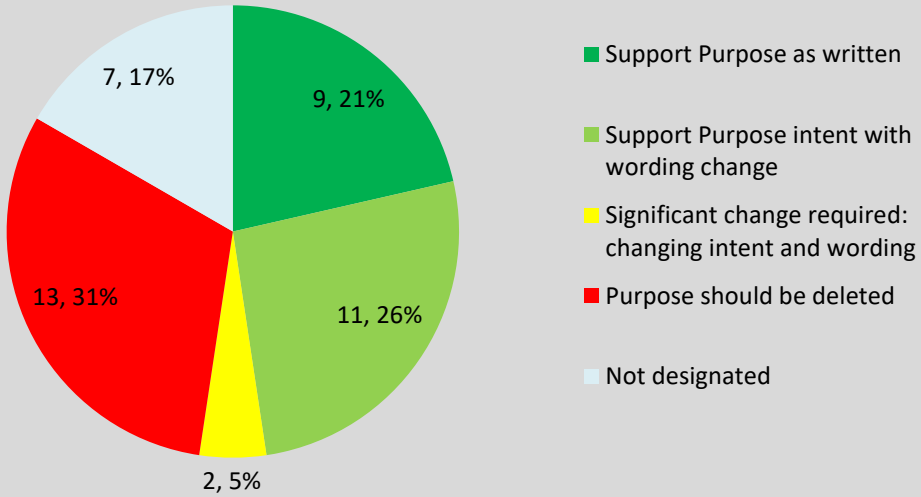
PURPOSE 2

#	Comment	Contributor	EPDP Response / Action Taken
	Maintaining the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission through the enabling of lawful access for legitimate third-party interests to data elements collected for the other purposes identified herein;		



Support Purpose as written

#	Comment	Contributor	EPDP Response / Action Taken
1.	No comments were made in support of this purpose statement.	• Tim Chen; DomainTools • Greg Aaron, iThreat Cyber Group • Monique A. Goeschl; Verein für Anti-Piraterie der Film- und Videobranche (VAP) • David Martel • Etienne Laurin • Ben Butler; SSAC • Evin Erdoğdu; ALAC	Support **EPDP Response:** The EPDP Team appreciates the support. **Action Taken:** None [COMPLETED]
2.	Domain names are valuable assets (worth hundreds of thousands or even millions of dollars) with a lengthy lifetime (i.e. not short-term disposable services like contracts for Netflix or electricity which are fungible and where no historical record is needed). Thus, it's essential that security and stability be maintained, including the provenance of domain name ownership (see my earlier comments for Purpose 1). Legitimate 3rd party interests should include the court system.	George Kirikos; Leap of Faith Financial Services Inc.	Support **EPDP Response:** The EPDP Team appreciates the support. **Action Taken:** None [COMPLETED]
3.	The AG IS expresses support in particular for Purposes 2, 3, and 4, which on their own and cumulatively empower the legitimate interests of the cybersecurity community in using Whois data for cybersecurity and overall data protection purposes. Moreover, it is critical to note that use of the DNS for cybercrime undermines trust in the system and the overall integrity of the DNS.	Greg Mounier on behalf of Europol AGIS; Europol Advisory Group on Internet Security	Support **EPDP Response:** The EPDP Team appreciates the support. **Action Taken:** None [COMPLETED]
Support Purpose intent with wording change			

