RECOMMENDATION #10 – Acceptable Use

Note – only input has been received from the RySG on the discussion items. Based on this input, the proposed path forward / common understanding is:

- Stick with the concept of one Central Gateway Manager and not one or more Gateway Managers designated for each top-level domain.
- Consider integrating this recommendation with Preliminary Recommendations 13 (terms of use) and 14 (data retention). Reduce duplication of requirements that are already found in other recommendations. Note that a through d do not seem to address use of the SSAD – consider where these belong in the reorganization of the different related recommendations.
- Historic data is considered out of scope.
- The AUP is a legal document that binds the requester to certain standards. The noted standards were an attempt at minimums standards of use / conduct, and must be agreed prior to access. This is not 'checkbox' for the requester - but legal protection for the SSAD/Gateway manager.

Questions:

1. Who is to trigger the enforcement mechanism referenced ("*The EPDP Team recommends that the following requirements are applicable to the requestor and MUST be confirmed by the Central Gateway Manager and subject to an enforcement mechanism. For the avoidance of doubt, every request does not have to go through an enforcement procedure; the enforcement mechanism MAY, however, be triggered in the event of apparent misuse").* Is it enforcement mechanism to be triggered by ICANN Compliance and if so, is ICANN Compliance willing to take on this responsibility as it would go beyond Contracted Parties?
2. Does everyone share the understanding that everyone is able to complain but the decision to trigger the enforcement mechanism is made by the Central Gateway Manager or its designee after considering a complaint?
3. Does everyone share the same understanding that the Acceptable Use policy is a living policy / document, not a checkbox exercise? It is accepted that every requester shall agree to accept the terms of use as a condition of their access to the system - not individual elements being 'ticked' in the manner suggested by one of the commenters.
4. Does the EPDP Team anticipate that the Central Gateway Manager does more than only an automatic check that the requestor has accepted the Acceptable Use Policy?
5. Is there concern regarding the following addition:
   d) For each stated purpose must provide (i) representation regarding the intended use of the requested data and (ii) **representation of procedural, rule of law and data protection safeguards in the accompanying documentation, if required by law (iii)** representation that the requestor will only process the data for the stated purpose(s~~)~~.

Disclaimer: *This overview has been developed to facilitate the EPDP Team's consideration of the concerns expressed and possible updates to the recommendations from the Initial Report. However, this does not replace the EPDP Team's obligation to review all input received in full and to indicate if any concerns in this overview have inadvertently been mischaracterized or left out.*

Instructions: Each team is expected to have reviewed the PCRT before filling out the tables below. Please focus on any new information or insights that have been provided. If it concerns information or perspectives that the EPDP Team already considered in the development of the recommendations, feel free to point this out.

Preliminary Recommendation #10. Acceptable Use Policy

The EPDP Team recommends that the following requirements are applicable to the requestor and MUST be confirmed by the Central Gateway Manager and subject to an enforcement mechanism. For the avoidance of doubt, every request does not have to go through an enforcement procedure; the enforcement mechanism MAY, however, be triggered in the event of apparent misuse.

Noted Concerns / Suggestions

a) Proposed Edit	**Corresponding PCRT Comment #**
"For the avoidance of doubt, every request does not have to go through an enforcement procedure; the enforcement mechanism may, however, be triggered **BY ICANN COMPLIANCE** in the event of apparent misuse."	#2
b) Clarification	**Corresponding PCRT Comment #**
It should be clarified regarding who can trigger the enforcement mechanism regarding "apparent misuse." The Centralized Gateway Manager? A Contracted Party? A third-party?	#3, 9, 11, 12
c) Comment	**Corresponding PCRT Comment #**
The Acceptable Use Policy elements to be reasonable. We note that for ease of use, the SSAD should enable these representations to be made by checking a box or an equivalent automated means (if the SSAD is available via API, for example).	#5
d) Proposed Edit	**Corresponding PCRT Comment #**
We recommend that "the Central Gateway Manager" be revised to "the designated Gateway Manager" consistent with our comments elsewhere regarding changing the requirement for a single, centralized gateway for all requests to a requirement for one or more Gateway Managers designated for each top-level domain.	#7
e) Concern	**Corresponding PCRT Comment #**
A typical Acceptable Use Policy (AUP) discusses the choice of law and reasonable uses of a service; this Preliminary Recommendation does not do that. The AUP as it applies to requestors ought to address things like credential sharing; abuse, including excessively high volume of requests, abuse of automated requests (where automated requests are in appropriate), and abuse of Urgent request	#14

