INPUT RECEIVED ON DRAFT INITIAL REPORT – STATUS 13 JANUARY 2020

Item	Page number (Google Doc)	Original Text	Comment / Proposed Change (By)	How to address
#1.	N/A – Overarching Comment		The EPDP team spent substantial time on the development of use cases. Whilst these were primarily worked on to serve as the factual basis for policy recommendations, we do think they should be made part of the report to inform both the community as well as those tasked with the implementation of the recommendations as they will then be in a position to test implementation for legal feasibility concerning our use cases (Are the use cases actually scenarios in which disclosure is legally possible?) and completeness (Have we considered all use cases that the EPDP team had in mind when drafting the policy recommendations?). If the EPDP team supports such reference to the use cases, we would be happy to help draft language for the report. (ISPCP)	
#2.	N/A – Overarching Comment		The SSAD shall be a globally applicable system goverened by ICANN based on community policy development. The SSAD might appear to be limiting and cumbersome to parts of the community and other stakeholders. We do think the report would benefit from a clarification describing that	

			going through the SSAD is one of two avenues for requestors to ask for non-public registration data. Requestors can use the SSAD, but they can also approach contracted parties directly. This applies particularly to public authorities who wish to obtain information from domestic contracted parties. Again, we would be happy to offer language for this if the EPDP team is supportive of such approach. (ISPCP)	
#3.	N/A – Overarching Comment		CPH proposal for a path forward to completing our work on a disclosure model – see https://mm.icann.org/pipermail/gnso-epdp-team/2020-January/002895.html (CPH)	
#4.	7 (Executive Summary)	Following the publication of this Report, the EPDP Team will: (i) continue to seek guidance on legal issues from the European Data Protection Board and others, (ii) carefully review public comments received in response to this publication, (iii) continue to review the work-in-progress with the community groups the Team members represent, and (iv) carry on deliberations for the production of a Final Report that will be reviewed by the GNSO Council and, if approved, forwarded to the ICANN Board of Directors for	The next steps should include the publication of the second / separate Initial Report and what will happen after that. If a separate Initial Report is going to be published, will a consolidated Initial Report be published? We should be clear on the next steps. (ISPCP)	Staff support to update language to reflect that a separate Initial Report will be published for priority 2 items which will follow its own timeline (i.e. no consolidated Initial Report is expected to be published).

		approval as an ICANN Consensus Policy.		
#5.	5 (EPDP Team Approach)	During phase 1 of its work, the EPDP Team was tasked to determine if the Temporary Specification for gTLD Registration Data should become an ICANN Consensus Policy as is, or with modifications	I would suggest that we tell the world how we answered that question (NCSG)	Staff support to update language to refer to phase 1 outcomes
#6.	9 (EPDP Team Approach)	recognizing that a decision on the roles and responsibilities of the different parties involved may be influenced by both legal advice and guidance from the European Data Protection Board ("EDPB"). In the absence of this guidance,	Propose to delete this. It adds no substance to the report and does not have any bearing on the three variations we outline. (NCSG) This part adds substance as part of our determination on which model to choose depends on the legal feedback and guidance provided by the EDPB (ALAC)	
#7.	9 (EPDP Team Approach)	the EPDP Team established that there would be roughly three variations of the SSAD: 1. Centralized model in which requests for access/disclosure are received through a central gateway, where the decision on whether to disclose data would be made by the entity responsible for managing the centralized gateway; 2. Hybrid model in which requests for access/disclosure are received through a central gateway, where the decision on whether to	We should consider suggesting one of the three variations as the "currently preferred" option. We support working on the first variation and centralizing as much as possible for reasons of consistency and to take work load off the contracted parties. (ISPCP) We cannot represent this as a "variation of the SSAD" for public comment. It would be confusing to the community if we presented this as a potential way to deliver an SSAD. We already have Model 3 today, and	