4.	ENSURING THE SECURITY, STABILITY AND RESILIENCY OF THE DOMAIN NAME SYSTEM IN ACCORDANCE WITH ICANN'S MISSION, COMMITMENTS AND CORE VALUES THROUGH ENABLING LAWFUL ACCESS FOR LEGITIMATE THIRD PARTY INTEREST OF LAW ENFORCEMENT, CYBERSECURITY, COMBATTING DOMAIN NAME ABUSE, CONSUMER PROTECTION AND INTELLECTUAL RIGHTS PROPERTY PROTECTION TO DATA ELEMENTS COLLECTED FOR THE OTHER PURPOSES IDENTIFIED HEREIN ICANN's stated mission is to ensure the stable and secure operation of the Internet's unique identifier systems; therefore Purpose #2 should embody the ""ensure"" language and imperative. Article 13(1) of the GDPR states: “Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: . . . (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;” (emphasis added)"" In order to comply with Article 13(1)(d), it is key that the legitimate interests pursued by the controller or by a third party be spelled out clearly in the Purpose statement and communicated to the data subject AT THE TIME WHEN PERSONAL DATA ARE OBTAINED. As a joint controller, ICANN’s purposes with respect to WHOIS data and registry directory services include, according to ICANN’S Bylaws “whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust, security, stability and resiliency, malicious abuse issues, sovereignty concerns and rights protection.” (ICANN Bylaws Section 4.6). Purpose #2 from the Initial Report only addresses “security, stability and resiliency” and does not address the other ICANN purposes and concerns as articulated in Section 4.6 of the Bylaws. The above suggested edits to Purpose #2 address this deficiency. In addition, the above suggested edits to Purpose #2 seek to ensure compliance with Article 13(1)(d) of the GDPR by: (i) enumerating more specific purposes, and (ii) identifying with greater specificity the legitimate interests of ICANN (as a joint controller) and the legitimate interests pursued by third parties that may seek access to the personal data for processing. Therefore, we believe it is important to spell out explicitly, as we have done in our suggested edits, the legitimate interests of law enforcement, cybersecurity, combatting domain name abuse, consumer protection and intellectual property rights protection. Intellectual property rights	Dean S. Marks; Coalition for Online Accountability	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	protection covers the universally and legally recognized rights of trademark, copyright and patent. In its letter of 11 April 2018, to Goran Marby, the Article 29 Data Protection Working Party stated that "purposes specified by the controller must be detailed enough to determine what kind of processing is and is not included . . . ." The letter also stated that the WP29 "stresses the importance of explicitly defining legitimate purposes in a way which comports with the requirements of the GDPR." Our proposed edits to Purpose #2 seek to incorporate and comply with this legal guidance that ICANN has received.		
5.	THE EVENTUAL GOAL OF MAINTAINING THE SECURITY,STABILITY,AND RESILIENCY OF THE INTERNET DOMAIN NAME SYSTEM IN ACCORDANCE WITH ICANN'S MISSION AS SPECIFIED IN ITS BYLAWS, BY FACILITATING LAWFUL ACCESS FOR LEGITIMATE THIRD-PARTY REQUESTS TO ACCESS DATA ELEMENTS COLLECTED FOR THE OTHER PURPOSES IDENTIFIED HEREIN. Minor language tweaks for sake of clarity and being more explicit.	DR. JAIDEEP KUMAR MISHRA; DIRECTOR MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
6.	MAINTAINING THE SECURITY, STABILITY, AND RESILIENCY OF THE DOMAIN NAME SYSTEM IN ACCORDANCE WITH ICANN'S MISSION. While the enabling of lawful access for legitimate third-party interests to data already collected may be a valid legal basis for processing data, it is not part of ICANN's existing mandate, and the EPDP team should be careful not to overstep the project goals by expanding ICANN's mission.	Tucows Domains Inc.	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
7.	Maintaining the security, stability, and resiliency of the domain name system in accordance with ICANN's mission through the enabling of lawful access for legitimate third-party interests -- including law enforcement, security, intellectual property, and consumer protection needs -- to data elements collected for the other purposes identified herein. Maintaining the stable and secure operation of the Internet's unique identifier systems requires that ICANN ensure access to domain registration data for law enforcement, cybersecurity, consumer protection, and intellectual property protection. Given the important role that access to domain registration data for these purposes plays in practice in the efforts to maintain security, stability and resilience of the domain name system, it is critical that these purposes are clearly identified from the outset. Disney's own experiences have tracked those reported in the multiple studies (SSAC in SAC 101, Anti-Phishing Working Group, Cybersecurity Tech Accord) submitted to this process, documenting that the current access provided today is inadequate – contracted parties are often either slow to respond to legitimate requests or do not respond at all.	Sajda Ouachtouki; The Walt Disney Company	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
