General Comments

#	Comment	Contributor	EPDP Response / Action Taken
General comments received in response to the Google Form or submitted separately.			
Additional comments or observations on Section 3 Part 1 (Part 1: Purposes for Processing Registration Data, incl. rec 1-3) that are not covered by these questions.			
1.	The recommendation shall be kept as it is. No additional requirements to verify the accuracy of data given by the data subject or to validate such data shall be part of any recommendation of the EPDP team. Whilst contracted parties shall ensure that data is accurately recorded in their system as provided by the data subjects, any additional requirements are neither warranted by GDPR nor in scope of the EPDP. *[Staff note – this comment appears to pertain to recommendation #3 although it was entered in the additional comments / observations section]*	• Wolf-Ulrich Knoben; ISPCP Constituency • Lars Steffen; eco – Association of the Internet Industry	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
2.	A balanced situation is needed. An accredited RDS access program will allow examination of the data and challenges by parties who are pre-qualified and responsible actors, and some better requirements around reasonable access would assist non-accredited parties and would also be part of a balanced solution. Please see our notes regarding Preliminary Rec #12 / Question #8 for community input below. This situation also makes it more important for ICANN Compliance—which can request the data for examination--to perform accuracy checks going forward. See SAC104 for additional comments and information.	Ben Butler; SSAC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
3.	Accuracy, insofar as the GDPR requires, primarily relates to the requirement that the data provided to the Data Controller / Processor is recorded accurately and is kept up to date, with the data subject's reasonable instructions. (e.g. where the data subject notifies you of an inaccuracy, the data must be changed without undue delay). Whereas, it is accepted that data controllers must make reasonable efforts to ensure the accuracy of the data they process; however, such reasonable efforts must be linked to practical matters such as: the likelihood of harm or damage to the DATA SUBJECT of an inaccuracy the use of the data by the controller (and whether the decisions made, by the controller, as a result of the data significantly affect the individual concerned, or others) the nature of the data processed the ability of the controller to verify accuracy with due regard to practical matters such as ability, technology and the cost of implementation (again all balanced against the potential impact to the rights of the data subject) It is submitted therefore that the current regime for accuracy, especially considering the most recent ARS report on WHOIS accuracy (Cycle 6) (June 2018) noted postal address operability is 99% and postal address syntax accuracy is 88% (up from 80% three years earlier). ICANN's own key findings include that "nearly all WHOIS records contained information that could be used to establish immediate contact: In 98 percent of records, at least one email or phone number met all operability requirements of the 2009 RAA.. In light of this report, it would appear that the accuracy requirements as contained in the RAA are objectively sufficient and reasonable, for the purpose to which the data is put. We submit, therefore, that no change to the recommendation is currently necessary. *[Staff note – this comment appears to pertain to recommendation #3 although it was entered in the additional comments / observations section]*	Wim Degezelle ; RySG	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
General comments received in response to the Google Form or submitted separately.			
Additional comments or observations on Section 3, Part 2 (Part 2: Required Data Processing Activities – Rec 4-13) that are not covered by these questions.			
4.	[As noted previously] The U.S. supports making a distinction between legal and natural persons as it pertains to the publication of registration data. Specifically, as GDPR does not apply to legal persons, the U.S. believes that information pertaining to legal persons should be publicly displayed. Recognizing that there are challenges in current systems making this distinction from both technical and procedural perspectives, rather than making it an immediate requirement, the U.S. believes that the EPDP should develop a recommendation that the GNSO immediately initiate a process to address this distinction as a future contractual requirement. The U.S. points to the wording proposed by the GAC, which ties the distinction directly to the further development and implementation of RDAP. Specifically: "the GAC proposes that the EPDP consider the following as a new recommendation: Recommendation x: A mechanism be developed within RDAP to differentiate between natural and legal persons. This differentiation is to be implemented within the rollout of RDAP along with a procedure to allow for a phased approach to update legacy registration information." *[Staff note – this comment appears to pertain to legal/natural person related questions although it was entered in the additional comments / observations section]*	Ashley Heineman; NTIA	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
5.	Again YOUR FORM prevented me--"Your response is too large ..."	John Poole; Domain Name Registrant	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
General comments received in response to the Google Form or submitted separately.			
General comments or observations you may have on the findings in Section 3, Part 3 (Data Processing Terms, i.e., roles and responsibilities of parties – Rec 14).			
6.	Starts at Page 67 of 130 of Initial Report - generally no.	John Poole; Domain Name Registrant	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
7.	The remaining thin gTLD registries should be required to move to thick status, per the Thick WHOIS Consensus Policy and Board Resolution 2014.02.07.08.	Greg Aaron; iThreat Cyber Group	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
General comments received in response to the Google Form or submitted separately.			
Additional comments or observations you have on Section 3, Part 4 (Updates to Other Consensus Policies – Rec 15-20) that are not covered by these questions.			
8.	Please see our comments to questions 145 and 147 below. In general, we note that it appears that the needs of users of WHOIS data are not being properly reflected or considered in the recommendations of the EPDP in favor of the desires to limit risk of the contracted parties and ICANN, and of consistently favoring the privacy interests of the registrants without appropriately balancing the needs of others. In addition, we are concerned that the Recommended Purposes do not set forth with sufficient specificity the legitimate interests of third parties, as well as the full range of ICANN purposes that are consistent with its mission, to comply with the GDPR. We hope the needs of WHOIS users will be more carefully considered as the EPDP work moves more firmly towards questions of access.	Brian King; IPC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
9.	The ALAC is concerned that problems may arise as time progresses due to the changes in the process of transfers. The EPDP should recommend that transfer and hijacking complaints be carefully and regularly monitored to ensure that such problems are well understood, with a commitment to rectification if there is an increase in transfer related problems.	Evin Erdoğdu; ALAC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
General comments received in response to the Google Form or submitted separately.			
Additional comments or observations you have on Section 3: Other Recommendations (Rec 21-22) that are not covered by these questions.			
10.	Thick WHOIS Transition Policy for .COM, .NET, .JOBS The ongoing existence of thin Whois databases is demonstrable proof that ICANN's mandate to protect the security, stability, and resilience of the Internet does NOT require the collection of personal data by registries. It may also point to the fact that it does not require the collection of personal data by registrars. ICANN should scrap any thick Whois transition for currently-thin registries and instead look to transition currently-thick registries to thin registries. Thick Whois is unnecessary for any TLD, including these. In this matter, the principle of data minimization is instructive: if the data are not necessary for provision of the service (as they are clearly not), it ought not be collected by the registry. Rules for Uniform Domain Name Dispute Resolution Policy Tucows notes that the URS procedures require communication by the vendor via secure means and note that this should be the standard for UDRP as well. Arbitration vendors are custodians of personal data and, as such, should only be communicating with contracted parties in a secure manner. Public PGP keys as are used by the URS vendors also help confirm the identity of a vendor. The URS rules are fine as is but this section should be extended to UDRP. WHOIS Data Reminder Policy The Whois Data Reminder Policy can be understood to require that personal data be sent via email, which is an insecure and thus problematic medium for such data transmission. This policy should be amended to allow for more secure methods of reminding the RNH of their domain data, and to clearly not require the inclusion of data that is no longer required (as the Admin and Tech contacts may be, pending the outcome of this EPDP) Transfer Policy The TechOps Group has provided helpful instruction and we recommend that the EPDP and ICANN defer to their expert opinion. Uniform Rapid Suspension System (URS) Rules	Tucows Domains Inc.	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	Because URS Rules for accommodate better privacy protections, Tucows notes recommends that certain of them (namely those that relate to public PGP keys) be extended to UDRP.		
11.	The transition of com, net and .jobs to "thick" should be stopped. They should remain as thin registries.	Michele Neylon; Blacknight Internet Solutions Ltd	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
12.	The ALAC would like to note that migration from thin to thick registries should be respected and that the registrars and registry operator of .COM, .NET and .JOBS should comply with the announcement made by ICANN on 25 October 2018 which states that - By 31 May 2019: The registry operator must begin accepting Thick WHOIS data from registrars for existing registrations in .COM, .NET and .JOBS. - By 30 November 2019: All registrars must send Thick WHOIS data to the registry operator for all new registrations in .COM, .NET and .JOBS. - By 31 May 2020: All registrars are required to complete the transition to Thick WHOIS data for all registrations in .COM, .NET and .JOBS. The vast majority of gTLDs are thick, and unless ICANN will take action to change all of these to thin, the results of the Thick WHOIS PDP must be honoured.	Evin Erdoğdu; ALAC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
13.	Proposed Policy Recommendation: In the case of a domain name registration where a privacy/proxy service used (e.g. where data associated with a natural person is masked), Registrar MUST return in response to any query full WHOIS data, including the existing proxy/proxy pseudonymized email.	Brian King; MarkMonitor, Inc., a Clarivate Analytics company	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
General comments received in response to the Google Form or submitted separately.			
Other comments or issues pertaining to the Initial Report? If yes, please enter your comments here. If applicable, please specify the section or page number in the Initial Report to which your comments refer			
14.	YES. [1] Similar to approach followed in section 2 of Temp. Spec, the final report of EPDP should include a section "Definitions and Interpretation" which clarifies the usage of terms "MAY", "MUST", "MUST NOT", "REQUIRED" etc. Perhaps, Glossary section of EPDP initial report may be reused for this purpose. [2] EPDP team final report should recommend Registrars to enter into appropriate data pocessing agreements with Resellers that operate under these respective Registrars.	DR. JAIDEEP KUMAR MISHRA ; DIRECTOR MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
15.	Yes, there are many comments I would like to make on the initial report, and on the progress of the EPDP thus far. I have been an active participant on the group and am quite frustrated with the situation as it stands. While I appreciated the intent of this polling device, as it seeks to make light work of digesting the comments on the report, I don't think a multiple choice questionnaire is a suitable device to seek comment on such a complex matter. I will send a written response to the email address of the EPDP. I hope that you will read it and accept it.	Stephanie Perrin	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