		disclose data would remain with the relevant contracted party; 3. Decentralized model in which requests for access/disclosure would be received by the relevant contracted party and the decision on whether to disclose would be made by the relevant contracted party (status quo, but with newly-defined standardized requirements).	will continue to have this regardless of whether we deliver variation 1 or 2 as an actual SSAD. We would therefore ask that this be listed as the present and permanent method, and we should solicit comments as to whether the SSAD should take the form of Model 1 or Model 2. (IPC) The third model, which is the status quo under Recommendation 18, will not scale to support cybersecurity incident response (e.g. member of RrSG has reperatedly warned that it will be hard to find qualified staff to perform these functions and that many Rrs will simply not attempt to do so). (BC) Model 1: when did we ever agree that the entity responsible for managing the centralized gateway would be responsible for the decision making as well? The centralized model - according to our discussions includes a centralized gateway, an identity provider and an authorization provider (decision maker). Whether the manager of the central gateway will also be the decision maker or not has not been discussed (It could be) however no such thing has been	

			concluded. What has been agreed that the decision would be made within the the centralized model by the authorization provider. This is also not consistent with other parts of the report, where we note on page 22 and 23 under Recommendation 6 " this confirmation could also be the responsibility of the central gateway manager if the manager is not the same entity as the authorization provider" (ALAC)	
#8.	9 (EPDP Team Approach)	The Centralized model may have variations with respect to how data is returned to the requestor. For example, the central gateway may return the data via its system, or, alternatively, the contracted party may return the data directly to the requestor following instruction from the authorization provider.	I still do not recall ever discussing this or anyone proposing it. Raises issues regarding logs, does it not? (NCSG) Logging is addressed below in terms that apply regardless of which party discloses the data. I am confident that these details can be worked out as in the other models. (BC)	
#9.	11 (Intro)	The EPDP Team will not finalize its responses to the charter questions and recommendations to the GNSO Council until it has conducted a thorough review of the comments received during the public comment period on this Initial Report. Additionally, if the EPDP receives further guidance from the European Data Protection Board ("EDPB"), the EPDP Team will consider this guidance in its Final Report. At the time of	The introductory paragraph suggests that the EPDP team might receive further guidance from the EDPB. In fact, the EDPB has never offered guidance to the EPDP team, but to ICANN. (ISPCP)	Staff support team to update this section to reflect that ICANN Org may receive guidance that may help inform the EPDP Team's deliberations.

		publication of this Report, no formal consensus call has been taken on these responses and preliminary recommendations; however, this Initial Report did receive the support of the EPDP Team for publication for public comment. Where applicable, differing positions have been reflected in the Report.		
#10.	11 (SSAD description)	Centralized model in which requests for access/disclosure are received through a central gateway, where the decision on whether to disclose data would be made by the entity responsible for managing the centralized gateway	Is there a reason why we talk about "the entity" and not ICANN? Is there any other "entity" that would be able to do this? (NCSG) Replace all references to "entity responsible" with "ICANN or its designee" (BC) I'd see this as "ICANN or its designee" (IPC)	
#11.	12 (Graphics)	See graphics	The org has some questions and comments for the team's consideration as it further develops these graphics: * It may be helpful to separate authentication from accreditation, as accreditation is possible after a user has been authenticated. * There is an appeal process indicated in all three. The team has not discussed this in much detail. Can the team provide more clarity on this point? How would these be handled?	

			What are the criteria? Who handles the costs? * There is also a complaint process noted in the chart. Similar to the questions above, can the team provide clarity on the details here? * The block that indicates whether a request is approved may be clearer if stated as a user is authenticated, as the request is not yet approved until the query has been authorized. * The box named “process request” seems unnecessary, the next step in processing after the request is acknowledged should be the authorization. * The contracted party responses are depicted in the design with multiple cards. Can the team explain the intent here? Does it mean there could be multiple responses to a single query? (ICANN Org Liaisons)	
#12.	12 (Graphics)	Model 1 graphics	Some more comments/questions related to model 1: * In the steps for executing the query and assembling the response to the requestor, the EPDP may want to indicate if the query to the contracted parties is going to be for the full data and then the SSAD will return to the requestor the subset that corresponds to the appropriate level of authorization , or if the query to the contracted party is going to ask for	

