Question #3 - Geographic Location

#	Comment	Contributor	EPDP Response / Action Taken
	a) What other factors should the EPDP team consider about whether Contracted Parties should be permitted or required to differentiate between registrants on a geographic basis? (For more information, please refer to the Initial Report, beginning on p. 47. b) Please provide the rationale for your above answer. **c)** Are there any other risks associated with differentiation of registrants on a geographic basis? If so, please identify those factors and/or risks and how they would affect possible recommendations, keeping in mind compliance with the GDPR.		
1.	Contracted Parties should NOT be required to differentiate between registrants on a geographic basis, and may not be able to do so consistent with their own respective legal counsel's advice. Requiring a Contracted Party to act contrary to legal counsel's advice is inappropriate. Rationale: See ICANN v. EPAG Domainservices, GmbH https://www.icann.org/resources/pages/litigation-icann-v-epag-2018-05-25-en Other Risks: The potential liability for violating GDPR via mistakes made in "differentiating registrants on a geographic basis."	John Poole; Domain Name Registrant	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
2.	The desires of the registrants themselves are often not being considered (see below). These need to be at the forefront of the analysis. Rationale: I agree with the BC that the GDPR should not be overapplied, and that registrants should not be thwarted from having their own data published in the WHOIS. I'm in Canada, and my company's WHOIS data is currently being redacted, against my desires, which is a major detriment. Open and public WHOIS has major benefits which are not being recognized by some quarters of the EPDP team, even when the registrant WANTS their own data to be fully public (to be able to fully document ownership of their own assets). Security through obscurity is a fallacy. Registrants who know this, and want security through public exposure of their contact info, should be allowed to have it published. Other Risks: No response	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
3.	The current Temp Spec allows RDDS operators complete freedom to choose when to redact domain contact data from publication, whether or not a domain contact is protected by GDPR or by any other local privacy law. The result has been blanket redactions, hiding more data than is legally called for. A more balanced and justified approach is needed. Redact data for data subjects covered under GDPR, but don't redact for those not covered by the law. Rationale: None provided Other Risks: No response	Greg Aaron; iThreat Cyber Group	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
4.	We don't support differentiating registrants on a geographic basis. Rationale: This requirement (differentiating registrants on a geographic basis) while costly from an implementation perspective by the contracted parties also implicitly assumes 100% WHOIS accuracy which is far from reality. However that having been said, there is no denying that "a one size fits all" kind of an approach prompted by and designed to comply with the GDPR might end up running foul with some of the national Privacy & Data Protection legislations of other jurisdictions. Other Risks: See #85	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.]
5.	The AG IS recommends the EPDP Team ensure that legal and natural persons are treated in a distinct manner to the extent that changes to personal data publishing and access are made. GDPR's definitions along with Recital 14 makes clear that it does not apply to the processing of "personal data which concerns legal persons." Rationale: None provided Other Risks: No response	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
6.	Registrants of commercial operations should be considered legal persons. Rationale: Good governance/due diligence Other Risks: It is not always possible to identify the geographic location of the registrant, for example if anonymization or proxy services are implemented.	Monique A. Goeschl; Verein für Anti-Piraterie der Film- und Videobranche (VAP)	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
7.	Tucows strongly supports the position taken by the Contracted Parties and NCSG on these questions. They have done a thorough and admirable job of identifying the risks and drawbacks of differentiating on geographic or person-type basis. Rationale: Privacy is a right that ought not inure solely to European citizens. In addition, the Internet being the global system that it is, there is no simple way to appropriately determine who is and who is not protected by the GDPR or other relevant data processing laws. For entities operating in or transferring data through the EU, these rights must be extended to all personal data that is transmitted. Other Risks: The Internet global system, and as such, there is no way of appropriately determining who is and is not a European citizen or otherwise protected by the GDPR. IP addresses can be spoofed, geolocation is only accurate to a point, and people move freely about the globe. It is not possible for a registrar to know the person type or location of a registered name holder with sufficient certainty to protect those whose data must be protected. In addition, the risk of releasing data is high: both to the natural person whose personal data was compromised and made public and to the company that released it. The monetary penalties to the company, however, pale in comparison to the compromised privacy of the natural person. Finally, there are many and varied similar laws, including in Argentina and the United States. Developing systems that respect personal privacy rather than adhere to a Eurocentric worldview is simply good sense.	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
8.	We support the reasons spelled out in the initial report in favour of a uniform approach globally. Rationale: None provided Other Risks: No response	• 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.]
9.	Contract Parties should be permitted to differentiate, if they choose, but it should not be required. Rationale: GoDaddy's position on this topic has been previously noted here, https://mm.icann.org/pipermail/gnso-epdp-team/2018-November/000749.html Other Risks: The distinction between registrants based on geographic regions does not currently exist in the Domain Name System. Therefore, any recommendation mandating this change is outside the scope of the ePDP, and possibly the "picket fence" of Registrar and Registry contracts.	Sara Bockey; GoDaddy	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
10.	The RrSG would like to spell out our numerous high-level concerns against making any Consensus Policy recommendations for contractual requirements regarding a mandatory distinction between legal and natural persons as well as requiring a differentiation of registered name holders on a geographic basis. Our concerns involve: • Legal - Aside from GDPR, other data protection laws around the world are less clear on the distinction between legal and natural persons. Future regulations may contain contrary requirements. Furthermore, data of legal entities may contain or consist of personal information of natural persons, which would be entitled to protection under the GDPR and similar data protection regimes. Likewise, the geographic distinctions also create uncertainties. The goal of whatever consensus policy comes out of this working group should be one that is not focused solely on one privacy law but rather creates policy that will be as future-proof as possible. • Technical - Contracted Parties are uniquely situated to assess the current level of the technological means available to us, and it is our position that a technical basis to reliably and confidently make such a distinction does not exist. Additionally, any distinction schema would be dependent upon Registrant Self-Identification, which is fraught with error and would create artificial barriers to entry for those persons or organizations around the globe looking to register and use a domain name. • Commercial - Developing and deploying this technology on a global scale will involve significant costs, which may be prohibitive for smaller organizations and a barrier to market entry. Regardless of whether the distinction(s) are applied to new registrations or legacy domain names, it would be a logistical nightmare for Contracted Parties, and a source of confusion for Registrants, many of whom could lose access to their registrations. • Asymmetrical Risks vs. Benefits - Contracted Parties would assume all regulatory risks of such an obligation, exclusively for the benefit of unburdened third parties. Simply put, registrars cannot accept a policy which creates such a high degree of risk for something that does not need to be differentiated. • Scope - The distinction between Legal and Natural persons, or geographic regions, does not currently exist in the Domain Name System. Therefore, any recommendation mandating this change is outside the scope of the ePDP, and possibly the “picket fence” of Registrar and Registry contracts. While some may point to certain ccTLD registries which do call for similar distinctions, attempting to equate that to the gTLD space (and its expansive, global nature) is simply not appropriate. Rationale: See above Other Risks: See above	• Zoe Bonython; RrSG • Volker Greimann; Key-Systems GmbH	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
11.	As INTA has noted previously, it shares ICANN's objective to "identify the appropriate balance for a path forward to ensure compliance with the GDPR while maintaining the existing WHOIS system to the greatest extent possible." In other words: whatever Consensus Policy emerges from the EPDP should be "calibrated" as much as possible – so as not to over-comply with the GDPR. INTA thus agrees with the reasoning of the BC and IPC, as articulated in the Initial Report, that Contracted Parties should be required (not merely permitted) to make differentiations (for example, in what gTLD registration data should be redacted vs. published in the public WHOIS) that are consistent with the territorial scope of the GDPR. At the least, INTA suggests that the EPDP consider other factors on this "permitted vs. required" distinction, such as: (a) the risk of fragmentation from a non-mandatory, permissive regime; and (b) whether existing examples where registries and registrars are already making similar kinds of differentiations may shed any light on the feasibility of how to do so at scale. That said, for the reasons outlined below, INTA does not necessarily agree with the premise of this question that the differentiation that Contracted Parties should be required (not merely permitted) to make will always necessarily be "on a geographic basis". As the Initial Report notes, the actual location of the registrant is not always dispositive as to whether GDPR applies. Fortunately, the EDPB has recently issued Guidelines on this exact question – the territorial scope of the GDPR – that are illustrative in this regard.