16.	With regard to recommendation # 2 Standardized Access the ALAC would like to note that since this initial report attempts to answer the gating questions necessary to start access discussions it is essential that the EPDP team establishes a date for the discussions about access to commence. The ALAC notes that although the efforts of this EPDP are focused on compliance with the EU GDPR, other privacy (and disclosure legislation and regulations exist in other jurisdictions. Some may be comparable to the GDPR, some more stringent, and some less so. Ultimately contracted parties must all be able to obey regulations that apply to them based on their geo-location and potentially that of their customers. This will inevitably imply that "one-size-fits-all" solutions will not be feasible in the general case, and we will have to move to rules-based (table-driven) algorithms to implement privacy and disclosure issues. The ALAC also notes that there has been significant discussion within the EPDP regarding risks to the contracted parties. There has been very little discussion related to risks to the Internet and to individual Internet users caused by the wholesale redaction of registration data. Privacy of registrant data is of course a significant consideration, but the privacy of Internet users who fall prey to a variety of fraud including phishing resulting in identity theft must also be considered.	Evin Erdoğdu; ALAC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	The ALAC notes that the SSAC has issued a revised version of SAC101, a paper that we have previously said is supported by the ALAC. We wish to in particular call attention to the statement: "RDDS access must comply with the law, but access should not be less timely, more restricted, and less public than law requires."		
17.	This EPDP WG -- like all working groups -- is obligated to work toward consensus. Regrettably, there has been a reluctance to consider the positions other than those of the contracted parties and the NCSG, or to include the other SOs/ACs and constituencies in consensus development. It should be pointed out that "consensus" in this scenario must include the vote of all SOs and ACs that have been participating, not just the constituencies of the GNSO. Lack of access to non-public Whois data is contributing to difficulties that worsen by the day. The BC has trusted that the question of access will be addressed by ICANN. Without doing so, the new policy will fail and ICANN's legitimacy will be challenged. The BC believes the "gating" questions have been sufficiently addressed and the time is right to open the discussion on access to non-public Whois by properly accredited requestors. In conclusion, the BC offers this observation about how ICANN Org, Board, and Community have responded to GDPR. ICANN's mission is to "ensure the stable and secure operation of the Internet's unique identifier systems". This EPDP is by definition an ICANN policy process, aligned exclusively and directly to this mission. And yet it will be clear to anyone following the EPDP that stability and security of the DNS is absent from most of the EPDP discourse. Worse, it is being willfully pushed aside in pursuit of other objectives. Instead, the results of this Interim Report reflect an unbalanced EPDP team where control of data seemingly begets policy authority, where technical limitations instruct policy outcomes, where pursuit of complete online anonymity is championed, and where self-administered risk-profiling of contracted parties is used to justify positioning. The GDPR clearly does not protect Legal Persons, yet there exists no willingness to account for this in the EPDP. The Registrant Organization field is legally valid to collect and display, yet efforts are underway to remove it despite the clear legal justification provided in a written response by ICANN in November. Whois data is clearly needed for ICANN to properly enforce compliance to the RAA, yet those same RAA contracted parties are deciding whether this data is made available to ICANN. That is	Steve DelBianco; BC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	the definition of moral hazard. Some individuals on the EPDP somehow claim to speak for internet citizens, and yet they dismiss the right of Registrants to retain the time-honored ability to publish their information in Whois. Security is enabled, in part, through transparency. In this EPDP, ICANN Org has has impaired its own ability to pursue the mission outlined in its bylaws. We strongly encourage ICANN Org and Board to evaluate the "progress" of this EPDP in the context of its mission and bylaws, and regain its footing lest it leave the security and stability of DNS to empowered individuals and organizations for whom this mission is seemingly last on their list of policy goals and priorities. Goran Marby repeatedly stated that ICANN wants "to retain Whois to the greatest extent possible." We encourage ICANN Org and Board to follow through on that sentiment and hold themselves accountable to those words.		
18.	The voice of registrants seems to be missing in this report. Registrants own very valuable domain names, and many of us *want* to have that data published. Yet, that perspective seems to be missing, as various other factions in this EPDP jockey for position (i.e. contracted parties seem to want to have greater control, and be gatekeepers of certain data; certain privacy advocates seem to want to *compel* private/redacted data, over the objections of the registrant themselves who wants that data public, and so on). I proposed a creative "outside of the box" solution earlier, namely to (optionally) allow registrants to publish their own data by running their own WHOIS servers, instead of making that the obligation of the registrar, which might be a path forward. This would be somewhat similar to the "impressum" requirement in Germany, but for WHOIS data in domains. Technically, it need not be port 43 or WHOIS, and could even be done in new manners (create an open source example that registrants can use, though), e.g. modeled on a robots.txt or other standard. But, ultimately it would need to have a cryptographic hash signature, so that folks could verify that the data held by the registrar (but not published by the registrant.	George Kirikos; Leap of Faith Financial Services Inc.	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
19.	The U.S. is committed to maintaining WHOIS to the greatest extent possible while complying with GDPR and other data protection rules. As such, we continue to actively support and participate in the EPDP as one of the GAC member representatives. The U.S. appreciates the complexity of the issues surrounding GDPR compliance as well as the time pressures associated with the first ever EPDP, however we are concerned with the progress of the EPDP to date and the time left to complete the work. It is time for the EPDP to wrap up its activities so that discussions on the access model can move forward. The U.S. recommends that the EPDP adopt the Temporary Specification with edits reflecting the work of the EPDP to date so that the access model discussion can begin in earnest.	Ashley Heineman; NTIA	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
20.	The RySG appreciates the opportunity to submit comments on the EPDP Initial Report. Given the significant impact that the resulting consensus policy will have on Registry Operators, the RySG representatives to the EPDP Team have participated actively and in good faith, and are committed to continuing this participation. While the RySG remains committed to supporting the work of the EPDP, we must express our concerns with the work methods that have been utilized thus far. We believe that far too much time was spent in the initial phase of work discussing the topic of providing third parties with access to registration data, despite the very clear directive in the EPDP Charter that discussions about access should not take place until the gating questions in the Charter were answered. Such discussions prevented the EPDP Team from engaging in the critical work of discussing and deliberating on foundational matters such as which data elements are required to fulfill various processing activities and purposes, and the roles and responsibilities of the parties involved in data processing. And although the Initial Report references the Charter questions, it does not provide answers to all of them. The amount of time discussing access, and other items outside the scope of the EPDP, led to a significant constriction of the already limited time available for the EPDP to issue an Initial Report. The result of this time crunch is that the EPDP Team did not have time to reach agreement on many of the recommendations that got included in the Initial Report. As the EPDP embarks on the next phase of work to consider public comments and refine the content of the Initial Report into policy recommendations in a Final Report, we urge the EPDP to stay focused on the task at hand and keep discussions within scope. We encourage the Team to engage in the necessary discussions and deliberations around data elements and also to consider the matter of how the final policy recommendations will be implemented.	Wim Degezelle ; RySG	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
21.	The EPDP recommendations may not have to be restrained by conflicts with the text of the GDPR; The policy development exercise by ICANN as a global, multi-stakeholder organization with a responsible role in the Domain Name System, needs to spell out its own purposes without restraint, irrespective of any conflicts with GDPR and communicate its recommendations to Europe as such.	Sivasubramanian Muthusamy; Internet Society India Chennai	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
22.	See SAC104 for a full account of comments, rationale, and recommendations by SSAC on the Initial Report.	Ben Butler; SSAC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
23.	Overarching Comments Summary 1. The EPDP WG has not addressed the subject of access to registrant contact data for legitimate purposes, nor the negative impact of lack of redaction to consumers and internet users. 2. In conflict with its charter, which is to affirm the Temp Spec, the EPDP WG has reduced scope of the Temp Spec, though the Temp Spec over-complies with GDPR as it is currently written and applied. 3. The EPDP WG has not been consensus driven, participation has been dominated and overly-influenced by the contracted parties house and the NCUC. 4. The EPDP WG has not considered real use cases nor the actual impact redaction is having on the operation, security and stability of the Internet. Supporting Detail 1. Access is a consumer safety and security issue which has not yet been addressed by the EPDP WG, the contracted parties, nor by ICANN org: ● See MarkMonitor's study here detailing lack of success in obtaining Whois data and the adverse impact it has had on MarkMonitor clients. Findings: ○ Only 9% of full publicly available Whois records have un-redacted registrant information post-GDPR.	Brian King; IPC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	○ Of more than 350 requests made to more than 70 registrars, Whois data was provided in response only 26% of the time. ○ 74% of Whois requests were either ignored or denied. ○ MarkMonitor has seen a 19% loss of operational efficiency regarding brand enforcement activities. ● See AppDetex letter here outlining lack of registrar fulfillment for reasonable Whois data requests. Findings: ○ Redacted Whois contact data is largely unavailable for legitimate and legal purposes. ○ The majority of registrars do not respond to requests for data. ○ The small percentage of requests that are fulfilled are not completed in a reasonable time period. ○ There is no consistency of process for requesting redacted Whois data. ○ Average response time to a data request: 9.13 days ● See Anti-Phishing Working Group's study here detailing the impedance of cybercrime investigations and the permission of harm to users. Findings: ○ Cyber investigations and mitigations are impeded because investigators are unable to access complete domain name registration data. ○ The mitigation or triage of cyber incidents cannot be accomplished in a timely manner. ○ Whois has become an unreliable or less meaningful source of threat intelligence. ○ Requests to access non-public Whois by legitimate investigators for legitimate purposes are routinely refused. ● See the Cybersecurity Tech Accord Statement here. Findings: ○ Redaction has impacted investigations and mitigations ○ There are real consumer and societal harms ○ Issues are escalating ● See SSAC 101 ○ As noted by SSAC in SAC 101, while legal obligations are a reality and must be complied with, access to registration data under the Temp Spec has been diminished far further than legal obligations require, and further than is prudent for responsible stewardship of the namespace. This point is more true under the EPDP's proposals. The EPDP is obligated to consider the recommendations of SAC 101, and the requirements as listed by the GAC in its recent Communique's related to WHOIS. To date, it has not. The negative impact from the reduced access to WHOIS data on public safety and security following the implementation of the of the Temporary Specification has been detailed by the Public Safety Working Group (PSWG) of the GAC and the presentation they gave in Barcelona. See: https://gac.icann.org/presentations/icann63%20pswg.pdf The PSWG conducted a survey of law enforcement agencies around the world and received responses from approximately 40 different countries, including a dozen EU Member States. The		