			the specific subset the requestor is authorized to access. * In the step where the contracted parties generate the response, the diagram design depicts multiple responses. It’s unclear what that means. Can the team clarify?. (ICANN Org Liaisons) There are 2 "Submit request" boxes in the Model 1 demand side swimlane. These should be replaces with "Submit request(s)". Likewise revise "Generate Response" and other singulars --> plurals. Perhaps Eleeza's "multiple responses" comment is related to this ambiguity? (BC)	
#13.	13 (Graphics)	Model 2 graphics	One question and comment that applies to both Model 2 and 3: The box “execute RDS query” seems unnecessary in these models since the contacted party is the authorized they could simply proceed to generate the response from their internal systems, the RDS wouldn’t need to be involved. (ICANN Org Liaisons)	
#14.	14	As of this Report’s publication, the EPDP Team has not yet decided *on a conclusive model*.	Replace with "which model it prefers. (NCSG)	Staff support team to make proposed update
#15.	14 (SSAD description)	Some members advocate for ICANN to take on this role, while others prefer Contracted Parties to remain responsible for making this determination. Some members of	We need either to delete this or to replace it with a more detailed and balanced discussion of the merits and de-merits of the three models. (NCSG)	

		the EPDP Team are of the view that a centralized model will result in increased uniformity and predictability, while a decentralized model will likely result in increased inconsistency and decreased predictability. Nevertheless,	according to the models we have been discussing the disagreement is mainly about whether the contracted parties should be the decision makers or an authorization provider (which would be one of the elements of the central gateway) should be the decision maker. But I don't recall that we actually discussed who this authorization provider would be, the authorization provider could be ICANN or any other entity. In the reply of ICANN org to the letter sent by the EPDP team in relation to the responsibilities that ICANN is willing to take, they indicated they are willing to take the role of the gateway operator. However according to the assumed model the gateway operator doesn't make the decision but the authorization provider does. My point here is that we never concluded who the authorization provider is. Therefore I would suggest replacing ICANN with an authorization provider and explaining what we mean by this (ALAC).	
#16.	16-21 (Accreditation)		The section after the definitions has headings in between paragraphs. These headings are not always matching the content of the following paragraphs and are at times misleading. We suggest to delete the headings. (ISPCP)	Staff support team to review issue with headings and address accordingly.

#17.	16 (Underlying Assumptions)	The objective of the SSAD is to provide a predictable, transparent and accountable mechanism for the access/disclosure of non-public registration data.	add "efficient" to the list of adjectives (NCSG) +1 (ALAC)	Staff support team to make proposed update
#18.	16 (Underlying Assumptions)	Compliance with the GDPR and other applicable data protection legislations for all parties involved underpins the SSAD.	Wording needs to be clearer and stronger. Replace with: "The SSAD must be compliant with the GDPR and other applicable data protection laws for all parties." (NCSG)	Staff support team to make proposed update
#19.	16 (Underlying Assumptions)	The mechanism chosen to *ultimately implement the SSAD must have the ability* to adhere to these policy principles and recommendations	Replace with "The mechanism chosen to implement the SSAD must adhere to these policy principles and recommendations. (NCSG)	Staff support team to make proposed update
#20.	16 (Accreditation)	Accreditation Authority Auditor - *Independent entity that is contracted by ICANN org* to carry out auditing requirements as outlined in auditing preliminary recommendation.	This can be either ICANN itself or an entity with which it contracts (IPC)	
#21.	17 (Accreditation)	De-accreditation of Accreditation Authority – An administrative action by which ICANN org revokes the agreement with the accreditation authority following which it is no longer approved to operate as the accreditation authority.	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 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)	
#22.	17 (Accreditation)		A term that could be added is De-authorization of identity provider (ALAC)	
#23.	17 (Accreditation)	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.*	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)	
#24.	18 (Accreditation)	f. Assertion as to the purpose(s) of the request	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)	