[5] For that reason, INTA also respectfully suggests that the EPDP consider (c) the recent guidance on the territorial scope of the GDPR from the EDPB. Rationale: a) Fragmentation. As noted in Section (e) of the EPDP Initiation Request, fragmentation of the WHOIS system is a policy outcome to be avoided – at least in part because it could jeopardize the security and stability of the Internet. INTA agrees with this. And so too, apparently, do those members of the EPDP (specifically, the Contracted Parties and the NCSG) who oppose requiring differentiation between registrants consistent with the territorial scope of the GDPR. As they have argued in the Initial Report: "Not having a common approach for all registrants could lead to two classes of registrants, which may result in competitive advantages to certain registrars/registries (due to their establishment in jurisdictions with privacy protection), fragmentation in the marketplace and interoperability issues." See: Initial Report at 48. In that sense, INTA and the Contracted Parties/NCSG appear to agree on the overarching policy objective – that "RDS policies should be as unified as possible", and that fragmentation is problematic. They just disagree on how to get there – specifically, on whether a "permissive" or "mandatory" policy is most likely to do so. On that specific disagreement, INTA does not understand how permitting but not requiring differentiation is somehow going to result in less (not more) fragmentation. The whole point of a "permissive" regime (as opposed to a mandatory one) is to allow each Contracted Party to make decisions as to differentiations on their own. The Contracted Parties/NCSG admit as much when they state: There are significant liability implications for Contracted Parties if they are incorrect in applying the appropriate data protection rules. Contracted parties should be free to choose whether or not to take that risk as a business decision rather than a contractual requirement. Whatever the merits of that argument on its own terms, it is clearly contrary to the reasoning of the EPDP Initiation Request, which cautioned against an outcome in which "each registry operator and registrar might make their own determination regarding what gTLD registration data should be collected, transferred and published, leading to a fragmentation of the globally distributed WHOIS system and the handling of gTLD registration data." (emphasis added). Obviously, different Contracted Parties are going to have different risk tolerances – and thus are going to answer this question, and others, differently. The whole point of a consensus policy is to avoid that kind of fragmented decision-making. INTA does not understand – and the Initial Report does not make clear – why this differentiation question is somehow special, such that it would warrant an exception to the general preference that RDS policies be as unified as possible. b) Existing examples. Unlike Question 90 below, which asks for "existing examples where a legal/natural differentiation is already made", for some reason the questions from the EPDP do not ask for existing examples where differentiations based on geography are already made. In that sense, the questions from the EPDP appear to take at face value (or at least, do not solicit any input from public comments that may be contrary to) the claims from the Contracted Parties/NCSG that: 1) "It is often difficult to identify a registrant's applicable jurisdiction with sufficient certainty to apply appropriate data protection rules"; and 2) that "Any consensus policy needs to be commercially reasonable and implementable, and in the current market place, differentiation based on geographic location will be difficult to scale, costly, and, accordingly, neither commercially reasonable nor implementable."[4] It is unfortunate that the EPDP did not ask for any input testing or challenging those assumptions – because the claim that geographic differentiation is somehow commercially unreasonable is inconsistent with numerous examples from the current marketplace that specifically differentiate between registrants on a geographic basis. Most obviously, various ccTLDs restrict registration to registrants with a nexus to a particular geographic region. (See, e.g., https://eurid.eu/d/205796/Registration_Policy_EN.PDF (outlining eligibility criteria for the .eu ccTLD); https://www.about.us/policies/ustld-nexus-requirements (outlining the United States nexus requirement for the .us ccTLD); https://cira.ca/sites/default/files/public/policy/cprregistrants-en.pdf (outlining the Canadian presence requirements for the .ca ccTLD). Likewise, various "geographic" gTLDs also restrict registration to registrants with a nexus to a particular geographic region. (See, e.g., https://www.ownit.nyc/policies/nyc-nexus-policy ("Registrants in .nyc must be either: a natural person whose primary place of domicile is a valid physical address in the City of New York . . . ; or an entity or organization that has a physical street address in the City of New York . . . .").) In addition, it appears that at least some registrars (such as GoDaddy) are already making geographic differentiations for purposes of providing various privacy-related account-management services to their customers. (https://www.godaddy.com/help/edit-my-privacy-options-for-european-economic-area-residents-27893 (noting that the process and information provided applies only to EEA residents); https://www.godaddy.com/help/download-my-data-for-european-economic-area-residents-27892) These examples belie the claim that differentiation based on geography is neither commercially reasonable nor implementable. At the least, they suggest that the EPDP should consider as an additional factor how the registries and registrars that are already making such differentiations have been able to do so. c) EDPB Guidelines. For the foregoing reasons, INTA sees no credible argument that differentiation should be permitted but not required (at least if uniformity is to be preferred over fragmentation). But INTA does agree with the point raised in the Initial Report that the actual location of the registrant may not always be dispositive as to whether the GDPR will apply. Fortunately, the EDPB has recently issued helpful Guidelines on that exact question – the territorial scope of the GDPR. INTA will not attempt in this Comment to exhaustively summarize those Guidelines. But in general terms, they do support a potential Consensus Policy that would require Contracted Parties to, for example, only redact gTLD registration data when: 1) the Contracted Party is collecting such data within the context of the activities of "an establishment in the EU" (as that term is defined in the EDPB Guidelines); or 2) when the Contracted Party is "targeting" domain-name registration services to individuals in the EU (as that term is also defined in the EDPB Guidelines). At a minimum, INTA suggests that the EPDP consider the recent EDPB Guidelines as an additional factor on this issue. Other Risks: The question assumes the conclusion – that there are some risks associated with differentiation. And it does not ask the converse question: whether there are any risks associated with not requiring (but merely permitting) differentiation – such as the substantial risk of fragmentation that will result if each Contracted Party is permitted to make its own determination on the basis of its own unique risk tolerance.	Lori Schulman Senior Director, Internet Policy; International Trademark Association (INTA	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
12.	A factor not properly aired in the Initial Report is the Internet's status as a global infrastructure and ICANN's status as a uniform policy maker for the global Domain Name System. One of the main reasons for creating ICANN was to ensure that the Domain Name System would have a globally consistent set of rules. The NCSG strongly opposes fragmenting the policies regarding domain name registration data on a geographic basis for that reason. ICANN should strive as much as possible to keep its rules and requirements the same for the entire Domain Name System. This helps maintain the global compatibility of the Internet. Recently published EDPB guidelines on territorial scope also indicate that there are more factors that require consideration on the territorial scope of GDPR, including targeting criteria (if the sale of goods and services is targeting EU/EEA residents) as well as whether the data controllers and/or processors have stable establishments located within the EU, irrespective of whether the associated data processing activities take place within the EU, or not. Rationale: None provided Other Risks: No response	Ayden Férdeline; NCSG	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
13.	The new policy should differentiate between registrants for which GDPR applies and registrants outside the jurisdictional reach of GDPR. There should be no redaction of data collected outside the E.U. in the provision of non-E.U. services. The Guidelines issued by the EDPB on November 16, 2018 should be used in determining how best to implement a differentiation between registrants on a geographic basis for the purposes of compliance with the GDPR. Proposals should be reevaluated and further justified in light of the Guidelines, which suggest that it would be possible to agree that redactions to the data of registrants for these purposes should only be applied where: (a) the contracted party is collecting such data within the context of an establishment of the contracted party in an EU member state, or (b) the contracted party is targeting domain registration services to EU data subjects. The EPDP Team should seek to develop practical measures based on these Guidelines. Rationale: It is not necessary to universally apply the geographically limited GDPR, particularly when practical measures exist to implement the law consistent with its jurisdictional limits. ICANN should be primarily concerned with the objectives set forth in its mission, which has from the inception of the WHOIS framework included the practice of collecting and displaying the information of domain registrants for the purposes of ensuring the security and stability and resiliency of the DNS. To the extent exceptions are required to accommodate national laws, ICANN has policy in place to deal with the conflict - the WHOIS Conflicts Policy. The purpose of the EPDP process is to determine how to accommodate current practices to be compliant with the GDPR. The purpose is not to globalize the application of the GDPR, which would also raise the risk that some countries may seek to enact counterbalancing rules or laws to oblige disclosure of registrant data for what it considers to be legitimate purposes, leading to a more fractured and complex compliance landscape. Other Risks: No response	Sajda Ouachtouki; The Walt Disney Company	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
14.	A factor not properly aired in the initial report is the Internet's status as a global infrastructure and ICANN's status as a uniform policy maker for the global DNS. One of the main reasons for creating ICANN was to ensure that the DNS would have a globally consistent set of rules. We strongly oppose fragmenting the policies regarding domain name registration data on a geographic basis for that reason. ICANN should strive as much as possible to keep its rules and requirements the same for the entire DNS. This helps maintain the global compatibility of the Internet. Rationale: None provided Other Risks: No response	Farzaneh Badii; Internet Governance Project	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
15.	The new policy should differentiate between registrants for which GDPR applies and registrants outside the jurisdictional reach of GDPR. In addition, the EPDP should consider a policy recommendation to explore whether it is possible for ICANN to create a "rules engine" or dynamic chart that determines how the various privacy laws that exist or will exist in the future apply to WHOIS. Recognizing the complexity of this analysis, this policy recommendation could be implemented on a timeline different from other policies emerging from the EPDP. For example, based on the EDPB's recent guidance, the dynamic chart could determine that the new WHOIS redactions implemented for GDPR apply to specific situations, such as where the contracted party is targeting domain registration services to the EU. Recently, the EPDP provided guidance on this issue in its Guidelines 3/2018 on the Territorial Scope of the GDPR. These Guidelines address the factors mentioned above and confirm that it should be feasible to distinguish between registrants on a geographic basis for the purposes of determining whether the GDPR should be applied. Redactions to the data of registrants for the purposes of compliance with the GDPR should be applied only where: (a) the contracted party is collecting such data within the context of an establishment of the contracted party in an EU member state, or (b) the contracted party is targeting domain registration services to EU data subjects. Rationale: The BC is concerned that the EPDP's proposed policies significantly reduce the utility of WHOIS through the over-redaction of data due to interpretations that, in the end, are not applicable to GDPR. Making a geographic distinction is consistent with ICANN's stated goal of preserving the WHOIS system to the greatest extent possible while complying with GDPR. ICANN (and its policies) should not serve as a means to achieve global application of a law that has limited territorial application. To do so adversely affects the ability of those that use WHOIS as a practical tool for easily resolving issues that protect consumers, mitigating security threats, and protecting its intellectual property without having resort to legal action. Other Risks: ICANN risks the adoption of onerous regulations to counter the unnecessarily broad application of GDPR.	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
