Please review the Appendix A Discussion Summary Index before providing your input on these questions (not that the issues identified have been summarized so it is important to review the full context as outlined in DSI).

Appendix A: §2.1–2.3 – Cat 1 & 2A Issues

Issue	Questions	Your input on the questions (please identify your name and affiliation)
While the contact details of legal persons are outside the scope of GDPR, contact details concerning natural persons are within the scope. Personal identifying individual employees (or third parties) acting on behalf of the registrant should not be made publicly available by default in the context of WHOIS. If the registrant provides (or the registrar ensures) generic contact information, the EDPB does not consider that the publication of such data in the context of WHOIS would be unlawful as such. (EDPB Advice)	What changes, if any, need to be made in order to address the EDPB advice?	Margie - BC: The new policy should treat legal and natural persons differently. 1- As suggested by Benedict- adding a requirement that the Registrant indicate whether it is a legal or natural person. 2- If a legal person - require a notice that it should use role email addresses, and if there is an intent to use a natural person, obtain consent for the use of the personal data 3- all of the contact data of the legal person appears unredacted in the WHOIS data fields Alex - IPC: Agree with input from Margie--BC. Legal person registrants should be able to--and required to--self-identify and be informed that data privacy protections apply only to natural persons, not legal persons. For contact information for legal persons, they should be informed and encouraged to use non-personal data (e.g. "Administrator" instead of a person's name for e-mail contact). But if they

		choose to use personal data for such contact information, then they must declare that they have obtained the free consent of the relevant individual to use such individual's personal data and to make it publicly available. With the foregoing procedures in place, all registration data of legal person registrants should be required to appear and be unredacted in WHOIS data fields..
Redaction of Personal Data – should additional fields be redacted (organization) or should certain fields no longer be redacted (email address, registrant city and postal code)? Should a distinction be made between natural and legal persons when it comes to redaction?	What is the rationale for redacting additional fields or no longer redacting certain fields? Is there a risk of non-compliance with GDPR if changes are made? If so, are these risks that can be mitigated? Are possible changes reasonably easy to implement?	Margie - BC: CCTLDs have made the legal person/natural person distinction, so its feasible and implementable

Appendix A: §2.4 – Cat 1 & 2A Issues

Issue	Questions	Your input on the questions (please identify your name and affiliation)
Registrants should not be required to provide personal data directly identifying individual employees (or third parties) fulfilling the administrative or technical	What changes, if any, need to be made in order to address the EDPB advice?	Alex - IPC: See comments in response to first issue for suggested procedure to address and incorporate this EDPB Advice.

functions on behalf of the registrant. This should be optional – it should be made clear that registrant is free to (1) designate the same person as the registrant as the admin or tech contact; or 2) provide contact information which does not directly identify the administrative or technical contact person concerned (e.g. admin@company.com). (EDPB Advice)		

Appendix A: §4 – Cat 1 & 2A Issues

Issue	Questions	Your input on the questions (please identify your name and affiliation)
Appropriate logging mechanisms should be in place to log any access to non-public personal data processed in the context of WHOIS. (EDPB Advice)	What changes, if any, need to be made in order to address the EDPB advice or is this advice directed at controllers?	Alex - IPC: No objection to logging mechanisms put into place. However, further discussion needed on public vs. confidential nature of such logs and disclosure of access requests to registrant. For example, important that requests from law enforcement remain confidential (at least for some period of time). markSv - BC: We agree that logging mechanisms must be in place and that there must be a balance of confidentiality (where justified, as in some law enforcement actions) and accountability (even law enforcement could be subject to audit under certain circumstances). We also feel that the

		logs should be maintained and administered centrally by ICANN to ensure consistency of format, reduce technical impact on contracted parties, and to shield contracted parties from any risks related to the disclosure of logged information.
Does this section need to be modified as not all disclosure of data will take place on the basis of Art. 6(1) (f) of the GDPR?	What are the views in this regard? What are the risks, if any, of modifying this reference?	Alex - IPC: Section 4 of Appendix A concerning Access focuses nearly exclusively on the basis articulated in Art. 6(1)(f) of the GDPR. This is not the only basis on which access to non-public/redacted Registration Data may occur. For example, access to such data may be granted, under Article 2(d) of the GDPR to "competent authorities for the purposes of prevention, investigation . . . of criminal offences. . ." because the GDPR itself does not apply to the processing of personal data under those particular circumstances. Similarly, under Article 6(1)(d) of the GDPR processing that is "necessary in order to protect the vital interests of the data subject or of another natural person" is not subject to the balancing test set forth in Article 6(1)(f). These are but two of several examples. Therefore, Section 4 of Appendix A is too narrowly crafted and doesn't take into account an important array of