#25.	18 (Accreditation)	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 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*.	Suggest "preferable where lawful" (BC / IPC)	
#26.	18 (Accreditation)	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: • A clear and concise explanatory statement. • A defined scope that determines the processing operations covered (the focus for SSAD would be on the Disclosure operation.) • Mechanism that allow for the monitoring of compliance with the provisions. • Identification of an *Accreditation Body Auditor*	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	

		(a.k.a. monitoring body) and definition of mechanism(s) which enable that body to carry out its functions. - Description as to the extent a "consultation" with stakeholders has been carried out. - Etc.	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)	
#27.	19 (Accreditation)	j) MUST define a dispute resolution and complaints process.	Add: "to challenge actions taken by the Accreditation Authority" to clarify the scope of the dispute resolution and complaints process. (ISPCP)	
#28.	20 (Accreditation)	t) Will not be restricted in the number of SSAD requests that can be submitted 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.	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 RDAP is the most likely protocol and that each request will be a discrete event occuring in in a series. (BC)	
#29.	20 (Accreditation)	The accreditation service should be part of a cost-recovery system. For further details, see the financial sustainability preliminary recommendation.	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)	
#30.	21 (Accreditation)	Logged data shall only be disclosed, or otherwise made available for review, by the Accreditation Authority or Identity Provider, where disclosure is considered necessary to a) fulfill or meet an applicable legal obligation of the Accreditation Authority or *Identity Provider; b) carry out an audit under this policy or;* c) to	This language is not legible (looks like one text on top of another). (GAC)	

		support the reasonable functioning of SSAD and the accreditation policy.		
#31.	22 (Purposes)	Preliminary Recommendation #4 - Third Party Purposes/Justifications	As noted in our calls, using the term "purposes" here is confusing at best and misleading at worst. These are justifications, not purposes. We'd like for this heading to read "Third Party Justifications." (NCSG)	
#32.	22 (Purposes)	As identified in the preliminary recommendation relating to criteria and content of requests, each request must include information about the legal rights of the requestor specific to the request and/or specific rationale and/or justification for the request, e.g. What is the basis or reason for request; Why is it necessary for the requestor to ask for this data? *The EPDP Team expects that over time, the entity responsible for receiving requests will be able to identify certain patterns that could result in the development of a preset list of rationales and/or justifications that a requestor can select from, while always maintaining the option for the requestor to provide this information in free form".*	This section requires further discussion. We recommend to not include the section until it is further matured. (ISPCP) NCSG is not entirely comfortable with this. This language might be acceptable if it makes some reference to Preliminary Recommendation #6 below (Auth provider MUST review every request on its merits...") (NCSG) IPC supports this kind of flexibility, to allow adaptation of the SSAD on the basis of experience. However, we expect we'll oppose eventual adoption by the EPDP of its final report if it does not provide a list of purposes identified as legitimate. (IPC)	
#33.	22 (Purposes)	Comment to section: To be further considered by EPDP Team.	We (NCSG) will have to oppose this language. The inclusion of these	

		Proposed language by BC: “The EPDP recognizes that third parties may submit data disclosure requests for the following specific purposes: (i) criminal law enforcement, national or public security, (ii) non law enforcement investigations and civil claims, including, intellectual property infringement and UDRP and URS claims, (iii) contacting registrants, (iv) consumer protection, abuse prevention, digital service provider (DSP) and network security, or (v) Registered name holder consent or contract.”	"specific purposes" seems to imply that any request that invokes them is legitimate and legal. Some of these purposes (e.g., contacting registrants) clearly will not justify disclosure in most cases. (NCSG)	
#34.	22 (Receipt of Acknowledgement)	Receipt of Acknowledgement	Replace with “Acknowledgement of receipt” (IPC)	
#35.	22 (Receipt of Acknowledgement)	*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.	"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)	