16.	A factor not properly aired in the initial report is the Internet's status as a global infrastructure and ICANN's status as a uniform policy maker for the global DNS. One of the main reasons for creating ICANN was to ensure that the DNS would have a globally consistent set of rules. We strongly oppose fragmenting the policies regarding domain name registration data on a geographic basis for that reason. ICANN should strive as much as possible to keep its rules and requirements the same for the entire DNS. This helps maintain the global compatibility of the Internet. Rationale: None provided Other Risks: No response	A. Mark Massey; Domain Name Rights Coalition	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
17.	On November 16, 2018, The EPDB issued Guidelines 3/2018 on the Territorial Scope of the GDPR. These Guidelines address the factors mentioned above. The Guidelines should be consulted by the EPDP Team as it considers the question of differentiating between registrants on a geographic basis. The Guidelines were issued following the expression of positions from contracted parties that it would not be feasible to distinguish between registrants on a geographic basis for the purposes of determining whether the GDPR should be applied. These positions should be reevaluated and further justified in light of the Guidelines, which suggest that it would be possible to agree that redactions to the data of registrants for the purposes of compliance with the GDPR should only be applied where: (a) the contracted party is collecting such data within the context of an establishment of the contracted party in an EU member state, or (b) the contracted party is targeting domain registration services to EU data subjects. The EPDP Team should continue to consider means to practically implement this principle, but the IPC submits that the principle itself should guide discussions, and not the purported impracticality of geographic differentiation. Rationale: The IPC is concerned that some have sought to globalize the application of the GDPR through the application of a policy that does not oblige contracted parties to apply a geographically limited law in a geographically limited manner. ICANN (and its policies) should not serve as a means to achieve global application of a law that has limited territorial application. ICANN should be primarily concerned with the the objectives set forth in its mission, which has from the inception of the WHOIS framework included the practice of collecting and displaying the information of domain registrants for the purposes of ensuring the security and stability and resiliency of the DNS. To the extent exceptions are required to accommodate national laws, the WHOIS Conflicts Policy was agreed. The purpose of this exercise is to determine how to accommodate exceptions to the collection and processing of data, as it existed prior to the GDPR, to accommodate the GDPR. The purpose should not be to maximize and globalize the application of the GDPR. While doing so may suit the objectives of some stakeholders, it would also raise the risk that some countries may seek to enact counterbalancing rules or laws to oblige disclosure of registrant data for what it considers to be legitimate purposes, leading to a more fractured and complex compliance landscape. Other Risks: The question should also be posed, what are the risks of not differentiating on a geographic basis. Longer term, the risks to the status of ICANN as an independent multistakeholder organization are greater where the geographic limitations of laws are not practically acknowledged in the implementation of its policies.	• Brian King; IPC • 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
18.	The EPDP team should recognize: 1. that the GDPR has no legal force outside the EU's jurisdiction, and so does not bind parties or services that do not have a significant EU nexus. 2. that ICANN President and CEO Göran Marby has made "it a high priority to find a path forward to ensure compliance with the GDPR while maintaining WHOIS to the greatest extent possible." Data Protection and Privacy Update—Plans for the New Year, ICANN Blog (Dec. 21, 2017), https://www.icann.org/news/blog/data-protection-and-privacy-update-plans-for-the-new-year. 3. that an ICANN policy that globalizes EU privacy law in such a way will put strains on the credibility and legitimacy of the multistakeholder governance model and independence of ICANN, increase the odds that nations enact WHOIS or ICANN-specific laws, and lead to fragmentation that creates added complexity in developing and enforcing ICANN policy as well as jeopardizes the security, stability, and resiliency of the DNS system. 4. that geographic differentiation is possible, as evidenced by the policies of certain country code TLDs and geography specific gTLDs to require a geographic nexus to be eligible to register for a domain name. Taken together, these points suggest that contracted parties should be required to differentiate between registrants on a geographic basis and that no redaction of data should occur regarding the collection, processing and sharing of data outside the E.U. in the provision of non-E.U. services. Rationale: It would be inappropriate for an ICANN policy decision to give the GDPR effect beyond the EU's jurisdiction. Such an ICANN policy decision would impinge on the policy prerogatives of other nations and the welfare of their citizens by unnecessarily and inappropriately extending EU privacy policy in a way that limits access to WHOIS data, which serves important law enforcement, consumer protection, public safety, cybersecurity, and intellectual property purposes that ICANN has itself recognized. It is one thing for ICANN policy to require contracted parties to abide by local laws that apply to them; it is another to require the contracted parties to abide by laws that would not otherwise apply, either geographically or in substance, and to do so in a way that contradicts longstanding WHOIS policies regarding the availability of data. In addition, requiring differentiation will lead to more consistent application than a permissive policy, which would likely result in a hodgepodge of different decisions by contracted parties. While prohibiting differentiation would result in a consistent approach, that approach would go beyond the requirements of the GDPR and contradict Göran Marby's statements regarding preserving WHOIS access to the greatest extent possible. Other Risks: No response	Neil Fried; The Motion Picture Association of America	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
19.	RySG comment:The RySG urges the EPDP team to consider the realistic effects of any recommendation that requires a delineation on geographic basis. The RySG reminds the EPDP Team that any recommendations made must ensure: A) that the rights of the data subject are best vindicated and protected; B) that due consideration is given to the state of the art, the nature of the data processed, and the cost of implementation to the contracted parties; C) that the focus of the EPDP recommendations remain in scope, i.e., that recommendations are based on whether the temporary specification, as written, or with modification as necessary, is capable of bringing the contracted parties into compliance with the requirements of the GDPR. The creation of new obligations on the CPH which are not necessary for such compliance, are not in scope for this process. The RySG reminds the EPDP team that there remain numerous considerations which, in our opinion, make a delineation on geographic basis, untenable; to the fore is the inability to adequately identify, with any degree of certainty, whether or not a particular registrant is subject to the GDPR. The ePDP team have provided no clarity as to how geographic delineation would be achieved with current technology and process, merely a suggestion from some quarters, that it MUST occur, or more worryingly, that additional data elements be collected to prop up an untested consent based delineation. The CPH members of the EPDP, are on record as having repeatedly expressed their frustration with such suggested recommendations, in the face of impossible and unrealistic expectations in implementation. For the avoidance of doubt, the RySG does not believe a "rules engine" is an acceptable "solution" and does not support the development of one. Further, the EPDP Team must take into account the widespread use by registry operators of backend providers, which may or may not be in the same jurisdiction as the registry operator and may or may not process data in the EU. This additional processing activity further complicates any potential geographic distinction. To reiterate, under GDPR, it is not sufficient for contracted parties to make this jurisdictional distinction in most cases, or even in nearly all cases. Contracted parties must get this right for all registrants or else the significant sanctions associated with violations of GDPR may apply. As a result, it is the edge cases that matter and until the community can demonstrate that these hard cases can be addressed accurately and reliably, contracted parties should not be required to onboard such significant liability. The RySG notes that the EPDP are not tasked with reinventing the DNS system. The Temporary Specification, as written, permits a registry / registrar to process data in a compliant manner. No change to the Temp Spec is therefore strictly necessary. Rationale: See response to Question 84 Other Risks: See response to Question 84	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
20.	On November 16, 2018, the EPDB issued Guidelines 3/2018 on the Territorial Scope of the GDPR. The Guidelines should be consulted by the EPDP Team as it considers the question of differentiating between registrants on a geographic basis. The Guidelines were issued following the expression of positions from contracted parties that it would not be feasible to distinguish between registrants on a geographic basis for the purposes of determining whether the GDPR should be applied. These positions should be reevaluated and further justified in light of the Guidelines, which suggest that it would be possible to agree that redactions to the data of registrants for the purposes of compliance with the GDPR should only be applied where: (a) the contracted party is collecting such data within the context of an establishment of the contracted party in an EU member state, or (b) the contracted party is targeting domain registration services to EU data subjects. Rationale: ICANN should be primarily concerned with the the objectives set forth in its mission, which has from the inception of the WHOIS framework included the practice of collecting and displaying the information of domain registrants for the purposes of ensuring the security, stability and resiliency of the DNS as well as transparency and accountability. To the extent exceptions are required to accommodate national laws, the WHOIS Conflicts Policy was agreed. The purpose of this exercise it to determine how to accommodate exceptions to the collection and processing of data to accommodate the GDPR. The purpose should not be to maximize and globalize the application of the GDPR. Other Risks: No response	Dean S. Marks; Coalition for Online Accountability	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
