose if the Contracted Party determines it has a lawful basis or is legally permitted to disclose the data.
    4.2 MUST deny the request if the Contracted Party determines it does not have a lawful basis or is not legally permitted to disclose the data.

---

[3] 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 MAY request the requestor to provide further information prior to denying the request.

[4] 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.

[5] For requests or jurisdictions where determination of a lawful basis is not required, a Contracted Party MUST at a minimum determine that it is legally permitted to process and disclose the data requested.

The Requestor:

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

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

7. If a requestor believes a Contracted Party is repeatedly and willfully engaging in the improper denial of requests, the requestor MAY notify ICANN Compliance further to the alert mechanism described in Recommendation 8.

Implementation Guidance

1. 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.
2. The EPDP Team notes the specifics of how the communication in Paragraph 5(b) will be assessed in the policy implementation phase; however, the EPDP Team provides this additional guidance to assist. The EDPP 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.
3. In situations where the requestor has provided a legitimate interest for its request for access/disclosure, the Contracted Party SHOULD consider the following:
   3.1. Interest must be specific, real, and present rather than vague and speculative.
   3.2. An interest is generally deemed legitimate so long as it can be pursued consistent with data protection and other laws.
   3.3. 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.
4. As part of the substantive review in 2.2, the Contracted Party SHOULD consider these factors:
   4.1. Has the requestor reasonably demonstrated/substantiated a legitimate interest or other lawful basis in its request?[6]

[6] For the avoidance of doubt, the Contracted Party's threshold determination of the lawful basis or legitimate interest is meant to assess the provision of a lawful basis or legitimate interest, rather than the merits of a potential legal claim.

4.2. Are the data elements requested necessary to the requestor's stated purpose? Necessary means more than desirable but less than indispensable or absolutely necessary.[7]
    4.2.1. 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.).
    4.2.2. In addition, the necessity of each data element in a request SHOULD be evaluated individually.

5. The Contracted Party SHOULD,[8] as part of its substantive review, assess at least:
    5.1. The applicable lawful basis and whether, based on the applicable lawful basis, further balancing or review is required.
    5.2. Where applicable, 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 Contracted Party SHOULD consider the totality of the circumstances outlined below:
        5.2.1. *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.
        5.2.2. Nature of the data. Consider the level of sensitivity of the data as well as whether the data is already publicly available.
        5.2.3. Status of the data subject. Consider whether the data subject's status increases their vulnerability (e.g., children, asylum seekers, other protected classes)
        5.2.4. *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),[9] provided that this is not intended to prohibit public disclosures for legal actions or administrative dispute resolution proceedings such as the UDRP or URS.
        5.2.5. *Reasonable expectations of the data subject.* Consider whether the data subject would reasonably expect their data to be processed/disclosed in this manner.

---

[7] 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] 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; 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.

[9] 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.

5.2.6. *Status of the controller and data subject.* Consider negotiating power and any imbalances in authority between the controller and the data subject.[10]

5.2.7. 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.

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

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.

[10] 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.