#36.	22 (Authorization Provider)	1. The authorization provider MUST review every request on its merits and MUST NOT disclose data on the basis of accredited user category alone. For the avoidance of doubt, automated review is not explicitly prohibited where it is both legally and technically permissible	Regarding the proposed language in Section 1, could a computer confirm whether or not all the requirements for a request are met and, if so, automatically arrange for the release the data, or does each request have to be reviewed for substance? Does this section simply mean that the authorization provider MUST NOT disclose data on the basis that the requestor is accredited in a specific user category? (ICANN Org Liaisons) A computer could confirm whether the requirements are met or not but this does not mean that the data could be automatically released. There is a difference between automated review and automatic disclosure and yes the authorization provider should not release the data based ONLY on the specific category of the requester. (ALAC)	
#37.	22-23 (Authorization Provider)	2. The authorization provider MUST confirm that all required information as per building block a) 'criteria and content of requests' is provided. Should the authorization provider determine that the request is incomplete, the authorization provider must reply to the requestor with an incomplete request response, detailing which required data is	Section 2 makes reference to building block a and Section 4 makes reference to preliminary recommendations 3 and 5. The reference to the building block needs to be removed and the preliminary recommendations do not match this report. (ISPCP)	Staff support to update this section and remove the reference to building block and confirm # of preliminary recommendations referenced.

		missing, and provide an opportunity for the requestor to amend its request. [Note: this confirmation could also be the responsibility of the central gateway manager if the manager is not the same entity as the authorization provider.		
#38.	23 (Authorization Provider)	3. While the requestor will have the ability to identify the lawful basis under which it expects the authorization provider to disclose the data requested, the authorization provider must make the final determination of the appropriate lawful basis.	In Section 3, whose "appropriate lawful basis" is the authorization provider required to determine? If this is a party other than the authorization provider, how would the authorization provider be expected to make this determination? (ICANN Org Liaisons)	
#39.	23 (Authorization Provider)	4. The authorization provider should make a threshold determination (without processing the underlying data) about whether the requestor has established an interest in the disclosure of personal data. The determination should consider the elements: • Is the identity of the requestor clear/verified? • Has the requestor provided a legitimate interest or other lawful basis in processing the data? • Are the data elements requested necessary to the requestor's stated purpose?	Ref to User Groups - Delete for accuracy since this is gone. We agreed to deletion User Groups only if Purposes is sufficiently explicit. (IPC) 'Usefulness and necessity of data elements' - At it stands, Rec#3 provides no such guidance. This shows why not using the User Groups we had developed, and not providing a list of purposes identified as legitimate, makes no sense: without them, the authorization provider(s) has/have to develop, and regularly update, by itself/themselves expertise on the data elements that are necessary for various types of requestors/purposes. (IPC)	

		○ Necessary means more than desirable but less than indispensable or absolutely necessary. • Using the guidance provided in *Preliminary Recommendation 3 (User Groups)* and/or 5 (Purposes) about the usefulness and n*ecessity* of data elements, the authorization provider should determine whether Are the data elements requested are *limited and reasonable* to achieve the requestor's stated purpose? ○ Each request should be evaluated individually (i.e. each submission should contain a request for data related to a single domain. If a submission relates to multiple domains, each must be evaluated individually.). ○ In addition, each data element in a request should be evaluated individually. If the answer to any of the above questions is no, the authorization provider may deny the request, or	Q: We should clarify the distinction between "necessary" (previous bullet) and "limited and reasonable." (IPC) I prefer "limited and reasonable", and would be fine with "proportional". We've seen repeated confusion regarding "necessary" in spite of clarification in B&B 13Feb2019 3.6/7/8 (BC) 'deny the request' - Add: "or may deny the request for those data elements which have not been deemed necessary" (IPC)	