21.	On November 16, 2018, the EDPB issued Guidelines 3/2018 on the Territorial Scope of the GDPR. "<https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf > Rationale: The Guidelines indicate that redactions to the data of registrants for the purposes of compliance with the GDPR should only be applied where (a) the contracted party is collecting such data within the context of an establishment of the contracted party in an EU member state, or (b) the contracted party is targeting domain registration services to EU data subjects. Other Risks: Although it is likely that additional privacy laws will be passed outside of the GDPR zone, it is not certain that such laws will be subsets of GDPR (i.e. application of GDPR-like redaction to all geographies may not remove additional legal obligation). History has shown that various compliance requirements are usually overlapping and intersecting rather than super/subsets. It would be short-sighted to create a new policy which is inherently unable to accommodate geographic differences and the local-law variations they represent. There are country-based laws, as well as regional laws and treaties that are important for parties to be aware of in the event that specific business conduct is contemplated.	Jeremy Dallman, David Ladd – Microsoft Threat Intelligence Center; Amy Hogan-Burney, Richard Boscovich – Digital Crimes Unit; Makalika Naholowaa, Teresa Rodewald, Cam Gatta – Trademark; Mark Svancarek, Ben Wallace, Paul Mitchell – Internet Technology & Governance Policy; Cole Quinn – Domains and Registry; Joanne Charles – Privacy & Regulatory Affairs; Microsoft Corporation	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
22.	The EPDP may not introduce such a complication for Registrars and Registries, but would rather insist on the non-geographic nature of the Domain Name System. Rationale: It would reverse the evolution of the global DNS; Also, it is not practical for Registries and Registrars to differentiate between Registrants on a geographical basis and grant different privileges, apply different rules between Registrants from different Economic Zones, from across 195 countries, some with multiple provincial legal frameworks. Other Risks: No response	Sivasubramanian Muthusamy; Internet Society India Chennai	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
23.	No response Rationale: No response Other Risks: There are risks associated with NOT differentiating registrants on a geographic basis. Under GDPR a registrar who operated solely outside of the EU and does not explicitly target potential registrants within the EU is not subject to GDPR. Cybersecurity professional have effectively used registration data to combat Internet security issues. The more information that is redacted, the more these cybersecurity professionals are crippled in their efforts. It is known that certain contracted parties have welcomed those who register domains for abusive uses. Allowing those contracted parties outside of the EU to redact all information gives the domain name abusers free reign. Note that a new guidance document from the EDPB makes it clear that an entity wholly external to the EU that does not explicitly target customers within the EU is NOT subject to GDPR, even if some customers in the EU happen to utilize their services.	Evin Erdoğdu; ALAC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
Not designated			

#	Comment	Contributor	EPDP Response / Action Taken
24.	No comments submitted for this question.	• David Martel • Etienne Laurin • Steve Gobin; Corporate domain name management • Ivett Paulovics; MFSD Srl URS Provider • Monica Sanders; i2Coalition • Theo Geurts • Brian Beckham; Head, Internet Dispute Resolution Section at WIPO • Domain.com, LLC & affiliates • Ashley Roberts; Valideus • Ashley Heineman; NTIA • Ben Butler; SSAC • Renee Fossen; Forum - URS and UDRP Provider • Michele Neylon; Blacknight Internet Solutions Ltd • Tim Chen; DomainTools • Stephanie Perrin • Fabien Betremieux; GAC	**EPDP Response:** none **Action Taken:** none [COMPLETED]

Question #3 - Legal v. Natural Persons

#	Comment	Contributor	EPDP Response / Action Taken
	a) What other factors should the EPDP team consider about whether Contracted Parties should be permitted or required to differentiate between natural and legal persons? b) Please provide the rationale for your above answer. c) Should there be further study as to whether procedures would be feasible to accurately distinguish on a global scale whether registrants/contracted parties fall within jurisdiction of the GDPR or other data protection laws? Please provide a rationale. d) Are you aware of existing examples where a legal/natural differentiation is already made and could it apply at a global scale for purposes of registration data? If yes, please provide additional information.		
25.	a) ICANN has NEVER limited registration of domain names to just "natural persons" and "legal entities." See 2013 RAA 3.7.7.1 "… Registered Name Holder that is an organization, association, or corporation …" Many unincorporated organizations and associations are not "legal entities" -- see https://content.next.westlaw.com/Document/I25017386e8db11e398db8b09b4f043e0/View/FullText.html In addition, many businesses are licensed or registered by state authorities as simply a DBA — also known as a trade name, fictitious name, or assumed name -- see https://www.sba.gov/business-guide/launch-your-business/choose-your-business-name. b) Rationale included in answer above. c) No. The EPDP should not be rendering legal advice. See ICANN v. EPAG Domainservices, GmbH. d) no response No.	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
26.	a) Yes, scalability and diverse impacts must be studied. b) i2Coalition notes that small business, which still make up the majority of Internet infrastructure companies, would be significantly adversely affected if required to add the layers of complex systems that are currently understood to be needed to differentiate registrants, both in terms of geography and with respect to legal versus natural registrants. Policies and procedures must not be so complex that only large incumbents have the resources to manage them. c) Yes, and there should be a study about the EPDP's scope and jurisdiction on this matter. It is important to maintain a sense of scope with respect to the EPDP. It an expedited policy regime, confirming the wording of a temporary specification is appropriate where there is consensus. In this instance, the questions is whether the temporary specification is sufficient to allow for GPDR compliance without further policy development. This is a more complex initiative that will require gaining further input and consensus. This may not be within the scope of EPDP. d) no response	Monica Sanders; i2Coalition	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
27.	a) The Initial Report does not discuss or weig the risks of over-redaction, such as how it inhibits contactability, anti-abuse and law enforcement efforts, and accuracy complaints. The act of balancing has not been performed adequately. b) no response c) Yes, there should. See above. d) Yes. See RIPE-NCC's relevant policies and practices. Nominet procedures for indicating and validating legal versus natural versus "commercial use".	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
28.	a) GDPR clearly states that it is not applicable to Legal persons. So clearly ICANN and Contracted Parties should avoid violation of GDPR, and differentiate between natural and legal persons, as far as collection, storage and display of WHOIS data is concerned. b) See #87 c) As per our answer in response to an earlier question we support that there needs to be further study. However, we also wish to emphaisize over here that there needs to be more done than merely study and there should in fact be a concerted effort on part of ICANN to get the contracted parties to agree to implement a solution that can be applied in such a way that it should be accurately possible to distinguish between registrants on a geographical basis. d) No	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.]
29.	a) See RrSG comment b) See RrSG comment c) no response d) No. Any study would not change the basis for the above rationale, so there would be no point on spending time and resources on it.	Volker Greimann; Key-Systems GmbH	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
30.	a) Suggest referring to legislation on unfair commercial practices b) no response c) Not until there is a decision on which address qualifies as the domicile/jurisdiction of the registrant (see also anonymized/proxy registration) d) no response	Monique A. Goeschl; Verein für Anti-Piraterie der Film- und Videobranche (VAP)	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
31.	a) It is simply not possible for a registrar to know whether a registrant is a natural person or a legal person with sufficient certainty to protect those whose data must be protected. Tucows conducted a sampling of domains registered to our family of registrars and noted that the majority of the data in the "org" field was the same as what appeared in "Registrant Name" or was a placeholder. We strongly caution against using this field as indicative of anything. In addition, the risk of releasing data is high: both to the natural person whose personal data was compromised and made public and to the company that released it. The monetary penalties to the company, however, pale in comparison to the compromised privacy of the natural person. Finally, there are many and varied similar laws, including in Argentina and the United States. Developing systems that respect personal privacy rather than adhere to a Eurocentric worldview is simply good sense. b) no response c) Tucows believes that privacy is a right that ought not inure solely to European citizens. As there are many current laws that also protect the privacy of the individual—and others being debated—we do not see value in conducting such a study. d) CIRA, the .ca registry, differentiates between "Individual" and "Non-Individual" domain registrant types; this is done by requiring each registrant to self-select from a set of possible options (https://cira.ca/canadian-presence-requirements-registrants). CIRA provides a Privacy service Domains owned by Individuals while publishing the contact info for domains owned by non-Individuals. This method does not scale for global use. It is a fairly common occurrence for a registrant to select incorrectly, and be surprised to find that their personal contact information has been published by the registry Whois page and made fully available on the Internet. If the person type is optionally self-reported it will be inconsistently used and unreliable, while if it is made mandatory in order for the registrar to validate the registrant's status then it violates the GDPR's principle of data minimization, since our industry history shows that domains can be registered without collection of this personal data.	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
32.	a) Contracted parties should not be required to make the distinction between natural and legal persons as legal persons' data can include personal data, which constitutes compliance risks. If and when there is a sufficient level of certainty that different treatment based on the self-identification by the registered name holder is a practice that will not be sanctioned by the authorities, a distinction can be considered. A sufficient level of certainty could be established with an affirmative statement by competent authorities, the EDPB or a code of conduct according to Art. 40 GDPR. b) no response c) No. A study will not help resolve the compliance questions. d) We are not aware of any examples where the practice of making a distinction between natural and legal persons has been approved by a competent authority.	• 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.]

