Issue List – Status 26 January 2020

Note: Blue highlighting denotes issues that were flagged but for which no change is proposed.

ACCREDITATION

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
#21	This can be either ICANN itself or an entity with which it contracts (IPC)	Current language: Accreditation Authority Auditor - Independent entity that is contracted by ICANN org**, or function that is carried out by ICANN Org itself if Accreditation Authority function is outsourced to a third party,** to carry out auditing requirements as outlined in auditing preliminary recommendation	
#22	In the accreditation principles below, principle (c) we say "The accreditation policy defines a single Accreditation Authority, run and managed by ICANN org." So how can ICANN revoke the agreement with itself? In addition if we have one single accreditation authority de-accrediting it leads to the collapse of the whole system leaving us with no system for disclosure of data as well as no guidance on how to build another one. Moreover, the term De-accreditation of Accreditation Authority is not a term used in the report, therefore its definition does not matter nor is necessary for the purpose of this report. In all cases I the issue of the accreditation authority being in breach of	ICANN org revokes the agreement with the accreditation authority, **if this function is outsourced to a third party,** following which it is no longer approved to operate as the accreditation authority.	

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
	the requirements is addressed under "accreditation Authority" on page 19 and is mentioned on Page 34 in relation to the audits of the accrediting Authority (ALAC)		
#23	A term that could be added is De-authorization of identity provider (ALAC)		Is this something that the accreditation authority should determine as it is up to the accreditation authority to decide whether or not to make use of identity providers?
#24	Shouldn't this be reversed? The accredited entity must warrant that the individual using its credentials are acting on its authority, and the accredited entity can be held accountable for the individual's actions. (NCSG)	Current language: Both legal persons and/or individuals are eligible for accreditation. An individual accessing SSAD using the credentials of an accredited entity warrants that the individual is acting on the authority of the accredited entity.	The EPDP Team can discuss this proposal but this is what the group agreed to in Montreal – it seems difficult for an accredited entity to warrant this?
#25	each request should have one purpose, data sets disclosed vary depending on the purpose and it is important to be able to track the data disclosed to a requester for a certain purpose. In addition different purposes have different legal basis and different rights to the data subjects associated with it. (ALAC)	Current language: f. Assertion as to the purpose(s) of the request	This is also a topic that the group discussed and previously agreed – a request may have multiple purposes associated with it.
#26	Suggest "preferable where lawful" (BC / IPC)	g. Validation of Identity Credentials and Authorization Credentials, in addition to the information contained in the request, facilitate the decision of the authorization provider to accept or reject the Authorization of an SSAD request. For the avoidance of doubt, the presence of	

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
		these credentials alone DOES NOT result in or mandate an automatic access / disclosure authorization. However, the ability to automate access/disclosure authorization decision making is possible under certain circumstances **where lawful**.	
#27	Several team members have asked for our report to be agnostic to any specific data protection law, but reviewing the report in its entirety, we should be clear that the recommendations are a response to the regulatory challenges posed by the GDPR. This manifests itself in many areas, such as legal basis and reference to the EDPB. Therefore, it appears disingenuous to make the report appear to work for multiple data protection laws without further explanation. Thus, we should state that the recommendations shall contribute to the proper application of the GDPR and – by doing so – likely to a huge number of other data protection laws. Further, in the same paragraph reference is made to an Accreditation Body Auditor (a.k.a. monitoring body). We suggest to delete the addition in brackets and ensure we do not introduce two terms for the same function and stick to Accreditation Body Auditor throughout the report. (ISPCP)	Current language: h. Defines a base line “code of conduct” that establishes a set of rules that contribute to the proper application of data protection laws - including the GDPR - for the ICANN community, including: (…)	This comment appears to be a general one and not specifically to this section. Consider asking the ISPCP to suggest language that could be included in the introduction to the report.