		require further information from the requestor before proceeding to paragraph 6 below.		
#40.	23 (Authorization Provider)	5. The authorization provider may evaluate the underlying data requested once the validity of the request is determined under paragraph 4 above. The purpose of paragraph 5 is to determine whether the paragraph 6 [meaningful human review] is required. The authorization provider's review of the underlying data should assess at least: • Does the data requested contain personal data? • If no personal data, no further balancing required. • *If the requested data contains personal data the authorization provider should consider if the balancing test, similar to the requirements under GDPR's 6.1.f, as described in paragraph 6 below is applicable and proceed accordingly.*	Section 5, second bullet point: Replace current language with: If the requested data contains personal data, the authorization provider must establish the presence of a legal basis for disclosure according to Art. 6 of the GDPR. (ISPCP) What about the other Art. 6 lawful bases which do not require a balancing test ? Do we need to add what factors the Authorization Provider should consider for these other bases? This language seems to imply that the balancing test applies to all requests. (GAC)	
#41.	23-24 (Authorization Provider)	*6. The* authorization provider should evaluate at least the following factors to determine whether the legitimate interest of the requestor is not outweighed by the interests or fundamental rights	As we noted during the team's most recent discussion on this, the building block seems to assumes that, at least in some cases, the authorization provider may review the underlying registration data in considering	

		and freedoms of the data subject. No single factor is determinative; instead the authorization provider should consider the totality of the circumstances outlined below: ● **Assessment of impact**. Consider the direct impact on data subjects as well as any broader possible consequences of the data processing (e.g., triggering legal proceedings). Whenever the circumstances of the disclosure request or the nature of the data to be disclosed suggest an increased risk[1] for the data subject affected, this shall be taken into account during the decision-making. ● ***Nature of the data***. Consider the level of sensitivity of the data as well as whether the data is already publicly available. ● ***Status of the data subject***. Consider whether the data subject's status increases their vulnerability (e.g., children, other protected classes) ● ***Scope of processing***. Consider information from the	whether to authorize a request (see Section 6: "The authorization provider may evaluate the underlying data.."). We believe that this raises important issues that need to be carefully considered by the EPDP team. If the authorization provider is an entity other than the contracted party, the authorization provider's review of registration data in the course of evaluating a request for access will require processing of that data (whether the request is granted or not). This processing must have its own appropriate legal basis and will require the contracted party to transfer the data to the authorization provider (resulting in a potential need for transfer safeguards). The "balancing test" factors listed in Section 7 may not be meaningfully determined on the basis of information derivable from the underlying registration data, nor can the application of the GDPR be safely derived from the underlying registration data. For example, a registrant's age (and status as a member of a potentially vulnerable population) is unlikely to be determined based on registration data, and a review of a registrant's	

[1] [include reference to relevant GDPR provision]

		disclosure request or other relevant circumstances that indicates whether data will be [securely] held (lower risk) versus publicly disclosed, made accessible to a large number of persons, or combined with other data (higher risk), .[provided that this is not intended to prohibit public disclosures for legal actions or administrative dispute resolution proceedings such as the UDRP or URS]. ● ***Reasonable expectations of the data subject***. Consider whether the data subject would reasonably expect their data to be processed/disclosed in this manner. ● ***Status of the controller and data subject***. Consider negotiating power and any imbalances in authority between the controller and the data subject. ● ***Legal frameworks involved***. Consider the jurisdictional legal frameworks of the requestor, Contracted Party/Parties, and the data subject, and how this may affect potential disclosures.	email address may not be determinative as to whether that address contains personal data or not. We would encourage the team to consider this threshold issue before finalizing this building block. We believe it may be possible for the relevant interests of the requestor and data subject to be balanced on a use case basis, provided the use cases are sufficiently specific. This could eliminate the need for the authorizer to review the underlying data, reducing associated legal and operational risks, and could also facilitate automation. If the EPDP team does recommend that the authorization provider may or must review the registration data, the team should be specific about whether this is a MAY or a MUST, an (ICANN Org Liaisons) The way this is drafted implies that this test is done in all cases (for all requests). This should be limited to cases where the balancing test is necessary (i.e. where the RNH data is personal data, and where the disclosure is based on 6.1.f.). (IPC)	