#	Comment	Contributor	EPDP Response / Action Taken
33.	a) GoDaddy's position on this topic has been previously noted here, https://mm.icann.org/pipermail/gnso-epdp-team/2018-November/000749.html b) Our high-level concerns are reiterated here: Legal: As other laws are less clear regarding the distinction between legal and natural, future regulations may run contrary to GDPR. Technical: a technical basis to reliably and confidently distinguish between legal and natural persons do not exist, and self-identification would be fraught with error creating unacceptable levels of risk. Commercial: There are practical challenges as well as significant cost, presuming a technology can be developed. Risk v. Benefit: Asymmetrical burden and risk placed on contracted parties for the exclusive benefit of unburdened third-parties. Scope: The distinction between Legal and Natural persons, or geographic regions, does not currently exist in the Domain Name System. Therefore, any recommendation mandating this change is outside the scope of the ePDP, and possibly the "picket fence" of Registrar and Registry contracts. c) no response d) no response	Sara Bockey; GoDaddy	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
34.	a) See above. [Geo?] b) See above. [Geo?] c) No. Any study would not change the basis for the above rationale, so there would be no point on spending time and resources on it. d) There are several European ccTLD registries which make such a distinction, however introducing such efforts at this late stage for all gTLDs across the board would be unfeasible, presenting a significant technical and logistical burden which disproportionately affects smaller registrars. Additionally, the existence of such programs in other contexts does not alleviate the concerns raised in #84 above, which remain valid and pose significant risks.	Zoe Bonython; RrSG	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
35.	a) GDPR does not apply to legal persons b) 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." c) no response d) There are other public online resources that make information associated with legal persons publicly available. Most notably are the business registers that are maintained and published by most European countries and consolidated by the European Business Register.	Ashley Heineman; NTIA	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
36.	a) The GDPR states clearly that it "does not cover processing of personal data which concerns legal persons." We recommend that registrars be required to deploy mechanisms that ensure a reliable declaration or determination of natural or legal person status for new registrations going forward, and to eventually obtain those declarations or determinations for existing registrations and their registrants. b) Contact data associated with natural persons should be published in RDS. In SAC101, SSAC stated: "The new policy [The Temporary Specification] allows RDDS operators complete freedom to choose when to redact domain contact data from publication, whether or not a domain contact is protected by GDPR or by any other local privacy law. The result has been blanket redactions, hiding more data than is legally called for. A more balanced and justified approach is needed…. access should not be less timely, more restricted, and less public than law requires…. We also note that as of this writing, most ccTLD operators in the European Union continue to publish some (and sometimes all) contact data fields for domains registered by legal persons. Some continue to publish some personal data for natural person registrants in public WHOIS output. c) SAC101 also highlights RIPE-NCC's solution, which allows for the publication of data about natural persons contained in the contact data for legal persons. This process provides mechanisms that RIPE-NCC says were specifically designed to comply with GDPR. The RIPE-NCC solution seems to be balanced in that it provides contactability and does not over-apply the law. SSAC believes that RIPE's model deserves a full examination and neutral legal evaluation. d) 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
37.	a) Considering the risk of fragmentation from a permissive regime and existing examples where a legal/natural differentiation is already made, INTA is of the view that this distinction is necessary and practicably achievable. The solution that the Contracted Parties/NCSG have proposed (namely, that differentiation between natural and legal persons should be permitted, but not required) appears to suit the conveniences of those parties, but is an incongruous means of addressing the purported risk of possible inadvertent disclosure of personal data relating to natural persons who work for or represent a legal person – such as natural persons who manage administrative or technical issues on behalf of a legal person registrant. The EPDP should not ignore that if policy makers and legislators had intended the GDPR to cover a broader group of data subjects, they would have specifically said so. While implementation may be a challenge, ICANN should not through its policies effectively extend the reach of the GDPR to an entirely separate class of data subject. b) Fragmentation - INTA has provided its rationale as to "fragmentation" in its Response to the question above. Existing examples - INTA has provided its rationale as to "existing examples" in its Response to the question above and has provided existing examples for the "legal vs. natural person" distinction in its Response to the question below. Fit - INTA agrees with the Initial Report that there may be some risk that stems from the fact that natural persons employed by a legal person (and who may be designated as the registrant, admin, or technical contact for that legal person) still enjoy rights and protections under the GDPR – even if their employer does not.[1] INTA is concerned that the Initial Report does not explain why the EPDP thinks the best way to address that risk is to permit Contracted Parties to make their own determination as to whether (and how) to differentiate between legal and natural persons. INTA respectfully suggests that a permissive regime would more likely exacerbate that risk (given the lack of uniformity for registrants across different Contracted Parties) than ameliorate it. INTA supports the alternative proposal referenced in the Initial Report namely, that the risk of inadvertent disclosure "may be minimized through clear explanatory language beneath each field when filling in data fields within domain name registrations". This solution is far more likely to address the potential risk identified. INTA does not share the concern that such explanatory language may be somehow inconsistent with the concept of "privacy by design." This solution seems tailored for privacy by design. It stands to reason that a policy that leaves the decision of how to handle the legal vs. natural person distinction to each Contracted Party to implement different safeguards on their own will be riddled with inconsistencies. On the other hand, a policy that implements, by design, a consistent explanatory language beneath each data field minimizes the risk of inadvertent disclosure for all registrants across all registries and registrars. Registrants are, therefore, offered informed choice rather than arbitrary decision making by a third party. This outcome is consistent of GDPR principles that keep control of the data with the data subject. c) INTA would welcome further study on procedures that could improve the means to distinguish between different registrants for the purposes of more accurately and precisely applying the GDPR. However, INTA would also wish to note that the Guidelines on the territorial scope of the GDPR that were recently issued by the EDPB shed a great deal more light on what factors need to be taken into account, and should be considered along with additional data about how the registries and registrars that are already making these types of differentiations (namely, geographic differentiations; or legal person vs. natural person differentiations) have already been able to do so. d) Yes. The registry that operates the .TEL gTLD makes this differentiation. So does the .eu ccTLD. See https://www.do.tel/wp-content/uploads/2017/05/Whois_Policy.pdf ("With respect to the amount and type of domain name registrant data provided in response to queries of the WHOIS service by the general public, the WHOIS service will distinguish between domain name registrants that are companies, businesses, partnerships, non-profit entities, associations, or other types of legal constructs ('Legal Persons'), and domain name registrants that are human beings, perceptible through the senses and subject to physical laws ('Natural Persons'). Domain name registrants will be required to specify whether they qualify as Legal Persons or Natural Persons by clicking the appropriate box during the registration process."). See also https://eurid.eu/d/205797/whois_policy_en.pdf.	Lori Schulman Senior Director, Internet Policy; International Trademark Association (INTA)	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
38.	a) The current discussion in the Initial Report covers all of the relevant factors regarding natural vs legal persons. There is a clear choice between staying firmly within the boundaries of data protection law on the one hand, and exposing more data for the sake of data miners and surveillance interests on another hand. The NCSG strongly believes that there is no need to consider additional factors. b) The NCSG strongly opposes any attempt to require registrars to separate natural and legal persons at the point of registration. Any attempt to sort out who is an organization and who is a natural person will pose major risks, and impose major cost burdens, on the contracted parties. More importantly, however, Registered Name Holders will be at risk of harm, because many registrants will not understand the distinction and will end up being misclassified as organizations and thus lose their legal entitlement to data protection. Furthermore, the GDPR does not distinguish between the protection of natural and legal persons per se, but rather the protection of personal data of natural persons, which is very likely to be included in gTLD Registration Data of domain names registered by legal persons. The obvious example is the Registered Name Holder email address, which would belong to an employee or representative of the legal person, typically being name@domain.TLD. c) No. The "E" in EPDP means expedited. The purpose of this exercise is to quickly turn the temporary specification into a consensus policy following ICANN procedures. Pausing to conduct studies about adding new elements into domain registration contracts is not appropriate in this expedited proceeding. Stakeholders who want to explore this further, have the possibility to initiate new PDPs after the tight deadline for this EPDP is met. New policies can always be proposed. The NCSG believes that there is no time for further studies within the timeframe of this EPDP. d) There are no directly applicable examples that would work at a global scale.	Ayden Férdeline; NCSG	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
39.	a) The team should revisit Recital 14 of the GDPR, which states: Protection afforded by this Regulation should apply to Natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data, which concerns Legal persons and in particular undertakings established as Legal persons, including the name and the form of the Legal person and the contact details of the Legal person. b) Registrars should distinguish between Natural and Legal persons when accepting registrant data for a domain name registration. Legal person data should not be treated as a Natural person's data since the GDPR does not apply. c) no response d) no response	Sajda Ouachtouki; The Walt Disney Company	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