designation; and illegitimate requests. Similarly, the AUP should address the consequences of violations, typically including termination of service. Termination of service is discussed in the "Accredited User Revocation & Abuse" section of Preliminary Recommendation #1 and is mentioned in Preliminary Recommendation #12; these disconnected elements, as well as the mention of the "enforcement mechanism" in this Preliminary Recommendation, should be brought together and harmonized to ensure alignment and lack of internal conflict.		
f) Concern		**Corresponding PCRT Comment #**
As noted in ICANN org's comments on Preliminary Recommendation #13, ICANN org recommends combining Preliminary Recommendation 10, Acceptable Use Policy with Preliminary Recommendations 13 and 14.		#18
Group	**Please indicate if you agree with the concerns and proposed language edits and indicate specific language changes that should be applied to address the concern? Agree / Disagree**	**If you agree with the concern, please provide specific language changes. If you disagree, please indicate why.**
ALAC		
BC		
GAC		
IPC		
ISPCP		
NCSG		
RrSG		
RySG	a)somewhat disagree b)agree c)disagree d)disagree e)agree f) no opinion	a) although we agree that the enforcement procedure should be triggered by a particular entity - we have not agreed that this entity should be ICANN Compliance. This may be ICANN compliance, but this is broadening their role outside of contracted party compliance, into being the compliance entity monitoring SSAD requester too - ICANN should clarify if this is something that they expect/intend to fulfil in this process? b) Although we agree. An enforcement mechanism should only be triggered by the receipt of a substantiated complaint. Anyone can complain - only the SSAD/centralized gateway manager or its designee should be able to trigger the enforcement after considering a complaint.

		c) This is moreso a disagreement with the concept being outlined by the commenter. The Acceptable Use is a living policy / document, not a checkbox exercise. It is accepted that every requester shall agree to accept the terms of use as a condition of their access to the system - not individual elements being 'ticked' in the manner suggested. d) The concept of a gateway manager per TLD is unnecessary duplication in the extreme, not to mention a duplication of processing of the PII of the requestors, which seems to fail Privacy by default and design (for natural person requesters)
SSAC		

Formatted: Outline numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

The requestor:

a. *MUST only request data from the current RDS data set (no historic data);*
b. *MUST, for each request for RDS data, provide representations of the corresponding purpose and lawful basis for the processing, which will be subject to auditing (see the auditing preliminary recommendation for further details);*
c. *MAY request data from the SSAD for multiple purposes per request, for the same set of data requested;*
d. *For each stated purpose must provide (i) representation regarding the intended use of the requested data and (ii) representation that the requestor will only process the data for the stated purpose(s). These representations will be subject to auditing (see auditing preliminary recommendation further details);*
e. *MUST handle the data subject's personal data in compliance with applicable law (see auditing preliminary recommendation for further details).*

g) Concern	**Corresponding PCRT Comment #**
a) Limiting requested data to only the current RDS data will impose a challenge on brand owners and other third-party requestors. There are a number of reasons it is very important to have the ability to also obtain historical data, for instance to learn the approximate date on which that registrant acquired the domain name (which may differ from the domain's original creation date by a prior registrant). Accordingly, there should be an option to also obtain historical data that is retained by the Contracted Party upon request. Both the UDRP and URS require a showing of bad faith registration and use, i.e., bad faith at the time the disputed domain name was acquired by the registrant. By limiting requested and disclosed data only to the current information, brand owners may not be able to ascertain whether the registrant's	#3, 10, 12, 14

acquisition of the disputed domain name predates the brand owner's trademark rights. This could result in the unintended filing of UDRP or URS complaints that have no chance of success. In such instances brand owners, through no fault of their own, could be found guilty of reverse domain name hijacking. In order to avoid this risk, requested data should not be limited to current RDS but should, upon request, be expanded to include archived/historical data as well to the extent such data is available. data can be essential to provide a complete picture, for example in case of suspected cyberflight.	
h) Concern	**Corresponding PCRT Comment #**
a) Regarding the proposed limitation on historic data, if limited to current data, at minimum, the date the current registrant became the registrant should be made available.	#13
i) Suggested edit	**Corresponding PCRT Comment #**
a) must only request data from the current RDS data set (no historic data) **as well as the historic RDS data set**"	#8
j) Clarification	**Corresponding PCRT Comment #**
Is it correct to assume that bullet a) is intended to mean that registrations with expired data cannot be requested through the SSAD and that a registrar will not disclose historic registration data beyond the life of the expired domain?	#18
k) Concern	**Corresponding PCRT Comment #**
(b) The "representations" required by this portion of the Recommendation must not be unduly burdensome and should, ideally, be satisfied by a check-the-box list of common reasons for such requests (with a catch-all "Other" checkbox and free text field for stating uncommon reasons). As for the "corresponding purpose and lawful basis for the processing", the comments set forth pertaining to Preliminary Recommendation #3 "Criteria and Content of Requests" are incorporated here as well.	#3, 8, 11, 12
l) Clarification	**Corresponding PCRT Comment #**
d) It is unclear what is meant by the "representation regarding the intended use of the requested data". If this simply means that the requestor represents that the stated intended use is the actual intended use, then this should be satisfied by a simple checkbox. However, if its meaning is intended to be broader and mean that the intended use must be specifically stated, this seems to be redundant to other parts of the process set out in the recommendations. If the latter is the case, then the representation should be satisfied by a standardized check-the-box list of common intended uses (with a catch-all "Other" checkbox and free text field for stating uncommon uses). Further, the "representation that the requestor will only process the data for the stated purpose(s)" should be satisfied with a simple checkbox.	#3, 8, 11, 12
m) Concern	**Corresponding PCRT Comment #**
The requestor requirements (a) through (d) do not belong in an Acceptable Use Policy and are duplicative of other Preliminary Recommendations. (a) is already in the Disclosure requirement section. (b) is in Rec. 3 criteria of requests. (c) is encompassed in Rec 3 c. (d) belongs in Rec 3 (c) but is	#14