#	Comment	Contributor	EPDP Response / Action Taken
	survey results found that since the Temporary Specification has come into effect, only 8% of the respondents find WHOIS meeting their needs, 25% say it partially meets their needs and now 67% say it doesn't meet their needs at all (as opposed to only 2% who said that it didn't meet their needs at all before the Temporary Specification became effective). Similarly, 52% say the current unavailability of WHOIS data has delayed investigations and 26% say it has caused investigations to be discontinued. 2. The EPDP has reduced the scope of Temp Spec which already over complied with GDPR ● Eliminates the Administrative Contact and the possibly redacting the Organization field. ● In SSAC 101, access to registration data under the Temp Spec has been diminished far further than legal obligations require, and further than is prudent for responsible stewardship of the namespace. ● SSAC - ICANN has an obligation to ensure the continued availability of gTLD registration data to the greatest extent possible. ● The EPDP has failed to consider SSAC 101, and GAC advice related to WHOIS 3. The WG has failed to consider SO/AC recommendations other than the NCUC and the CPH ● Consensus must include the vote of all participating SOs and ACs, not just the constituencies of the GNSO. ● The EPDP WG is failing ICANN's multi-stakeholder policy development model by ignoring the needs of key third party interests such as cybersecurity and intellectual property. ● The WG has been unreasonably focusing on cost minimization, rather than to design a policy that is reasonably implementable, and allowable under GDPR. ● This is evident from the inexplicable opposition to conduct research and consider what is already implemented in CCTLDs. 4. The WG is not considering the real impact of redaction and unavailability of whois data for day-to-day tasks. ● Transferring domain names ● Issuing certificates ● Remediation of security and consumer protection threats ● ICANN compliance ● Blocking of harmful content such as phishing and malware on compromised legitimate sites		
24.	On Proposed Purposes for processing of WHOIS data Consideration of Reliance Art 6.1 (c) with regards to disclosure of registration data Regarding the consideration by the EPDP Team of the lawfulness of processing and disclosure of registration data (see section "A-PA3" of Data Element Workbooks related to each purpose), the	Fabien Betremieux; GAC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:**