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
#28	Add: ”to challenge actions taken by the Accreditation Authority” to clarify the scope of the dispute resolution and complaints process. (ISPCP)	j) MUST define a dispute resolution and complaints process **to challenge actions taken by the Accreditation Authority**.	
#29	NCSG has a problem with this, and several other similar assertions that seem to blur the line between bulk access and individual requests. In what sense is "each and every unique request for RDS data" being processed when thousands of them are submitted at the same time? We believe that assumptions about automatic access and disclosure are being insinuated into the draft report in a number of ways, and we want it to be known that we will resist that. (NCSG) I don’t understand the concern about this language. This merely says that multiple requests may be SUBMITTED together. Elsewhere, this policy requires each request to be evaluated on its own merits. We have agreed that prohibitions on “bulk access” are based on its definition in the 2013 RAA. (IPC) Suggest changing to "submitted during a specific period of time" to recognize that	Current language: t) Will not be restricted in the number of SSAD requests that can be submitted **during a specific period of** ~~at a~~ time, except where the accredited entity poses a demonstrable threat to the SSAD. It is understood that possible limitations in SSAD’s response capacity and speed may apply. For further details see the response requirements preliminary recommendation	These comments also come up in other sections but the issue of multiple requests has been discussed and it was agreed that this is addressed by the recommendation that each request should be considered on its merits – regardless of whether it was submitted in a batch or individually. Why is this not considered sufficient? BC proposed addition seems non-controversial.

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
	RDAP is the most likely protocol and that each request will be a discrete event occurring in in a series. (BC)		
#30	The accreditation service will be a service that is financially sustainable. Fur further details, see the financial sustainability preliminary recommendation. The reason for the request for change is that the system will likely not only be designed to recover cost, but may also include a component to cover legal risk for the parties involved. (ISPCP)	~~The accreditation service should be part of a cost-recovery system.~~ **The accreditation service will be a service that is financially sustainable.** For further details, see the financial sustainability preliminary recommendation.	

RECEIPT OF ACKNOWLEDGEMENT

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
#36	"Urgent" requests (circumstances that pose an imminent threat to life, serious bodily injury, critical infrastructure ((online and offline)) or child exploitation) require a different system. Consider ensuring that normal business hours are prominently posted on the relevant web site along with a dedicated contact number for the exclusive use of urgent requesters to contact the potential disclosing party and notify them of the request. We should also consider how urgent requests should be handled after normal business hours. (GAC)	The EPDP Team recommends that, consistent with the EPDP Phase 1 recommendations, the response time for acknowledging receipt of a SSAD request should be without undue delay, but not more than two (2) business days from receipt, unless (i) shown circumstances do not make this possible or (ii) the SSAD is implemented using technologies which allow instantaneous responses to disclosure requests, in which case, the acknowledgement of receipt must be instantaneous.	Note – The Registrar Accreditation Agreement already maintains requirements for reports of abusive use in Section 3.18, e.g., “[r]egistrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall **publish an email address to receive such reports on the home page of Registrar's website** (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
			any reports of abuse." SLA for urgent request is dealt with in the response requirements and an updated SLA for urgent requests is included in the Chameleon proposal section. Consider adding language there that requires CPs to post business hours on the relevant web site along with contact information for the exclusive use of urgent requestors.

RESPONSE REQUIREMENTS

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
#45	Suggestion from Brian King: We should insert language akin to that in the P/P policy "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." I see no reason for our policy to categorically eliminate what in some cases could be perfectly valid reasons not to disclose. The last part (IP infringement in content on a website) (NCSG)	Current language: d. Responses where disclosure of data (in whole or in part) has been denied should 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.	EPDP Team to consider but it appears to go too far to include in policy for which reasons disclosure cannot be refused as each case may be different?

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
	'For example' – delete (IPC) Insert: if the request was denied, in whole or in part, because the requested data is already publicly available, the response should indicate exactly where. (IPC)		
#46	Suggestion from Daniel Halloran: Should this be 'OR'? It definitely should be OR (NCSG) "OR" makes more sense here. If we're trying to address two separate scenarios, it probably makes sense to make this two sentences. Disclosure shouldn't "result in inconsistency with these policy recommendations" in any situation I can envision – what scenario are we trying to address with this language? (IPC)	The EPDP Team recommends that if ~~the entity disclosing the data~~ **a Contracted Party** determines that disclosure would be in violation of applicable laws ~~AND~~ **and consequently** result in inconsistency with these policy recommendations, the ~~entity disclosing the data~~ **Contracted Party** must document the rationale and communicate this information to the requestor and ICANN Compliance (if requested).	Changing this to or seems to change the meaning of the original intent – alternative wording proposed.
#47	The section on Implementation Guidance starting at the bottom of p.27 seems to be mostly duplicative of other parts of the report. We suggest deleting it. (ISPCP)	Current language: Implementation Guidance: a. The entity receiving the access/disclosure request must confirm that the request is syntactically correct, including proper and valid Authentication and Authorization Credentials. Should the entity receiving the access/disclosure request establish that the request is syntactically incorrect, the entity receiving the access/disclosure request must reply	This section was originally created to separate out implementation related items from policy recommendations. If the group agrees that it is duplicative, it can be removed.

