Appendix A relevant input	**Relevant input Appendix A – section 4:** RySG: Changes to the access requirements outlined in Section 4 of Appendix A should be considered during discussions of a standardized access model, which will take place later in the ePDP, following the discussion of the other elements of the Temporary Specification and completion of the Gating Questions in the ePDP Charter. Early input feedback: The WG should defer access discussions until after it has completed its deliberations on other Temporary Specification elements and answered the gating questions set forth in the WG's charter. (App. A, § 4) The RYSG believes that the parties involved in the processing of data to effect domain name registrations are in the unique position of defining purpose. The EDPB has stated that third party purposes (i.e., access) should not be included in that effort. The RYSG looks forward to dedicating time to discussing a more standard and predictable approach to access at a later stage within the EPDP. RrSG: A court of competent jurisdiction has decided that access to personal data was appropriate in a single case, it may not be extrapolated that either, (a) access to that personal data is appropriate in all cases, (b) access by that party to other personal data is appropriate in all cases, or (c) access by similar parties to similar data is appropriate in any case. So while 4.2 is fine as written, there are significant opportunities for ICANN or other interests to stretch the meaning of it until personal data protection is a mere collection of words with no meaning whatsoever. For example there are huge issues with the concept of giving access to a "class of third party". IPC: The IPC supports this section and strongly believes that the EPDP is responsible for developing policy that defines the term "reasonable access" which will enable access to non-private whois data as permitted by the GDPR. This includes the concept of "tiered access" and its implementation via the RDAP protocol. Regarding providing reasonable access the IPC believes that 90 days is too long suggests that access should be required as soon as commercial feasible but in no event longer than 15 calendar days, which is consistent with the time period in which registrars must comply with the requirements of the current WHOIS Accuracy Specification under the 2013 RAA, unless the time period for publication or disclosure is otherwise specified by the applicable legislation, court order, or other binding legal authority. The IPC also believes that Section 4.2. is too limited and doesn't take into account law enforcement and other processing even under GDPR that is NOT subject to the balancing test. At the very minimum, there should be added here a new Section 4.2 that reads as follows and existing Section 4.2 should become 4.3: "Registrar and Registry Operator MUST provide immediate access to Personal Data in Registration Data to competent authorities that seek access to Personal

	Data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Such access shall be granted without any financial charge and the Processing of such Personal Data by such competent authorities is not subject to any restrictions or qualifications that may be set forth in this Temporary Specification and Registrar and Registry Operator may not impose any restrictions or qualifications." The suggested language follows from Article 2(d) of the GDPR. Access and processing of personal data by law enforcement is not subject to the GDPR and therefore is not subject to any restrictions set forth in the GDPR. ICANN org has utterly failed to recognize this critical point in the Temporary Specification and has arguably violated its Charter and By-laws by so doing. BC: BC agrees with this section and suggests the following topics for future discussion: • While we anticipate that "reasonable access" will require RDAP and differentiated ("tiered") access, it is the task and responsibility of this policy development panel to work out the definition for reasonableness - panel must delineate processes, timelines, and detailed expected response from Registries and Registrar to reasonable access requests based on legitimate interests as allowed under the GDPR. • As mentioned elsewhere, it may be too soon to determine whether service level assurances ("SLA") such as "within 90 days" are appropriately quick or technically achievable. At this moment, 90 days seems excessively long for most cases. • Regardless of the SLA for access that is ultimately decided, if a Registrar or Registry is presented with an ambiguous situation (where ICANN has not yet published guidance), we believe that there must be an obligation on the Registrar or Registry operator to take immediate action to seek guidance upon receiving a request. Early input feedback: The BC is concerned about the over lack of a definition of "reasonable access" in the context of access to non-public registration data. The ensuing ambiguity has led contracted parties to make their own interpretations, many of them needlessly restrictive, which has then led to over-compliance with GDPR and fragmentation of the WHOIS system. We find that a description is within scope of the EPDP working group, which should work toward a practical definition of "reasonable access." Some have suggested that reasonable access may be achieved via the legal system. The BC believes this to be a spurious argument that presents users and contracted parties with burdensome processes. The BC instead advocates for a sensible approach to access --one that can be relied upon by those with legitimate reasons for access and contracted parties alike. Reasonable access can flow