not clear enough there and should be expanded in that Preliminary Recommendation. The only point that properly belongs in the AUP is (e).	
n) Proposed edit	**Corresponding PCRT Comment #**
This recommendation is labeled as "Acceptable Use Policy" yet bullet points a) through d) do not seem to address use of the SSAD. Could the EPDP revisit the title of Preliminary Recommendation 10 to ensure it applies to the entire recommendation? The use of "Central Gateway Manager" in Preliminary Recommendation 10 seems to contradict the role of the Central Gateway Manager in the rest of the policy recommendations. Elsewhere the Central Gateway is expected only to carry out automated checks of requests. This does not seem to align with the language in Preliminary Recommendation 7, which requires the Central Gateway Manager to confirm the elements of the Acceptable Use Policy. Does the EPDP team anticipate this to be more than an automatic check? ICANN org suggests that the EPDP team further clarify if the intention of this paragraph is to reflect that review of disclosure requests is intended to be automatic as noted in footnote 14. It is ICANN org's understanding that all recommendations are subject to ICANN Contractual Compliance enforcement. However, as enforcement is referenced only in Preliminary Recommendations 10 and 11, is the EPDP team recommending that other requirements in the policy are not subject to compliance enforcement?	#18
d. Concern	**Corresponding PCRT Comment #**
~~(d) provides that "exceptional circumstances MAY include the overall number of requests received if the number far exceeds the established SLAs." As discussed in the Preliminary Recommendation #9 response, these SLAs are being set by the EPDP Phase 2 Team in a vacuum; there is no understanding of the request volume or how this may affect the staffing needs of all Contracted Parties. There must be flexibility for each individual Contracted Party to identify exceptional circumstances.~~	~~#20~~
~~**e. Proposed Edit**~~	~~**Corresponding PCRT Comment #**~~
~~d) For each stated purpose must provide (i) representation regarding the intended use of the requested data and (ii) **representation of procedural, rule of law and data protection safeguards in the accompanying documentation, if required by law (iii)** representation that the requestor will only process the data for the stated purpose(s). These representations will be subject to auditing (see auditing preliminary recommendation further details);~~	~~#6~~
~~**f. Proposed Edit**~~	~~**Corresponding PCRT Comment #**~~
~~SSAD requests that meet the automatic response criteria must **MAY** receive an automatic disclosure response"~~ ~~Contracted Parties should always maintain the ability both to determine which categories of requests receive automated responses and to audit the disclosure of the personal data of which they are stewards, among other things, to protect themselves from liability. Deciding in advance that certain categories of requests must always be automated is not realistic; any automated disclosure must be reevaluated on an ongoing basis to prevent abuse and allow for improvements.~~	~~#20~~

~~g. Proposed Edit~~		~~Corresponding PCRT Comment #~~
~~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.~~ ~~Delete - non-exhaustive and not always applicable example.~~		~~#20~~
Group	**Please indicate if you agree with the concern and provide specific language changes that should be applied to address the concern? Agree / Disagree**	**If you agree with the concern, please provide specific language changes. If you disagree, please indicate why.**
ALAC		
BC		
GAC		
IPC		
ISPCP		
NCSG		
RrSG		
RySG	g)Disagree h)Disagree i)Disagree j)Agree / correct k)Disagree l) Disagree m) agree n) Agree more clarity could be beneficial d)agree e) agree f)agree g)agree	g) historical data is out of scope h) historical data is out of scope k) The Acceptable use Policy should be as burdensome as is necessary to prevent misuse and to protect the SSAD / Central Gateway manager from over zealous requester - this remains a matter, we contend, for the central gateway/SSAD to define based on a proper analysis of risk, and expected behavior. l) It would appear that the intention of the Acceptable Use Policy is misunderstood by the commenters. The AUP is a legal document that binds the requester to certain standards. The noted standards were an attempt at minimums standards of use / conduct, and must be agreed prior to access. This is not 'checkbox' for the requester - but legal protection for the SSAD/Gagteway manager.
SSAC		

Formatted: Font: (Default) +Headings (Calibri), Font color: Black

Formatted: Indent: Left: 0.5"

Formatted: Font: (Default) +Headings (Calibri), Font color: Black