40.	a) The current discussion in the initial report covers all of the relevant factors regarding natural vs legal persons. There is a clear choice between staying firmly within the boundaries of data protection law on the one hand, and exposing more data for the sake of data miners and surveillance interests. There is no need to consider additional factors. b) We strongly oppose any attempt to require registrars to separate natural and legal persons at the point of registration. Any attempt to sort out who is an organization and who is a natural person will pose major risks to data protection and impose major cost burdens and risks on the contracted parties. Many registrants will not understand the distinction and will end up being misclassified as organizations and thus lose their data protection. c) No. The "E" in EPDP means expedited. The purpose of this exercise is to quickly turn the temporary specification into a consensus policy following ICANN procedures. Pausing to conduct studies about adding new elements into domain registration contracts is not appropriate in this proceeding. Stakeholders who want to explore this further can initiate new PDPs after we have met the tight deadline for this EPDP. New policies can always be proposed. We simply do not have to the time to do so this time around. d) There are no directly applicable examples that would work at global scale.	Farzaneh Badii; Internet Governance Project	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
41.	a) The team should revisit Recital 14 of the GDPR: Protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data, which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person. A registrar should distinguish between natural and legal persons when accepting registrant data for a domain name registration. Legal person data should not be treated as a natural person's data since the GDPR does not apply. b) As the BC has stated above, legal persons' data should be publicly accessible. A registrar or registry should make the distinction between natural and legal persons in their processes and keep the data separate from natural persons' data so as not to confuse the treatment of legal persons' data. c) no response d) Many ccTLD registries differentiate between natural and legal persons in the registration process. The extensive list below demonstrates that this differentiation is both practical and workable: .AT: Legal person data is publicly available in the whois and provides the organization, Street address, postal code, city, country, phone, email, and NIC handle. .BE: Legal person data is publicly available in Whois and provides the organization, language, street address, city, country and phone. A contact form is available. .CZ: Legal person data is publicly available in Whois and provides registrant organization, street address, city, country and NIC handle. It also provides the same data fields for admin and tech contacts. .DK: Natural and legal person data is treated identically in the publicly available whois and provides registrant organization, street address, city, country and nic-handle. (See .dk statement - https://www.dk-hostmaster.dk/en/gdpr) .ES: Legal person data is publicly available in Whois and provides registrant organization, admin contact name and name of technical contact. .EU: This ccTLD differentiates in the publicly available Whois record and provides the registrant name, language, city, country and email address. .FI: Legal person data is publicly available in the Whois and provides the registrant name, street address, city, country and phone. The technical contact's name and email address are available. .FR: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country, phone and email address; the technical contact's name, registrant org, street address, city, country, phone and email address; and the admin contact's, name, registrant org, street address, city, country, phone and email address. .IE: Legal person data is publicly available in Whois and provides the registrant organization, admin and tech NIC handles. .IT: Legal person data is publicly available in Whois and the registrant organization, street address, city, country postal code, phone number and email address. The same data fields are available for admin and tech contacts and include individual names. .LT: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code, phone number and email address. The same data fields are available for tech contact. .LV: This ccTLD distinguishes between natural and legal persons. Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code, phone number and email address. The same data fields are available for admin and tech contact and includes individual names. .LU: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country and postal code. The admin and tech contacts are masked. .MT: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code, phone number and email address. The same data fields are available for admin and tech contact. .NL: Legal person data is publicly available in Whois and provides the registrant organization and admin email address. .PL: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code. Organization is indicated in the record. .PT: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country and postal code. The same data fields are available for the managing body role. .SI: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code, phone number and email address. The tech contact's email address also is provided. .SE: Legal person data is publicly available in Whois and provides the registrant organization, street address, city, country postal code, phone number and Contact ID. The same data fields are available for admin and tech contacts and includes individual names.	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
42.	a) A domain registration for a Legal Person is an act of a Legal Person. Any data present in that registration is not subject to GDPR, including the business email of an employee. b) no response c) no response d) no response	Tim Chen; DomainTools	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
43.	a) DNRC strongly opposes any attempt to require registrars to separate natural and legal persons at the point of registration. Any attempt to sort out who is an organization and who is a natural person will pose major risks to data protection and impose major cost burdens and risks on the contracted parties. Many registrants will not understand the distinction and will end up being misclassified as organizations and thus lose their data protection. Furthermore, the GDPR does not distinguish between the protection of natural and legal persons per se, but rather the protection of personal data of natural persons, which is very likely to be included in gTLD Registration Data of domain names registered by legal persons. The obvious example is a registrant's email address, which would belong to an employee or representative of the legal person, typically being name@domain.TLD. b) no response c) no response d) no response	A. Mark Massey; Domain Name Rights Coalition	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
44.	a) The other factors to consider are the practicalities of application and looking to live examples of other businesses and entities that are differentiating between legal and natural persons because that is how the GDPR is set-up and it needs to be applied as intended, if not immediately, eventually. Therefore, if not required immediately, it should be required to be implemented within a reasonable timeframe when the technical set-up is commercially feasible. It is possible to set-up a self-identification system, with supportive educational language, alerting RNH to the definitions of legal and natural persons and to specify that any information provided is attested to be true, accurate and submitted to the best knowledge of the RNH. We note that in the GDPR Domain Industry Playbook v. 1.0 issued by eco it was recommended that "input from DPAs should be sought as to whether a distinction could be made based on a self-identification by the registrant." Due account should be taken of existing registers (ccTLD, company, trademarks, etc.) to which the GDPR applies. Based on existing processes with various ccTLD registry operators, such as EURid, the distinction can be made based on the self-identification of the registrant together with clear information on the implications of each choice. The registrant must be made aware that the name and contact information of a legal person will be published and that he is responsible for providing non-identifiable contact information. With regard to natural persons designated as admin or technical contact, an option can be provided to redact the name of that person in case he/she is a natural person. b) The distinction would prevent the over-application of the GDPR and allow for the required transparency and accountability online. The information of legal persons must be made available by default for law enforcement, consumer protection, anti-counterfeiting and cybersecurity purposes. In this regard, the EU E-Commerce Directive also requires legal entities who provide services to Internet users to be transparent and provide their identification and contact information in a direct and easily accessible manner (Art. 5 E-Commerce Directive 2000/31/EC). An incorrect self-identification could serve as an indication of bad faith and a legitimate reason for the registrar or registry to immediately disclose the identity and contact information of the underlying registrant upon request. The risks of making the above distinction would be minimal. Registrars would only be required to provide clear information so to avoid unnoticed or unintended publication of personal data. A person registering a domain name for a legal person is not required to provide contact information which are related to an identified or identifiable natural person as this contact information can easily be anonymized (i.e. domainadmin@company.com). In situations where it is difficult to separate the data of natural persons from that of legal persons, such as if the legal person is a sole proprietorship, if the name of a person appears in the company's name, or if the business address is a natural person's residence, this relevant (personal) information is also made public on a mandatory basis in the national company register where the legal entity is registered (see art. 30 and onwards of Directive 2017/1132). Registrars would not face an increased liability unless related to their transparency requirements. Sufficiently clear information must be provided to prevent a registrant from unwillingly disclosing personal data. With regard to the provision / collection of information, it is not required to discharge the registrant of all responsibility for providing non-identifiable information, as long as the registrant is properly informed. c) The IPC supports a study showing live examples of the application of the natural and legal persons differentiation. MM - This appears to be feasible but impractical. It does not appear that the outcome of this study would be useful; instead MarkMonitor supports a study showing live examples of the application of the natural and legal persons differentiation. d) The .TEL gTLD has been making this distinction since at least 2006. See TEL Registry Agreement, Appendix S, Part VI, Section B, (May 2016). Generally, in ccTLDS and certain gTLDs, a system of self-identification is implemented where a potential registrant must indicate whether it is a natural or legal person (most notably EURid for .eu, and others below). The registrant is informed of the implications of this choice (such as the publication of the legal person's name and contact information) before registering. A registrant which is a legal person must then evaluate whether his contact information refers to an identified or identifiable natural person and adjust accordingly (or not). EURid's Domain Name Whois Policy v. 4.0, Sections 2.3 - 2.4 provides that "those requesting to register a .eu Domain Name in one of the available scripts are required to provide certain information through an accredited Registrar. In respect of the name of the Registrant there are two fields: The first is 'Name' and the second is 'Company'. Both fields may be completed or just the 'Name' field. If only the first field is completed, it is assumed that the registration is in the name of a private individual (natural person). If the 'Company' field is completed, it is assumed that the company is the Registrant. ... All Registrants are required to accept the Terms and Conditions in which the Registrant authorises the Registry to publish certain personal data. (i) When the Registrant is a legal person or another form of organisation the Registry generally publishes the following information in its WHOIS: a) name, address and telephone and fax number of the Registrant; b) technical contact person; c) e-mail address ...". [Domain Name Whois Policy v. 4.0, EURid, available at https://eurid.eu/d/22380/whois_policy_en.pdf] The CENTR Report on WHOIS Status and Impacts from GDPR determined that "to differentiate between private and organisations as registrants, 68% of registries allow the registrant to self-select. In several cases, the registry uses social security number, business number or even tax file number. 