	from an effective process for handling data requests, which could include A request that adheres to the parameters of the Temp Spec; • A review by the contracted party of the data request; and • An expeditious timeline for action and resolution by the contracted party; The BC notes the intersection of the recently released Uniform Access Model (UAM) and the efforts of the EPDP. We urge the working group to specify the types of access available to parties that are accredited using the UAM. E-mail Redaction Even for natural person registrants, certain data elements that are designated for redaction should not be redacted. At minimum, the registrant's e-mail address, as supplied to and verified by the registrar, should not be redacted. These views have been expressed repeatedly by the BC, IPC, the GAC and others over the past months both before and after the Temp Spec was issued. ISPCP: This section needs to be rewritten. Not all disclosure of data will take place on the basis of Art. 6 I f GDPR. Also, there is an issue with making disclosure of data mandatory with such a broad brush statement. This section is best amended when the access discussion has been held. GAC: Section 4 and related subsections: The GAC would like “reasonable access” defined. The GAC would also like these sections to be clarified to make clear that Registrar and Registry Operator responses to access requests are time bound and that any refusal to provide access be accompanied with a rationale for why. Early input feedback: It is not clear whether Appendix A section 4.4.8 (“Supporting a framework to address issues involving domain name registrations, including but not limited to: consumer protection and DNS abuse”) and section 4.4.9 (“Providing a framework to address appropriate law enforcement needs”) are formulated as defining a legitimate purpose in a way that is consistent with the GDPR. The GAC intends to review this language and provide alternative text (if necessary) to ensure that these purpose statements are constructed in a way that provides lawful basis for the processing of information. The GAC welcomes recent efforts in the EPDP Team to request appropriate clarification from the ICANN Org on Appendix A section 4 of the Temporary Specification. The GAC would like “reasonable

	access" to be clearly defined. As currently drafted, "reasonable access" can be interpreted in a variety of ways and does not offer a sufficient level of predictability for registry operators, registrars, or the users of the data. Additionally, the GAC would like these sections to be clarified to make clear that Registrar and Registry Operators must respond within a specified timeframe yet to be defined and that any refusal to provide access should be accompanied with a rationale. The GAC believes that the issue of "reasonable access," articulated in section 4 of Appendix A of the Temporary Specification, is a central component of the Temporary Specification, and must be addressed in the initial EPDP report. Consideration of section 4 of Appendix A should not be confused with the consideration of a "standardized access model" and other items listed in the Annex of the Temporary Specification dealing with "Important Issues for Further Community Action", which are set to be addressed at a later stage of the group's work, per relevant section of the EPDP Charter. Several sections of the Temporary Specification cannot appropriately be considered or agreed upon as they depend on the definition of a Registration Data Access Protocol (RDAP) Profile by a deadline that is now passed (31 July 2018). In its current form, and due to the lack of contractual relationship between ICANN and Resellers, it appears that none of the provisions of the Temporary Specification would apply to Resellers of ICANN-accredited Registrars. The EPDP Team should consider this issue when drafting its policy recommendations 4: Section 4 and related subsections: The GAC would like "reasonable access" defined. The GAC would also like these sections to be clarified to make clear that Registrar and Registry Operator responses to access requests are time bound and that any refusal to provide access be accompanied with a rationale for why. SSAC: No, because registrars and registry operators must be required to participate in a uniform, coordinated access program that allows predictable tiered access and credentialing. The current language in 26 allows all manner of non-uniform implementations, with no predictability and potentially large operational barriers. **Relevant input Appendix A - section 2.5.1**: RySG: The method(s) by which Registrars provide email communication to registrants outlined in Section 2.5 should be discussed further by the ePDP team.

	RrSG: In relation to 2.5.1.3 - RrSG applauds the sentiment, but the wording could do with a review. What does 'feasible' mean in this context? No system is completely resilient against hacking or other breaches. I think what we want is for contracted parties to take appropriate information security measures to protect the personal data that they process from breach or other intrusions. The response to privacy/proxy reveal requests needs more precision - what if no legitimate purpose is revealed in the request for data? In what timeframe ('reasonable'? other?) is the registrar required to provide the data? GAC: Section 2.5.1: GAC Representatives are seeking a unique anonymized email address to identify and reach a given contact across domains and gTLDs, consistent with GAC Advice. SSAC: SSAC agrees with 24 with the addition of the following: 1) If the registrar uses a web form, the URL of the registrar's web form must be published in the registrar's WHOIS/RDAP output. 2) If the Registrar or Registry Operator provides a web-based form or a general email address not customized to the domain, the Registry and Registry Operator must: a) provide an email receipt to the user of the web-based form or general email address stating that the email has been received and will be forwarded to the domain contact, and b) shall document delivery to the domain contact of the communications submitted via the web-based form or general email address. Registrar or Registry Operator shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period shall provide such records to ICANN upon reasonable notice. [This language is based on similar requirements in the RAA regarding abuse complaints.] BC: Final policy must accommodate circumstances beyond those supported by an unmonitored web form. Examples include providing a registrant's unique, verified email address (anonymized or other) and registrar being accountable to ensure that mail sent from a web form is received by the registrant and responded to within a defined time interval.
Relevant Discussion Summary Index	Appendix A