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
		with an error response to the requestor detailing the errors that have been detected. b. Should the entity receiving the access/disclosure request establish that the request is incomplete, the entity receiving the access/disclosure request must reply with an incomplete request response to the requestor detailing which data required by policy is missing, providing an opportunity for the requestor to amend its request. c. Typically the acknowledgement response will include a "ticket number" or unique identifier to allow for future interactions with the SSAD. An example of online critical infrastructure includes root servers; an example of offline critical infrastructure includes bridges. [examples to be provided by the EPDP Team]	

ACCEPTABLE USE POLICY

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
#48	I do not envisage any mechanism within SSAD enabling a request for historical data, so this recomendation seems harmless but unnecessary. It's also redundant to at least 2 other references below. (BC)	Current language: a) Must only request data from the current RDS data set (no historic data)	If it is considered harmless suggest leaving it as some have stated that this is important to be restated where applicable.

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
	Unclear: if requestor wrongly requests historical data AND current data, is the request for current data still considered? In any case, it's redundant with other language (see c. in last subsection of recommendation 9.) (IPC)		
#49	'and every unique' - Unclear and redundant: delete. (IPC)	b) Must, for each **~~and every unique~~** 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);	
#50	different purposes have different lawful basis and different data subject rights associated with it. therefore submitting a request with different purposes does not really work. However, the data might be used for purposes related and consistent with the original submitted purpose. if we allow a single request to have multiple purposes then in assessing the request it should be treated as multiple separate requests each with a single purpose. where disclosure could be allowed for one of the purposes and denied for the others. Also if we take b) and d) into consideration then practically speaking the request would be treated as multiple separate requests (ALAC)	c) MAY request data from the SSAD for multiple purposes per request, for the same set of data requested;	See also #25. This is also a topic that the group discussed and previously agreed – a request may have multiple purposes associated with it.

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
#51	'intended use' - Unclear how this is different from "stated purpose". (IPC)	Current wording: 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);	There does appear to be a difference – EPDP Team to consider but note that this language was previously agreed.
#53	This section only refers to the right to erasure. We suggest to include all rights of the data subject that need to be informed about under the GDPR or – in more general terms, just make reference to the information duties in the GDPR. (ISPCP) why do we specifically and only mention erasure, there are other rights like rectification (ALAC)	g) Where required by applicable law, must provide mechanism under which the data subject may exercise its right to erasure **and any other applicable rights**;	
#55	'no historic data' - Delete: it's redundant with other language (see c. in last subsection of recommendation 9.) (IPC)	Current wording: a) Must return current data or a subset thereof in response to a request (no historic data);	If it is considered harmless suggest leaving it as some have stated that this is important to be restated where applicable
#56	2 comments: 1. Replace with "inform." 2. When: upon request or in their privacy policy? (IPC)	h) Confidentiality of disclosure requests – Data controllers of RDS data must ~~make it clear to~~ **inform** data subjects the types of entities/third parties which may process their data. Upon a request from a data subject the exact processing activities of their data within the SSAD, should be disclosed as soon as reasonably	

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
		feasible. However the nature of legal investigations or procedures may require SSAD and/or the disclosing entity keep the nature or existence of these requests confidential from the data subject. Confidential requests can be disclosed to data subjects in cooperation with the requesting authority, [and] [or] in accordance with the data subject's rights under applicable law	

QUERY POLICY

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
#57	Unclear what a and b respectively are supposed to cover. (IPC) Changing “access” to “credentials” resolves the ambiguity Franck mentions. (IPC) ‘Abusive’ use of SSAD - Does this refer to a (which mentions abuse AND misuse), b or both? (IPC)	Current language: a) Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system; b) May take measures to limit the number of requests that are submitted by the same requestor if it is demonstrated that the requests are of an abusive* nature. *“Abusive” use of SSAD may include (but is not limited to) the detection of one or more of the following behaviors/practices:	This language was extensively discussed and finally agreed to – suggest not reopening this section unless there is information that was previously not considered.
#58	Still don’t know what it means to say “unless otherwise required or permitted (NCSG).	a. Unless otherwise required or permitted, not allow bulk access*, wildcard requests, ~~[reverse lookups]~~, nor boolean search capabilities.	Update to reflect agreement from 23/1 meeting.