			Nature of the data – publicly available: Ok if that includes “for free.” and available in the RDDS. (IPC) Legal frameworks involved. Consider the jurisdictional legal frameworks – Unclear (IPC)	
#42.	24 (Authorization Provider)	**Assessment of impact**. Consider the direct impact on data subjects as well as any broader possible consequences of the data processing (e.g., triggering legal proceedings). Whenever the circumstances of the disclosure request or the nature of the data to be disclosed suggest an increased risk[10] for the data subject affected, this shall be taken into account during the decision-making. [10] [Include reference to relevant GDPR provision]	Section 6, first bullet point: Remove the footnote. There is no specific section in the GDPR on this. The language was discussed to ensure that the authorization provider takes into account the risks for the data subject under the given circumstances for each case. It may well be that an alleged crime might lead to financial fines or prison in most jurisdiction (“normal risk”), but it may lead to corporal punishment or torture in other jurisdictions, which is what would establish an increased risk. We can be more wordy, but the essence is that the legal framework of the jurisdiction of the requestor needs to be taken into account. The same would go for alleged crimes that could lead to death penalties. We could clarify that the balancing test should take into account criteria for MLADs. In other words: The SSAD should not go further in offering information on alleged criminals than would be given through “official channels”. (ISPCP)	

#43.	25 (Authorization Provider)	Implementation Guidance As noted in paragraph 4 above, in situations where the requestor has provided a legitimate interest for its request for access/disclosure, the authorization provider should consider the following: • Interest must be specific, real, and present rather than vague and speculative. • *An interest is generally legitimate so long as it can be pursued consistent with data protection and other laws.* • Examples of legitimate interests include: (i) enforcement of legal claims; (ii) prevention of fraud and misuse of services; and (iii) physical, IT, and network security.	How is it envisioned that requirements for the authorization provider will be enforced? If the authorization provider is the contracted party, this requirement could be enforced under existing compliance processes. But if the authorization provider is a third party, who would oversee those decisions? Or what if the authorization provider is ICANN? (ICANN Org Liaisons) If the authorization provider is ICANN, then enforcement will have to come from the Data Protection Authorities. Any and every decision ICANN makes would be subject to scrutiny and potential legal challenge, which seems burdensome and is one reason we favor distributing responsibility across the relevant contracted party. (NCSG) We seem to be converging on ICANN or its designee as "the entity", so I would assume that any 3rd party would be under contract to ICANN. (BC) Implementation Guidance, p.26, second bullet point: “An interest is generally legitimate so long as it can be pursued consistent with data protection and other laws”.	

			This statement is too broad. We cannot tell what all data protection laws globally would allow for and whether that would meet our legal standards. This reservation is even more true for “other laws”. A lot of laws would permit for exactly what we are trying to protect registrants against. The implementation guidance does not seem to offer a lot of benefit, so we suggest deleting this entire section. (ISPCP)	
#44.	25 (Response Requirements)	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.	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) is most certainly not acceptable. (NCSG)	

			'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)	
#45.	26 (Response Requirements)	The EPDP Team recommends that if the entity disclosing the data determines that disclosure would be in violation of applicable laws *AND* result in inconsistency with these policy recommendations, the entity disclosing the data must document the rationale and communicate this information to the requestor and ICANN Compliance (if requested).	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)	
#46.	26 (Implementation Guidance)	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	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)	

		reply 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. d. 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]		
#47.	27 (Acceptable Use Policy)	a) Must only request data from the current RDS data set (no historic data)	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) 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)	
#48.	27 (Acceptable Use Policy)	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);	‘and every unique’ - Unclear and redundant: delete. (IPC)	
#49.	27 (Acceptable Use Policy)	c) MAY request data from the SSAD for multiple purposes per request, for the same set of data requested;	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)	

