

Open Questions / Open topics identified in the zero draft	Volunteers to work on a draft response to serve as a starting point for further deliberations during the LA F2F meeting
Demand side: Requestor	
<p>Building block b) (Purposes) Legitimate interests identified are based on EPDP Team’s categorization of use cases – will need to be reviewed. For example, for e, if RNH has provided consent there may not be a need to go through SSD?</p>	
<p>Building block b) (Purposes) EPDP Team noted that rec 1, purpose 2 was a placeholder and should be further reviewed in the context of phase 2 deliberations. Also consider the European Commission on this topic, in its 17 April 2019 letter submitted during the public comment period and the clarifying letter sent to ICANN org on 3 May 2019.</p>	
<p>Building block c) (User Groups) List of user groups is based on users identified in use cases. This list will require further review and consolidation by EPDP Team.</p>	
<p>Building block d) (Acceptable Use Policy) EPDP Team to further define / clarify who and how auditing is expected to be carried out.</p>	
<p>Building block f) (Authentication / authorization / accreditation) Also need to address charter question a7) How can RDAP, that is technically capable, allow Registries/Registrars to accept accreditation tokens and purpose for the query? Once accreditation models are developed by the appropriate accreditors and approved by the relevant legal authorities, how can we ensure that RDAP is technically capable and is ready to accept, log and respond to the accredited requestor’s token? EPDP Team to consider reviewing Sections 5 and 6 in TSG01, which discusses technical requirements for credentials in RDAP.</p>	
<p>Building block f) (Authentication / authorization / accreditation) Further details would need to be provided about what the benefits of accreditation are.</p>	
<p>Building block f) (Authentication / authorization / accreditation)</p>	

<p>“shared with the EDPB for review” - Need to confirm what happens after this review – is it ICANN Org who then modifies the implementation of the policy to add the accreditation mechanism and related requirements?</p>	
<p>Building block f) (Authentication / authorization / accreditation) Need further details on what revocation would mean in practice e.g. no further access to SSAD?</p>	
<p>Supply Side – Entity Disclosing the Data</p>	
<p>Supply side – entity disclosing the data</p> <ul style="list-style-type: none"> ● Who will be the entity (or entities) disclosing the data? 	
<p>Supply side – entity disclosing the data</p> <ul style="list-style-type: none"> ● Will there be a single access point or multiple? 	
<p>Supply side – entity disclosing the data</p> <ul style="list-style-type: none"> ● If/how can liability be reduced / shared between contracted parties, entity disclosing the data (if different from contracted parties) and requestor?) 	
<p>Building Block g) (Response requirements / expectations, including timeline/SLAs) Consistent with the EPDP Phase 1 recommendations, the EPDP Team recommends that [TBC]</p>	
<p>Building Block h) (Acceptable Use Policy) “must log requests” - Must all requests be logged? What information must be logged? Who would be able to access the logs? EPDP Team may want to consider the guidance the European Data Protection Board provided on this issue in its 5 July 2018 letter. (“The EDPB considers that, unless there is an explicit prohibition in national law, appropriate logging mechanisms should be in place to log any access to nonpublic personal data processed in the context of WHOIS. In this context, such logging is considered required as part of the security obligation of controllers (article 32), as well as the obligation and in order to be able to demonstrate compliance with the GDPR (accountability) (article 5(2))... It is up to ICANN and other controllers participating in the WHOIS system to ensure that logging information is not disclosed to unauthorized entities, in</p>	

particular with a view of not jeopardizing legitimate law enforcement activities.”)	
Building Block h) (Acceptable Use Policy) “The data subject should be able to challenge –with proper substantiation- the balancing test with rights to object and to erasure” - Does this imply that the data subject is informed every time a balancing test is carried out with respect to his/her data?	
Building Block i) (Query Policy) “of an abusive nature” - Consider including specific examples of what is considered abusive to ensure that no legitimate and/or authenticated requestors are blocked.	
Building Block j) (Authentication / Authorization / Accreditation) “accreditation authority” – Needs a definition / description	
System for Standardized Access / Disclosure (SSAD)	
Building Block m) Terms of use / disclosure agreements / privacy policies The EPDP Team recommends that [TBC]	
Building Block n) Financial sustainability The EPDP Team recommends that [TBC]	