#	Comment	Contributor	EPDP Response / Action Taken
	GAC would like to call the attention of the EPDP on the fact that such disclosure may take place on the basis of a legal obligation ICANN, a registry or registrar may be subject to (pursuant to Article 6.1 (c) of the GDPR). In particular where ICANN, a registry or registrar established in one country receives an order to disclose gTLD Registration data from law enforcement or a judicial authority in that country, ICANN, the registry or registrar may be obliged to disclose the information. Consideration of Reliance on GDPR Art. 6.1 (f) The EPDP, in the context of drafting processing purposes, also discussed and identified corresponding legal basises for each processing activity. Many of the processing activities have been associated with GDPR Art. 6.1 (f), which is based on processing being necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This basis therefore requires that an assessment and decision be made on whose interest outweighs the other. The GAC is concerned that there has not yet been any substantive discussion within the EPDP on how such an assessment is to be made. The GAC would like the EPDP to carefully consider this matter with particular focus on how to ensure consistency and predictability in such assessments in order for ICANN and the broader community to have faith in the process and assessments being made. Additional comments on other sections of the report In the GAC Barcelona Communiqué (25 October 2018) the GAC stated that it "remains committed to working with the community and the Expedited Policy Development Process (EPDP) to ensure that third parties are able to have timely and predictable access to redacted WHOIS information in a manner that complies with the applicable data protection laws. Although the EPDP Charter tasks the team with defining what is meant by "reasonable access," community work on developing a unified access model should proceed in parallel and can complement the EPDP's efforts". As far as the EPDP Team is concerned, and considering the progress to date, the GAC believes that greater priority should be given to discussion of a "standardized access model" as referenced in its charter, along with the relevant charter questions.		[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
25.	MPA-5 and MPA-6 The ECO GDPR Domain Industry Playbook v.061 states that data for a UDRP proceeding "may be	Brian Beckham; Head, Internet Dispute Resolution Section at WIPO	Concerns Divergence Support New Idea **EPDP Response:**