18% make no distinction." [CENTR Survey - Whois status and impacts from GDPR, June-July 2018, available at https://centr.org/library/library/survey-report/centr-report-whois-status-and-impacts-from-gdpr.html.] For trademark applications in the EU or national trademark registers, an applicant is asked whether he is a natural or a legal person. Irrespective of the distinction, the name and address of the applicant is always made publicly available, as this information is considered to be of public interest (article 111(9) Regulation 2017/1001). .AT legal person data is publicly available in the whois and provides the organization, Street address, Postal code,City, Country, Phone , Email,Nic-hdl .BE legal person data is publicly available in the whois and provides the Organization, language, street address, city, country and phone. Contact form available .CZ legal person data is publicly available in the whois and provides registrant organization, street address, city, country and nic-handle. Also provides the same data fields for admin and tech contact. .DK treats natural and legal person data the same in the publicly available whois and provides registrant organization, street address, city, country and nic-handle. See .dk statement - https://www.dk-hostmaster.dk/en/gdpr .ES legal person data is publicly available in the whois and provides registrant org, admin contact name and name of technical contact .EU differentiates in the publicly available WHOIS record and provides the registrant name, language, city, country and email address. .FI legal person data is publicly available in the whois and provides the registrant name, street address, city, country and phone. Technical contact name and email address. .FR legal person data is publicly available in the whois and provides the registrant org, street address, city, country, phone and email address. Technical contact name, registrant org, street address, city, country, phone and email address. .IE legal person data is publicly available in the the whois and provides the registrant org, admin and tech nic-handles .IT legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code, phone number and email address. Same data fields are available for admin and tech contact and includes individual names. .LT legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code, phone number and email address. Same data fields are available for tech contact. .LV distinguishes between natural and legal person. Legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code, phone number and email address. Same data fields are available for admin and tech contact and includes individual names. .LU legal person data is publicly available in the the whois and provides the registrant org, street address, city, country and postal code Admin and Tech contacts are masked. .MT legal person data is publicly available in the the whois and provides the registrant org, street address, city, country postal code, phone number and email address. Same data fields are available for admin and tech contact. .NL legal person data is publicly available in the the whois and provides the registrant org and admin email address.	• Brian King; IPC • Brian King; MarkMonitor, Inc., a Clarivate Analytics company • Dean S. Marks; Coalition for Online Accountability	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
45.	a) The EPDP team should recognize: • that the GDPR applies only to natural persons, see GDPR, art. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN), and so does not require redaction of any data regarding businesses or other legal persons. • that ICANN President and CEO Göran Marby has made "it a high priority to find a path forward to ensure compliance with the GDPR while maintaining WHOIS to the greatest extent possible." Data Protection and Privacy Update—Plans for the New Year, ICANN Blog (Dec. 21, 2017), https://www.icann.org/news/blog/data-protection-and-privacy-update-plans-for-the-new-year. • that an ICANN policy that overbroadly applies the GDPR will put strains on the legitimacy of the multistakeholder governance model, increase the odds that nations enact WHOIS or ICANN-specific laws, and lead to fragmentation that creates added complexity in developing and enforcing ICANN policy as well as jeopardizes the security, stability, and resiliency of the DNS system. • that differentiation between natural and legal persons is possible, as evidenced by the practices of certain country code TLDs and gTLDs to do precisely that. Taken together, these points suggest that contracted parties should be required to differentiate between natural and legal persons and that no redaction of data should occur regarding the collection, processing, or sharing of data related to legal persons. b) It would be inappropriate for an ICANN policy to apply GDPR beyond its scope. Such a decision would unnecessarily and inappropriately limit access to WHOIS data, which serves important law enforcement, consumer protection, public safety, cybersecurity, and intellectual property purposes that ICANN has itself recognized. In addition, requiring differentiation will lead to more consistent application than a permissive policy, which would likely result in a hodgepodge of different decisions by contracted parties. While prohibiting differentiation would result in a consistent approach, that approach would go beyond the requirements of the GDPR and contradict Göran Marby's statements regarding preserving WHOIS access to the greatest extent possible. c) no response d) no response	Neil Fried; The Motion Picture Association of America	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
46.	a) The EPDP team is urged to consider the realistic effects of any recommendation that requires a delineation on natural/legal person basis. The RySG reminds the EPDP Team that any recommendations made must ensure: A) that the rights of the data subject are best vindicated and protected; B) that due consideration is given to the state of the art, the nature of the data processed, and the cost of implementation to the contracted parties; C) that the focus of the ePDP recommendations remain in scope, i.e., that recommendations are based on whether the temporary specification, as written, or with modification as necessary, is capable of bringing the contracted parties into compliance with the requirements of the GDPR. The creation of new obligations on the CPH which are not necessary for such compliance, are not in scope for this process. The RySG reminds the EPDP team that there remain numerous considerations which, in our opinion, make a delineation on legal / natural person, untenable; to the fore is the inability to adequately identify, with any degree of certainty, whether or not a particular registrant is subject to the GDPR or not. The EPDP team have provided no clarity as to how such a delineation would be achieved with current technology and process, merely a suggestion from some quarters, that it MUST occur, or more worryingly, that additional data elements be collected to prop up an untested consent based delineation. The CPH members of the EPDP, are on record as having repeatedly expressed their frustration with such suggested recommendations, in the face of impossible and unrealistic expectations in implementation. To reiterate, under GDPR, it is not sufficient for contracted parties to make this distinction in most cases, or even in nearly all cases. Contracted parties must get this right for all registrants or else the significant sanctions associated with violations of GDPR may apply. As a result, it is the edge cases that matter and until the community can demonstrate that these hard cases can be addressed accurately and reliably, contracted parties should not be required to onboard such significant liability. The RySG notes that the ePDP are not tasked with reinventing the DNS system. The Temporary Specification, as written, permits a registry / registrar to process data in a compliant manner. No change to the Temp Spec is therefore strictly necessary. b) See response to Question 87. c) The RySG would pose the question as to how research of other, as of yet untested applications, in different industries, or even in domain name registration outside of the ICANN construct, would be beneficial. Review of the deliberations thus far has provided the team with on the record statements as to the current unavailability of the adequate technological means to implement any such mandatory delineation, that may be considered to be expert opinion, based on experience of both day to day implementation concerns as to available technology, implementation difficulties and on the basic feasibility of such a policy recommendation for all members of the CPH, from small scale, to large. We are unsure as to why further delay and expense regarding 'further research' is considered to be necessary here. d) No	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
47.	a) It is practical to design a user experience which at the time of registration clearly informs the registrant of the data processing which will occur in their geography and how such processing may be impacted by their identification as a legal person or as a natural person. Such a system might include self-attestation, be derived from other data such as use of the Organization field or use of a purchase order, or a combination of several factors. Note that many European country-code registries already apply geography-specific policies, which should demonstrate the practicality of such an approach. b) Unnecessary redaction of data makes investigations and dispute resolution unnecessarily difficult. A registrar should clearly inform the registrant of the data processing which will occur in their geography and how such processing may be impacted by their identification as a legal person or as a natural person, then make a distinction between natural and legal persons during registration and publish the registration data of companies separate from natural persons. Note that in situations where it is difficult to separate the data of natural persons from that of legal persons, such as if the legal person is a sole proprietorship, if the name of a person appears in the company's name, or if the business address is a natural person's residence, this relevant (personal) information is already made public on a mandatory basis in the national company register where the legal entity is registered (see art. 30 and onwards of Directive 2017/1132). c) no response d) Many examples from various ccTLDs and gTLDs have been provided by multiple other parties and will not be repeated here. Suffice it to say that there is enough evidence that the distinction is being routinely made by many registries.	Jeremy Dallman, David Ladd – Microsoft Threat Intelligence Center; Amy Hogan-Burney, Richard Boscovich – Digital Crimes Unit; Makalika Naholowaa, Teresa Rodewald, Cam Gatta – Trademark; Mark Svancarek, Ben Wallace, Paul Mitchell – Internet Technology & Governance Policy; Cole Quinn – Domains and Registry; Joanne Charles – Privacy & Regulatory Affairs; Microsoft Corporation	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