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
	"unless otherwise required or permitted" is from the New gTLD Registry Agreement. The original registration date is in the data formerly known as "thin WHOIS", so we agree that this language could be clearer. (IPC) Define "bulk access" according to meaning in the 2013 RAA Section 3.3.6.1 "a complete copy of the data available" (IPC)	***As described in the RAA, section 3.3.6**	
#59	Re: history, what about the domain's original date of registration? (NCSG)	Current language: d. Only return current data (no data about the domain name registration's history)	Original creation data is part of minimum public data set.
#60	Delete: it's redundant with language in c. above. (IPC) redundant with 8(a) and 9(c)#2 (BC	Current language: Requests must only refer to current registration data (historical registration data will not be made available via this mechanism).	If it is considered harmless suggest leaving it as some have stated that this is important to be restated where applicable.

TERMS OF USE

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
#62	We should make reference to the component parts and information that a privacy policy must have under the GDPR. (ISPCP) 'The types of third parties with whom personal data is shared' - Replace with "may be" (IPC)	Current language: Privacy Policy The EPDP recommends, at a minimum, the privacy policy shall include: • Relevant data protection principles, for example, • The type(s) of personal data processed	Request ISPCP to provide specific changes but note that the EPDP Team previously discussed to keep this at a high level.

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
	'Where applicable, details of any international data transfers/requirements thereof' - To what does thereof refer? If to "transfers", then edit sentence to read "data transfers and their requirements." (IPC)	• How and why the personal data is processed, for example, ◦ verifying identity ◦ communicating service notices • How long personal data will be retained • The types of third parties with whom personal data ~~is~~ **may be** shared • Where applicable, details of any international data transfers **and their** ~~/~~requirements ~~thereof~~ • Information about the data subject rights and the method by which they can exercise these rights • Notification of how changes to the privacy policy will be communicated • Further consideration should be given during implementation whether updates to the RAA are necessary to ensure compliance with these recommendations.	
#63	Not only the disclosing party and ICANN, but all parties involved in the SSAD must be indemnified. (ISPCP) Are we contemplating that requestors indemnify the disclosing party and/or ICANN as a condition of using the SSAD? (GAC)	Current language: The EPDP recommends, at a minimum, the terms of use shall address: Indemnification of the disclosing party and ICANN.	This may require further discussion and input – not clear if this is possible or feasible?

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
	Red flag: this is likely not possible. We can discuss insurance, bonding, and other options, but many requestors (e.g. law enforcement and other government uses) will not be able to indemnify. (IPC)		

LOGGING

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
#64	I think we should split ID provider and accred provider into separate bullets. This verbiage seems to conflate them. (BC) Identity or accreditation provider? (IPC)	At a minimum, the following events must be logged: • Logging related to the Identity Provider • **Logging related to the accreditation provider**	

IMPLEMENTATION GUIDANCE

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
#66	Problem is, multiple requests at the same time is NOT consistent with the preliminary recommendation. We could not accept this formulation. (NCSG) I don't see any inconsistency, as we noted above. (IPC) I don't envisage any mechanism which would enable this within SSAD (BC)	Current wording: The EPDP Team recommends that, consistent with the preliminary recommendation that an SSAD request must be received for each domain name registration for which non-public registration is requested to be disclosed, it must be possible for requestors to submit multiple requests at the same time, for example, by entering multiple domain name registrations in	These comments also come up in other sections but the issue of multiple requests has been discussed and it was agreed that this is addressed by the recommendation that each request should be considered on its merits – regardless of whether it was submitted in a batch or individually. Why is this not considered sufficient?

# on Issue List	Comment (by)	Proposed Rewording (in bold)	Leadership Notes
	submitting multiple domain names in the same request dos not mean that it will be handled as one single request (ALAC)	the same request form if the same request information applies	