#	Comment	Contributor	EPDP Response / Action Taken
	disclosed on the basis of Art. 6(1)(b)." We submit that Art. 6(1)(f) is also applicable. Note also that many global ccTLD policies require similar notification/due process as the UDRP. As is also described in the WIPO Center informal Q&A concerning the GDPR as it relates to the UDRP – What is the legitimate purpose for which WIPO collects and processes personal data? "The above-described information relates to registrar provision of non-public WhoIs data. As to WIPO's role as a UDRP Provider subject to the UDRP Rules, the legitimate purpose for which personal data is collected and processed by WIPO flows from the administration of cases under the UDRP – this includes notably: • assuring timely and reliable notice of UDRP complaints to domain name registrants (i.e., forwarding the complaint via email, and the Written Notice to all addresses available for the registrant); • understanding the "mutual jurisdiction" in a particular case; • relaying registrant information which a complainant is required to include in its UDRP complaint; • allowing a UDRP complainant to amend, if it chooses, its complaint upon being apprised of the registrant's contact details; • providing the fullest possible record on which appointed panelists decide a UDRP case; • within appropriate limits, providing case information legitimately retained by WIPO to parties involved in subsequent litigation; • publishing a range of statistical information on domain name disputes. The categories of personal data necessary for the administration of a UDRP cases are: names, postal addresses, email addresses, telephone numbers and fax numbers for complainants and domain name registrants (and any authorized representatives)."		**Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
26.	It is crucial for the EPDP Team to consider the importance of cybersecurity and how use of the DNS for DNS abuse, which perpetuates cybercrime, and cyberattacks, ultimately undermines trust in the system and the overall integrity of the DNS. Accordingly, the EPDP should consider and articulate a true assessment of interests in rights considering the victims of DNS abuse, the security and stability of the DNS, the many GDPR recitals articulating overriding interests, and the GDPR's risk-based approach to appropriate safeguards for personal data.	Greg Mounier on behalf of Europol AGIS; Europol Advisory Group on Internet Security	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
27.	In reviewing the EPDP Initial Report we note that the EPDP is tasked with determining "if the Temporary Specification for gTLD Registration Data should become an ICANN Consensus Policy as is, or with modifications". On the assumption that elements of the Temp Spec not specifically identified for change in the Initial Report might be expected to continue "as is", we would like to raise a concern regarding the definition of "Registration Data", as used in the Temp Spec, which we consider requires review. In the Temp Spec the following definition is used: "Registration Data" means data collected from a natural and legal person in connection with a domain name registration. This definition is insufficiently precise, open to interpretation, and potentially could be taken to cover various other data that might be collected from time to time from a registrant and which is not intended to fall within scope. The term "Registration Data" is also used as part of the defined term "Registration Data Directory Services", but this does not satisfactorily assist in interpreting the definition of Registration Data since it refers to the WHOIS Protocol, which is being superseded. Since an important role of the EPDP is to identify precisely the data elements to be processed in future, in our view a permanent definition of Registration Data should be adopted which clearly enumerates the data elements which are intended to be covered. We would propose: "Registration Data" means the data elements identified in Annex [X] Annex [X] would then enumerate the relevant data elements. These would be the data elements identified in EPDP Team Preliminary Rec #4 (as they might subsequently be amended following this public comment period) but excluding any "Additional optional data elements as identified by Registry Operator in its registration policy".	Ashley Roberts; Valideus	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
28.	I agree with the GNSO's Contracted Parties House (Registrars and gTLD Registry Operators): "The initial report does not present for review any concrete policy. Instead it is a discordant document filled with tentative suggestions and polarised arguments." https://mm.icann.org/pipermail/gnso-epdp-team/2018-November/000994.html	John Poole; Domain Name Registrant	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
29.	Domain.com supports the overall input provided by the Registrar Stakeholder Group and specifically supports the the Registrar Stakeholder Group's rationale regarding Purpose #2 and the collection of the technical contact data.	Domain.com, LLC & affiliates	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:**

#	Comment	Contributor	EPDP Response / Action Taken
			[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
30.	COA submits two additional recommendations not covered by the questions. The first concerns granting registrants the opportunity to consent to have their full WHOIS data published. We note that the issue of consent does not seem to be addressed in the questions. We recommend that the wording of the Temporary Specification be used as modified below: Registrar MUST provide the opportunity for the Registered Name Holder to provide its Consent to publish whatever personal data elements are currently redacted with respect to the Registered Name Holder. Where such Consent is sought by Registrar, the request for Consent SHALL be presented in a manner which is clearly distinguishable from other matters (including other Personal Data Processed based on a legitimate interest). The request for Consent SHALL be in an intelligible and easily accessible form, using clear and plain language. The Registered Name Holder SHALL have the right to withdraw its Consent at any time. The withdrawal of Consent SHALL NOT affect the lawfulness of Processing based on Consent obtained before the withdrawal. Registrar MUST publish the personal data elements for which it has received Consent. COA's second recommendation concerns how Privacy/Proxy data should be displayed. We suggest that the wording from the Temporary Specification be used as revised below: In the case of a domain name registration where a privacy/proxy service used (e.g. where data associated with a natural person is masked), Registrar MUST include in the public WHOIS and return in response to any query full WHOIS data, including the existing privacy/proxy pseudonymized email. Except as set forth above, the privacy/proxy service policy should not be addressed in the EPDP, and instead, ICANN should immediately proceed with finalizing implementation of the PPSAI.	Dean S. Marks; Coalition for Online Accountability	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
31.	Because of the compressed and externally driven time frame to implement these changes, we do not believe there is sufficient time to refer these recommendations (if adopted) to an Implementation Review Team. Therefore, we recommend that registrars be permitted to operate (at their own risk and where applicable) under the new recommendations or the requirements of the Temp Spec for a period of up to one year.	Sara Bockey; GoDaddy	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
32.	As a registrar based in Ireland we are bound by Irish and EU law. It is critical that we are able to both comply with the law and, where possible, our ICANN contracts and policies. However we	Michele Neylon; Blacknight Internet Solutions Ltd	Concerns Divergence Support New Idea **EPDP Response:**