48.	a) The GAC would recommend that the temporary specification require contracted parties to treat legal and natural persons differently because, the GDPR "does not cover processing of personal data which concerns legal persons." (Recital 14). Hence, as we recognized in our San Juan Communique advice, the personal information of legal persons should be part of the publicly available WHOIS data. We recommend that contracted parties develop mechanisms that ensure a reliable determination of natural or legal person status for registrants going forward (post- implementation of new contract specifications) and for their legacy registrants and recognize that these procedures will likely require a phased approach that allows more time for contracted parties to deal with their legacy customers. However, we recognize that there are challenges in making this distinction in the context of domain name registrations as well as the potential implementation of any new functionality that would apply to pre-existing registrations. Additionally, other jurisdictions may have other categories of protected groups or other requirements that would need to be factored in. Consequently, we recommend that the EPDP WG: • research how ccTLDs and contracted parties currently distinguish between natural and legal persons; • consider which data fields (if any) need to be added to accomplish this distinction (this could require further liaising with the IETF if data fields in RDAP need to be added or changed); • consider the timeline needed to implement this requirement which could follow a phased approach whereby implementation would start immediately after agreement on a satisfactory manner to distinguish between legal and natural persons for new registrations while existing registrations would be phased in upon renewal, transfer, or by other means; • direct registries, registrars and ICANN to each develop (educational) resources available that help registrants understand the distinction between a domain name that is registered by a natural person vs. legal person / entity. These resources and communications should highlight that the name and contact information of legal persons will be disclosed in the public WHOIS and therefore encourage legal persons to provide non-personal information for their email address and other contact information. The GAC would also like to point to, as noted previously, the existence of online/public European Business Registers as a potential model to emulate in terms of addressing the challenges associated with differentiating between legal and natural persons. In light of the above, 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. b) no response c) no response d) no response	Fabien Betremieux; GAC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
49.	a) The ALAC strongly supports differentiation of Legal and Natural Persons. GDPR only applies to Legal Persons. Although a Legal Person's registration data may contain personal information, as per EDPB recommendations, they should be advised to take care to ensure that they are not doing so without due authorization. b) The risks listed in reply to #86 apply here as well. If there are particular risks associated with treating specific classes of legal persons as described here, they need to explicitly enumerated with carve-outs. c) The ALAC does not believe that further study is needed, but is willing to consider rationale's provided by others. d) no response	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
50.	a) In Data Protection terminology, "Personal data" is more of a generic or 'loose' term that happens to apply indiscriminately both to individual and business data. In DNS, Registration Data does not make any distinction between individual registrants and business registrants whose web space is for some form of (e)commerce activity. While there is a need for privacy of personal data of individual registrants, the opposite, need for greater transparency, may be required in the case of data related to any form of commercial, perhaps even Government and non Government web spaces. The rationale is that the online presence of small and large businesses alike are often short of information pertaining to physical location, names of functionaries, officials or the person in-charge. A Phone company does not have listed phone number, an email company does not have a visible email addresses! This is part of a pattern of multiple players transacting business online from a carefully guarded climate of "do-not-reply" email accounts, phones without a call back number, answering machines, conveniently assisted by BPO intermediaries who keep the consumer at an unapproachable distance. A hotel reservation portal or a small shop online transacts business online without allowing the consumer the ability to reach them for various reasons Limiting access to Registration data without discrimination of whether the data belongs to an individual as personal data or if it is Registration data of a domain name that points to a commercial web space, and limiting access only for 'legitimate uses' may perpetuate this trend of inaccessibility of business entities, widen the disconnect between business and consumer with the effect that multiple commercial registrants would continue to design their online presence to transact business without due accountability. The sections on Lawfulness & Purposes of Processing gTLD Registration Data as written, might have the unintended consequence of perpetuating unhealthy protection for segments that actually require information disclosure and transparency. EPDP team could actively consider this, and persuasively convey to Europe that ICANN as a responsible global multistakeholder organization would make this distinction in global public interest. Also, for this specific purpose, it is not sufficient to fit data into two classes namely "identifiable natural persons" and "artificial persons". The emphasis here is on Domain Names of Web spaces with commercial activity or intent, usually distinguished by the presence of a payment gateway or other forms of payment information; In this context, it is not sufficient if incorporated companies legally known as "artificial persons" are alone classed for additional data elements for transparency. Commercial Activity could also be undertaken by non-commercial entities in the form of subscription plans or donation requests; by individuals who operate businesses as individuals; Registrant Data needs to make a distinction between personal domain names such as the domain name for a personal blog and a commercial domain name which carries out any form of commercial activity. b) GDPR is a good start. It is a very good start. It seeks to set right certain imbalances concerning the collection and use of personal data. However the GDPR may have to be more balanced in its next versions. What is legislated to safeguard privacy rights may get distorted to compromise other values, such as transparency. One example from history is from the legislation on Rights. A thoughtful author cites in his book, "Of the ten amendments that make up the US Bill of Rights, corporations have successfully asserted the applicability of five to win protections for themselves. These include the First Amendment right to free speech; the Fourth Amendment freedom from unreasonable search and seizures; the Fifth Amendment prohibition against takings and double jeopardy despite the fact that the Amendment clearly refers to natural persons; and the Sixth and Seventh Amendment rights to jury trials in criminal and Civil matters respectively" The instances cited are: "The concept of property rights, originally developed to preserve an individual's right to property is used to grant individual rights to entities that are themselves a form of property. As early as 1818, Congressman Daniel Webster used the idea of property rights to limit a state's influence over a corporation. These were the earliest advances on the road to granting individual rights to fictional persons. This was when real people were still bought and sold as property with fewer protections than corporations." "Corporations aren't specifically mentioned in America's 14th Amendment, or anywhere else in the Constitution. U.S. corporations have sought many of the same rights guaranteed to individuals, including the rights to own property, enter into contracts, and to sue and be sued just like individuals." "A 1978 Court decision on the Bellotti case granted corporations the right to spend unlimited funds on ballot initiatives as part of their First Amendment right to freedom of speech; In the 2010 case Citizens United v. Federal Election Commission (FEC), the most sweeping expansion of corporate rights yet, the US Supreme Court cited that political speech by corporations is a form of free speech that is also covered under the First Amendment." Irrespective of how Europe may strengthen the GDPR by way of well considered safeguards against limitations and possible abuses of privacy legislation, the EPDP could work though resistant and misdirectinal arguments on the need to differentiate between natural and legal persons (and go beyond this categorization of differences to further differentiate between domain names for personal and commercial use. c) No d) Even in simple web spaces, such as that of a non-profit organization with a membership form, such a distinction is easily made by a simple form that leads to a different set of questions if the membership is sought by an organization, and often differential membership fee is applied. While technical implementation in the case where Registrants themselves correctly disclose if the domain name is for personal or commercial use, in situations where a commercial domain name Registrant seeks to classify his commercial domain as a personal domain name, certain automated post-domain-registration checks could flag the domain name automatically. These include metadata scanning for commercial keywords, or automated crawling to look for signs of commercial activity such as the presence of a payment gateway or bank account information.	Sivasubramanian Muthusamy; Internet Society India Chennai	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
51.	a) no response b) no response c) Yes. d) Yes, some ccTLD registries such as EURid automatically hide the registrant's data if the registrant is an individual (if the organisation field is left empty) and don't hide it when it is an organisation.	Steve Gobin; Corporate domain name management	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
52.	a) no response b) no response c) No. The only people who benefit from "studies" are the consultants paid to do them d) Several ccTLDs do this, but comparisons between them and gTLDs tend to fail for a number of reasons. First off gTLDs have worked for more than 20 years without this distinction and to attempt to make it now is unworkable. Secondly the ccTLDs often retain a tripartite relationship whereby there is a contractual link between the registrant and the registry. This is not the norm in the gTLD space	Michele Neylon; Blacknight Internet Solutions Ltd	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
Not designated			

#	Comment	Contributor	EPDP Response / Action Taken
53.	No comments submitted for this question.	• David Martel • Etienne Laurin • Ivett Paulovics; MFSD Srl URS Provider • George Kirikos; Leap of Faith Financial Services Inc. • Theo Geurts • Greg Mounier on behalf of Europol AGIS; Europol Advisory Group on Internet Security • Brian Beckham; Head, Internet Dispute Resolution Section at WIPO • Domain.com, LLC & affiliates • Ashley Roberts; Valideus • Renee Fossen; Forum - URS and UDRP Provider • Stephanie Perrin	**EPDP Response:** none **Action Taken:** none [**COMPLETED**]