#50.	27 (Acceptable Use Policy)	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);	‘intended use’ - Unclear how this is different from “stated purpose”. (IPC)	
#51.	27 (Acceptable Use Policy)	The EPDP Team recommends that the following requirements are applicable to the entity disclosing the data and must be confirmed by [TBC] and subject to an enforcement mechanism. For the avoidance of doubt, every response does not have to go through an enforcement procedure; the enforcement mechanism may, however, be triggered in the event of apparent misuse.	‘entity disclosing the date’ - Do we not mean “authorization provider” here? For example, the balancing test is performed by the authorization provider. (IPC)	
#52.	27 (Acceptable Use Policy)	g) Where required by applicable law, must provide mechanism under which the data subject may exercise its right to erasure;	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)	

#53.	27 (Acceptable Use Policy)	a) Must return current data or a subset thereof in response to a request (no historic data);	‘no historic data’ - Delete: it’s redundant with other language (see c. in last subsection of recommendation 9.) (IPC)	
#54.	27 (Acceptable Use Policy)	g) Where required by applicable law, must provide mechanism under which the data subject may exercise its right to erasure	Of what data, from what database, on what ground, and when/how/with what limits? If the authorization provider (or entity disclosing the data) isn’t the registrar, does that mean that: a. the RNH is given a new channel for editing his registration; and b. the authorization provider is supposed to keep a copy of the registration data? This might be a good opportunity to discuss in terms of obligations of controllers, perhaps in a JCA (IPC)	
#55.	27 (Acceptable Use Policy)	h) Confidentiality of disclosure requests – Data controllers of RDS data must make it clear to 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 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	2 comments: 1. Replace with “inform.” 2. When: upon request or in their privacy policy? (IPC)	

		cooperation with the requesting authority, [and] [or] in accordance with the data subject's rights under applicable law		
#56.	28 (Query Policy)	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:	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)	
#57.	28 (Query Policy)	a. Unless otherwise required or permitted, not allow bulk access, wildcard requests, [reverse lookups], nor boolean search capabilities.	Still don’t know what it means to say “unless otherwise required or permitted (NCSG). “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)	
#58.	29 (Query Policy)	d. Only return current data (no data about the domain name registration’s history)	Re: history, what about the domain's original date of registration? (NCSG)	
#59.	29 (Query Policy)	Requests must only refer to current registration data (historical registration data will not be made available via this mechanism).	Delete: it’s redundant with language in c. above. (IPC) redundant with 8(a) and 9(c)#2 (BC)	
#60.	28-29 (Query Policy)		The contents of this section must be mirrored or made reference to in the Acceptable Use Policy. (ISPCP)	Staff support team to update Acceptable Use Policy by including reference to query policy recommendation.
#61.	29 (Terms of Use)	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 • 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 shared • Where applicable, details of any international data	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) ‘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)	

		transfers/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.		
#62.	29 (Terms of Use)	The EPDP recommends, at a minimum, the terms of use shall address: • Indemnification of the disclosing party and ICANN.	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) 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)	
#63.	32 (Logging)	At a minimum, the following events must be logged Logging related to the Identity Provider	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)	
#64.	32 (Automation)	The SSAD [*must or should*] allow for automation of the processing of well-formed, valid, complete, properly-identified requests from accredited users with some limited and specific set of legal basis and data processing purposes which are yet to be determined. These requests MAY be automatically processed and result in the disclosure of non-public RDS data without human intervention.	Revisit factoring in guidance received from ICANN org (see https://mm.icann.org/pipermail/gnso-epdp-team/2019-December/002873.html.	
#65.	35 (Implementation Guidance)	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 the same request form if the same request information applies.*	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) submitting multiple domain names in the same request dos not mean that it will be handled as one single request (ALAC)	