#	Comment	Contributor	EPDP Response / Action Taken
	will always choose compliance with Irish law over any ICANN contract or policy. We would prefer that there was not a gap between the two requirements. If this policy work does not reach consensus or attempts to oblige us to breach Irish law (and GDPR) we will have to comply with the law.		**Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
33.	Privacy rights are fundamental but not absolute. The balancing of rights is not a new concept. 1948 The Human Rights Declaration, these universal values of human society are part of the ICANN bylaws. Art 12 The right to privacy. Art 19 Freedom of expression. While Art 12 and 19 can conflict with each other, it was already recognized that the two rights should be balanced, hence Art 29.2 which includes balancing. Seventy years later it is up to the EPDP team and the ICANN community to balance the interests and the rights of the data subject. --- Report & Temp Spec The current report and recommendations and the temporary specification are from a compliance point of view hard to digest. A considerable part of compliance is to demonstrate accountability. As a registrar who offers a platform for resellers and registrars on a global basis, this is a challenge as a registrar we have to factor in all data protection laws and other laws and regulations and derogations & directives. --- Accountability Accountability is a cornerstone of the GDPR and data protection law in general (OECD guidelines, Convention 108, etc.). --- GDPR The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)" The above-quoted art 5.2 doesn't look like much, yet for people who deal with compliance, it is	Theo Geurts	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	of paramount significance as you must be able to demonstrate compliance with the six privacy principles (Art 5.1) of the GDPR. Art 5 governs any data processing under the regulation. 1 Lawfulness, fairness and transparency 2 Purpose limitation 3 Data minimisation 4 Accuracy 5 Storage limitation 6 Integrity and confidentiality Most of the principles are not covered in the report, so it is not possible at the moment to demonstrate compliance in my opinion. However, the controller & processor are accountable and must be able to demonstrate compliance, a violation of any of the principles can result in action from the supervising authorities. To expand on the above some more. Art 25, privacy by design and by default is a requirement of the GDPR. It is also a great tool to assist organizations to achieve compliance with the six privacy principles, as PbD would require an organization to document the entire process. The GDPR forces organizations to focus on preventive data protection concepts to achieve compliance as they are directly enforceable. Art 35, DPIA The DPIA is absent, yet it is a requirement of the GDPR for controllers dealing with high-risk data elements. https://iapp.org/resources/article/pii-risk-matrix/ A DPIA is an excellent tool (if done right) to get an overview of all your data and processes. It helps on many levels to make determinations. It also assists organizations when it comes to joint controller determinations. Risk analysis is also part of a DPIA, yet there is no documentation of risk in the report, yet there is a lot of risks involved. - https://www.fin24.com/Finweek/Featured/the-rise-of-sim-swap-fraud-20170906 - https://www.theregister.co.uk/2018/12/07/linuxorg_hacked/ - https://medium.com/@valgaze/this-is-what-happens-when-whois-data-is-made-public-60b419bc2e89 Concerning Accountability, The Report Is Not Ready		

#	Comment	Contributor	EPDP Response / Action Taken
	As privacy principles have not been applied on many levels, the current recommendations resemble a house of cards which could lead to the situation that in the event a consensus-based proposal would be deemed invalid by a supervisor authority it affects several if not all consensus-based recommendations, putting the community back to square one. --- Data Collection While the report contains the word phone 97 times, not once is mentioned why this high-risk data element is being collected and processed on so many different levels. Taking such a data element out of the required collection would make a huge difference in case of a breach or other GDPR requirements. A supervisory authority would be likely to weigh in the factor of the absence of high-risk data elements positively if it had to issue a fine or order a stop of the processing of all personal data. The latter would be even worse than a monetary fine. Conclusion Without a good level of accountability, the current recommendations are not GDPR compliant. The EPDP team should focus that the proposals are GDPR complaint before trying to get consensus on them. --- Miscellaneous observations and problem scope After 200+ days of redacted WHOIS, it is time to collect and analyze and prioritize the problems. It seems the current discussion is very focused to preserve as much of the WHOIS without a problem scope. As such the EPDP team spends a lot of time on seeking exemptions of the GDPR, apply legal shortcuts and impose more barriers s on contracted parties and registrants. It is clear that certain types of abuse, if not most abuse continues with or without redaction. So it begs the question if a centralized WHOIS or UAM is a solution. WIPO statistics are comparable in line with 2017. https://www.wipo.int/amc/en/domains/statistics/ It does not seem that trademark holders have an issue post GDPR. Spam numbers have not gone up; in fact, they went down; https://www.talosintelligence.com/reputation_center/email_rep		

#	Comment	Contributor	EPDP Response / Action Taken
	Malware, phishing did not go down at all, CEO fraud was a big issue this year. These types of DNS abuse are a high priority in my opinion. Pseudonymization techniques within a non-public environment powered by RDAP on a decentralized basis with strong user credential management should be fast-tracked by the ICANN community to explore. Adding "noise" to the current data sets might also be an option worth exploring; https://www.winton.com/research/using-differential-privacy-to-protect-personal-data When the interests or fundamental rights and freedoms of the data subject are balanced towards the benefit of the controller, successful pseudonymization might be a deciding factor for processing based on prevailing legitimate interests of such a controller. --- The Publication Of The Organization Field Data The first question is always, what is the purpose? Publication of the contents of the organization field without further information is, in my opinion, meaningless and useless and as such, there is no longer a valid purpose. If there is no valid purpose, it will be most likely not data protection law compliant. The definition of an organization is very comprehensive and by its definition most likely will contain personal data. During the Translation and Transliteration WG sessions, it could be often observed that translations can turn into different meanings which can lead to unexpected results. Unless we exactly know what meaning the word organization has all over the world the EPDP team should operate risk-based concerning data protection laws on a global level. As such this also involves that the EPDP team should be fully aware of all data protection laws and possible derogations which is impossible from an operational point of view as these things happen to change. The EPDP team could consider the following alternative. For commercial or business related activities an OV or EV SSL certification requirement could be an option? After all, these Certificate Authorities have extensive experience with validating and verifying companies and organizations. For any avoidance of doubt, I am not suggesting regular DCV validated SLL certificates as an option; a 5-year-old can validate such certificates. https://ssl.comodo.com/articles/the-ssl-certificate-domain-validated-organizational-validated-or-extended-validated.php The above suggestion moves away from the ancient WHOIS to the browser level, which every		