		circumstances for which processing--and therefore access to-non-public/redacted Registration Data--is warranted and permitted in accordance with the GDPR. It therefore needs to be expanded to take into account these other circumstances and bases for access.

Appendix A: Cat 2B Issues

Issue	Questions	Your input on the questions (please identify your name and affiliation)
Appendix A, §1 RDAP – should data for SLA definition be deleted or amended? Is the search capability paragraph necessary as it is already covered through existing agreements? Do the restrictions in this section address the risks associated with the aggregation of data?	What changes, if any, should be made to address these issues?	Margie (BC): The policy needs to accommodate the ability to conduct large volume, multiple query searches as needed for specific purposes that require correlation analysis (ie cybersecurity)
Appendix A, §4 What is meant with 'reasonable'? Should this be further defined or deleted? Response from ICANN Org indicates that compliance with the term 'reasonable' is evaluated on a case by case basis, similar to how that is done in the context of other RAA provisions where the term 'reasonable' is used.	May not be possible to find a one size fits all definition of what is meant with reasonable? Should focus instead be of identifying examples of what is considered reasonable / unreasonable to provide guidance to compliance enforcement of this requirement?	Alex – IPC: The IPC submits that the word "reasonable" should be maintained and that policy should be set that defines reasonable requirements for requests, and reasonable commitments/requirements/etc. for responses (specificity, timeliness, etc) While there is no "one size fits all" definition of "reasonable," there is a

		dictionary and regularly-used and acceptable legal definition that is relevant and important here “as much as is appropriate.” Reasonable in this Section 4 is necessary to apply the required laws and legal obligations herein and to address the comment above that Section 4 is far too narrowly drafted in terms of addressing the various warranted circumstances and bases for granting access to non-public/redacted Registration Data in accordance with the GDPR. To try to list examples would be an endless and inaccurate mechanism through which to continuously try to find adaptive application. Margie BC: In our experience, the current implementation of “reasonable access” is unworkable and unsustainable. We are seeing very low response rates, despite the fact that we have provided legal basis, letters of authority, and evidence of our rights to access the full WHOIS contact data. We will be sharing statistics from the last few months shortly. The new policy emerging from this EPDP must have specificity and required timeframes for response marksv (BC) Here’s a proposal for “reasonable access:

		1. Reasonable requirements of the request for a domain name record :
		    1. Identity of the requestor
		    2. Domain name
		    3. Legal basis for processing
		    4. Commitment to process lawfully and/or under some code of conduct or terms of use, including model clauses
		    5. Contact info for company data privacy officer, when available
		2. Reasonable commitment/requirement/SLA for the contracted party:
		    1. CPs should explicitly designate an email address or web form where requests should be made
		    2. A response should be sent within 24 hours acknowledging receipt of the request.
		    3. Confirmation that request is approved or denied should be sent within 7 days.

		4. Requests should be processed in good faith (e.g. no “blanket denials”). 5. Denied requests must be provided with a written explanation.It may be helpful if there is a standard list of responses that all CPs can consistently use. 6. If a requestor makes a request for which they are not authorized, only public data and the defined error code shall be returned 7. CP should return data provided by the registrant, appropriate to the legal basis submitted by the requestor. 8. All details of the query are logged. Logs are maintained for at least as long as the data being accessed. 9. Special considerations can be made to maintain certain query logs as non-public (e.g. when related to Law

		Enforcement and cybersecurity), but there shall be no unlogged access. 10. CPs may display specific terms of use for the data which are appropriate to the legal purpose under which the data was requested. .
Appendix A, §2.3 & 2.4 There is no established and widely used mechanisms for obtaining or tracking this consent, or passing that consent from the Registrar to the Registry Operator.	Is further guidance from the EPDP Team necessary here or is this an implementation issue?	
Other issues?		