#	Comment	Contributor	EPDP Response / Action Taken
	internet user uses. --- Personal Data Or Not Personal Data? Recital 14 is clear; the regulation applies to natural persons. A legal person is any human or non-human entity; the regulation does not cover them. There is an exception to the rule, one-man-owned entities are viewed as a natural person as it is not possible to separate personal and corporate data in this situation. Why EU lawyers and GDPR practitioners have this view is due to following; https://www.i-scoop.eu/personal-data-natural-persons-of-legal-persons-entities/ The above article also has a link to an article on Linkedin, this is relevant for the context and provides further information. Also pertinent to get the full picture here is the EDPB opinion on personal data; https://iapp.org/media/pdf/resource_center/wp136_concept-of-personal-data_06-2007.pdf Meaning of personal data; -any info -relating to -an identified or identifiable -natural person Additional relevant is the below URL. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en The above is for sure somewhat academic but relevant due to the recommendation made by the Berlin Group consisting over 100 DPA's worldwide. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2017/2017-IWGDPT_Working_Paper_WHOIS_ICANN-en.pdf 7 Commercial data which may be disclosed must not include personal data. Recommendation 7 is crystal clear and is an indication that controllers might be liable after all. The above is also in line with the advice from the lawyers contracted by ICANN ORG themselves. https://gnso.icann.org/sites/default/files/file/field-file-attach/wsgr-icann-memorandum-25sep17-en.pdf The above is a strong argument that most likely we will see in the future that one man owned entities or entities or similar will be able to join a certain degree of protection. That will cause		

#	Comment	Contributor	EPDP Response / Action Taken
	issues for contracted parties, and ICANN as the controller for this purpose as the organization field is littered with one man owned entities which by definition of the organization field is correct. --- Consent To Publish Personal Data What is the problem scope? What are we trying to solve that is not an issue at many ccTLDs for years? How do controllers get meaningful consent? A simple checkbox won't cut it, and 30 checkboxes pointing out all the dangers and other requirements is going to be costly to implement. How would the technical implementation look like to comply with Art 17.2? Must we assume that the word "reasonable" in Art 17.2 carries more obligations for controllers within the DNS? Think about this; publication equals the access of data to an indefinite number of persons, companies, whatever. It's not that a data subject can consent at this moment to have a limited set of his or her data being published in the WHOIS. Linkedin, for example, does have such specific privacy setting which you can turn on or off and as such limit the access to third parties and what is visible for other Linkedin users. So we first might want to define a policy to which data elements a data subject can consent to for publication. Provided we can find a way to deal with Art 17.2 first. Privacy by default, Art 25, would be highly relevant to develop such a policy. Contracted parties spent a lot of time and money on security, train staff, encrypt data and a lot more to protect their systems and the data of customers. It is hard to demonstrate compliance under 5.1.F (security) when you do all of the above, yet offer an option in your system or a command in the API that could result in an accidental data breach. --- Geographical Distinction There should be a problem scope here. What are we trying to solve and how many people would affect this? Key considerations; An economic advantage for EU registrars. The applicability of all data protection laws, not just the GDPR. - Asia https://iapp.org/news/a/as-asia-pacific-rises-and-integrates-so-too-could-the-apec-cross-		

#	Comment	Contributor	EPDP Response / Action Taken
	border-privacy-rules/ - African countries are working very hard and make good progress to sign Convention 108, which runs in parallel with the GDPR. Convention 108 is often confused as a law from the EU, it is, however, international law and not EU law. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures -Data protection around the world https://www.dlapiperdataprotection.com/ - Track privacy around the globe https://iapp.org/news/privacy-tracker/ Note to the EPDP team, ICANN's global nature, one world one internet does include the EU, and Art 3 of the GDPR would apply. It is very likely that ICANN is not in a position to create policies that would make distinctions or exclusions depending on geographical locations without violating its bylaws and mission. --- Resellers The 1.4 million resellers need to be discussed and their role within the DNS. Or can be part of the JCA discussions. --- Joint Controllers ICANN ORG and the contracted parties should lead the way and be a thought leader in respect of joint controller agreements. The ccTLD community divided in the allocation of the respective roles and responsibilities. --- Cities The argument that the content of the city field can be displayed in the public WHOIS as it does not contain personal data is incorrect. https://www.onlyinyourstate.com/usa/smallest-towns-usa/ It's straightforward to single out persons in small towns. --- Accuracy The accuracy principle hinges on a few, yet critical considerations: reasonable and concerning the purpose.		

#	Comment	Contributor	EPDP Response / Action Taken
	Incorrect data can negatively affect a data subject; inaccurate medical records could cause wrong treatment of a patient. It is essential that data subjects can rectify and correct their data to correct such mistakes. The accuracy principle is out of scope for the EPDP team. The accuracy principle is subject to compliance of the GDPR and as such, it is up to the controller to determine the compliance requirements. At this moment it is not clear who will be the data controller for this principle. Organizations who are subject to compliance requirements of the accuracy principle should be able to demonstrate compliance towards the applicable supervising authorities and not to ICANN ORG or its community. After all, it will be the DPA's who will determine non-compliance for the accuracy principle and issue fines if required and the EU and not ICANN govern the regulation. Note to the EPDP team; the WDPR policy is one of the acceptable methods to demonstrate compliance regarding the accuracy principle, provided it is sent to the registrant and not the admin contact. Think about this. Given the high-risk nature of certain data elements sending WDRP notices through unencrypted email might not be compliant with data protection law. Data minimization can easily tackle this issue and avoid high operational costs. Think about this; completing, incomplete data, leads to an increased amount of data being processed and should only take place if it is necessary for the purpose of processing. As such it should be crystal clear what the goal is and its necessity and the risk for the data subject. There is also the consideration if completion of data is proportionate for the specific processing. GDPR Art 16 and recital 65 might be relevant here. Cross-border Data Transfers To Third Countries. The report is silent about this. Actors within the DNS face a significant legal struggle with registrations of gTLDs in Russia, Brazil, China, and other third countries where registries operate. Demonstrating compliance towards chapter 5 of the GDPR is tough. --- Data Retention Personal data shall be kept for no longer than is necessary for the purposes for which it is being processed. For compliance purposes the following is relevant.		

#	Comment	Contributor	EPDP Response / Action Taken
	Art 5.1.E and 5.1.B which connects to Art 6. The overarching compliance principle is Art 30 (record keeping). The above results in a set of policies and frameworks. -Data retention policy -Data destruction policy. In your procedure you layout the purposes why you store data for one year or whatever years. Reducing your retention period from 2 years to 1 year does not explain your intentions. What is also absent, do we need all the data elements to achieve whatever purposes? Privacy by design is an essential tool on current forms of processing to assist organizations. https://iapp.org/resources/article/check-or-mate-strategic-privacy-by-design/ --- RDAP While RDAP is a great protocol, it is overkill to implement this when most of the data is redacted; the current protocol is more than sufficient to display redacted data. RDAP could play a role in a UAM setup, or be a great addition to replace thick WHOIS and enhance security. Till the EPDP team finds a real use for it, implementation is burning money and wasting precious development capacity. --- Article 3 The current setup of the registry contracts, registrations available to everyone in the world, triggers Art 27 & 30 for registry operators outside of the EU and add additional operational costs and legal complexity. The GDPR is not the only data protection law that requires controllers or processors of personal data to assign a representative. If registries are required to process personal data as they are now, it is not unthinkable that within 4-6 years, registries will have to assign representatives in over 100+ countries in those countries themselves. --- Art 3 And Newest EDPB Guidelines Currently, the new guidelines are positioned as a draft for consultation, which leaves the door open for the EDPB to further clarify and refine the language. I would not recommend the EPDP team to use the guidance at this moment for obvious reasons. Also, these guidelines can only be evident if all the relevant roles have been identified and labeled. If ICANN ORG keeps switching roles and does not take a position, it is impossible to determine the roles correctly of the other relevant parties.		

#	Comment	Contributor	EPDP Response / Action Taken
	Clarity on ICANN's role, in general, would also help the EPDP team. --- Because It Is In The Contract Requirement(s) prior to the contract; -Necessity test -Reasonableness test -Relevance test If the purpose(s) fail the above criteria (taking in mind all the relevant GDPR requirements), then you can generally assume that 6.1.B is not a legitimate basis for processing. --- 6.1.B Processing is deemed necessary if the contract could not be fulfilled without processing taking place. This argument is hard to make given the fact that 75% of the domain name registrations for the last two decades has been done at a registry level without processing personal data. .COM & .NET It is not that registries have to ship the domain name by FedEx to the registrant or anything. --- Domain Name A domain name is personal data. Pre GDPR you could look up a domain name and get all the personal data of the registrant, Post-GDPR with the WHOIS redacted can be compared with an IP address of an internet user and an ISP. While you need the ISP to disclose the personal data of the internet users IP address the same applies for a domain name. With the domain name, you can go to the registrar who has the personal data of the domain name owner. A domain name does not have to have a website, many other services that are not public can be used in combination for a domain name. So many parts of the GDPR are directly applicable to domain names as personal data. Think about this. Why do we use domain names? So we do not have to remember IP addresses. --- Public access to the zone files Domain names need to be published in the zone file to make it work. Providing public access to the changes in the zone file is a different matter. On the one side of the spectrum, we see criminals, scammers and a lot more abuse domain names for whatever. On the other side of the spectrum, we have the anti-abuse community		

#	Comment	Contributor	EPDP Response / Action Taken
	trying to mitigate the damage caused by criminals. It would be logical to deprive access to public information of the zone files and as such prevent abuse and ensure we have a legitimate basis and access for those who fight cybercrime and DNS abuse. Even with the WHOIS redacted we can still see criminals and scammers use big data and historical records to predict who the registrant is and treat them with fake invoices. Another crude tool is to send all newly registered domain names fake invoices or scams using email addresses like info@newdomain.com, postmaster@newdomain.com, admin@newdomain.com, etc. So put a stop regarding the harvesting of the public info of the zone files. Many ccTLDs operators already quit making that info public for obvious reasons. --- Webform A web form is a very privacy friendly option to contact the registrant. An email address that has been hashed or pseudonymized is still subject to the GDPR and can again lead to the identification of a person. The temporary specification has this wrong in my opinion and many other sections. --- Change of Registrant/COR policy While the COR policy is not in scope for the EPDP team, but the EPDP team should highlight the fact that the IRTP-C/Change of Registrant policy might violate Art 16, Right to rectification. Most likely, the ineffective purpose to avoid domain theft, and this policy does not prevent domain theft, is no relation to the barriers it can create for data subjects to correct their data (without undue delay the rectification of inaccurate personal data concerning him or her). --- Tech Contact/Admin Contact Many ccTLD registries do not require the Tech and Admin contact. For years these contacts were replaced with proxy/privacy services by registrants in the gTLD space. Observing the top 10 ICANN registrars, most of them re-use the registrant data for the other contacts, i.e., they are same. The above is pre-GDPR and not a result of post GDPR. If the above facts had caused real issues, we would have a PDP about this years ago pre GDPR. The EPDP team should not lose sight of data minimization due to some anecdotal stories which are in no relation to the current over-collection of data. The redaction since May 25th of all contacts is another indication that the Tech and Admin		

#	Comment	Contributor	EPDP Response / Action Taken
	contact had no real function within the DNS. --- The GDPR The GDPR is a principle-based law formulated abstractly. While such an approach lacks in clarity it's level of abstraction allows the GDPR to become unconstrained from technological changes ensuring the regulation is technology neutral. As such the regulation is very sustainable and always ensures the right level of security is required under all circumstances. While the GDPR is a regulation enforceable in the entire EU it does not mean that the different EU member states cannot set additional data protection requirements, quite the contrary, it is expected that over the years member states will introduce new data protection requirements. The EPDP team should keep the above in mind during its discussions and give contracted parties the flexibility they require. Only then we can create a policy that is enforceable and meets the standards of data protection law worldwide. Creating a policy that mirrors requirements like the temporary specification is not the way to go. For any avoidance of doubt, the temporary specification is in most areas NOT GDPR or data protection law compliant due to its narrow and specific requirements and one size fits all approach. Thanks Theo Geurts CIPP/E		