8.	Maintaining the security, stability, and resiliency of the domain name system in accordance with ICANN's mission through the enabling of lawful access for legitimate third-party interests -- including law enforcement, security, intellectual property, and consumer protection needs -- to data elements collected for the other purposes identified herein. Purpose 2, as stated, is very general and non-specific. Legitimate third party interests are part of the fabric of security, stability and resiliency for the domain name system. Since the institution of the Temp Spec, the community has seen a degradation in its ability to investigate or address problems in the DNS -- a problem that can be remediated by access granted to these parties. It's important to enumerate the types of third parties that are warranted access for previously identified legitimate purposes. Key findings of multiple studies have clearly demonstrated that lack of reasonable access is causing harm, and that contracted parties are either slow to respond to legitimate requests or do not respond at all: ● As noted by SSAC in SAC 101 (https://www.icann.org/en/system/files/files/sac-101-en.pdf), while legal obligations are a reality and must be complied with, access to registration data under the Temp Spec has been diminished far further than legal obligations require, and further than is prudent for responsible stewardship of the namespace. This point is more true under the EPDP's proposals. The EPDP is obligated to consider the recommendations of SAC 101, and the requirements as listed by the GAC in its recent Communique's related to WHOIS. To date, it has not. ● According to the Anti-Phishing Working Group's study (https://apwg.org/apwg-news-center/icann-whois-access/temporySpecSurvey#_ftn1), cybercrime investigations have been seriously impeded, permitting harm to users, and Whois has become an unreliable or less meaningful source of threat intelligence. ● The Cybersecurity Tech Accord recently published its own study (https://cybertechaccord.org/mechanism_to_access_whois_data/), detailing the fact that partial data in public Whois following redaction is insufficient to investigate or respond to incidents, and that requests for access for legitimate purposes are routinely refused. Access for legitimate purposes is a pressing matter and increasing in urgency."	Steve DelBianco; BC	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
9.	ENSURING THE SECURITY, STABILITY, AND RESILIENCY OF THE DOMAIN NAME SYSTEM IN ACCORDANCE WITH ICANN'S MISSION, AS SET FORTH IN ICANN'S BYLAWS TOGETHER WITH ICANN'S COMMITMENTS AND CORE VALUES, THROUGH THE ENABLING OF LAWFUL ACCESS FOR LEGITIMATE THIRD- PARTY INTERESTS, SUCH AS LAW ENFORCEMENT, INTELLECTUAL PROPERTY RIGHTS HOLDERS AND CYBERSECURITY PROFESSIONALS, TO DATA ELEMENTS COLLECTED FOR THE OTHER PURPOSES IDENTIFIED HEREIN. As described in the Bylaws, ICANN's mission is to "ensure" the security, stability and resiliency of the DNS, not merely "maintain" it. This underscores that ICANN's policies in this regard are proactive. The scope of ICANN's Mission was carefully clarified and described in its Bylaws, and this is what should guide the interpretation of this purpose. For clarity sake, reference to the definition in the Bylaws is important. Furthermore, in order to ensure that there are examples of what may constitute legitimate third party interests, INTA believes strongly that those of law enforcement, intellectual property owners, and cybersecurity professionals are recognized as stakeholders in this area. This has been historically true at ICANN and should remain so, and is consistent with ICANN's obligation to uphold the broader public interest, in furtherance of fulfilling ICANN's Mission, under its Bylaws.	Lori Schulman Senior Director, Internet Policy; International Trademark Association (INTA)	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
10.	ENSURING THE SECURITY, STABILITY AND RESILIENCY OF THE DOMAIN NAME SYSTEM IN ACCORDANCE WITH ICANN'S MISSION THROUGH THE ENABLING OF LAWFUL ACCESS FOR LEGITIMATE THIRD-PARTY INTERESTS TO DATA ELEMENTS COLLECTED FOR THE OTHER PURPOSES IDENTIFIED HEREIN. ICANN's mission is to ensure the stable and secure operation of the Internet's unique identifier systems, which is a stronger imperative than "maintaining," and requires that ICANN ensure access to domain registration data for law enforcement, cybersecurity, consumer protection, and intellectual property protection. Some parties contributing to this EPDP have argued that ICANN's mission does not extend to matters concerning "the use of such domain names," and that therefore ensuring third-party access is beyond ICANN's remit. We do not find that argument persuasive in this context, and we do not ask for ICANN's active involvement in any such investigation, dispute, or litigation. Rather, we submit that ICANN's role should remain as has always been, as supported by its bylaws: to ensure that mechanisms exist which enable domain registration data to be made available for those who need it for legitimate purposes. "	Brian King; MarkMonitor, Inc., a Clarivate Analytics company	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
11.	ENSURING THE SECURITY, STABILITY, AND RESILIENCY OF THE DOMAIN NAME SYSTEM IN ACCORDANCE WITH ICANN'S MISSION, COMMITMENTS, AND CORE VALUES THROUGH THE ENABLING OF LAWFUL ACCESS TO DATA ELEMENTS FOR LEGITIMATE THIRD-PARTY INTERESTS OF LAW ENFORCEMENT, CYBERSECURITY, CONSUMER PROTECTION, INTELLECTUAL PROPERTY RIGHTS PROTECTION, COMBATTING DOMAIN NAME SYSTEM ABUSE, COLLECTED AND FOR THE OTHER PURPOSES IDENTIFIED HEREIN For the sake of clarity and notice, this purpose should specifically identify as permissible the collection and processing of data for the long acknowledged legitimate interests of law enforcement, cybersecurity, consumer protection, and combatting intellectual property infringement and domain name abuse, including for investigations and enforcement actions related to those interests. Providing this added is consistent with Article 13(1) of the GDPR and the April 2018 letter from the Article 29 Data Protection Working Party to Göran Marby, both of which indicate that notice should be provided regarding the purposes for processing data. See GDPR, art. 13(1), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN; Letter from ARTICLE 29 Data Protection Working Party to Göran Marby, President and CEO, ICANN, April 11, 2018, https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf.	Neil Fried; The Motion Picture Association of America	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

12.	Ensuring the security, stability, and resiliency of the domain name system in accordance with ICANN's mission through the enabling of lawful access for legitimate third-party interests such as cybersecurity investigations, intellectual property enforcement, consumer protection, DNS abuse mitigation, and law enforcement, to data elements collected for the other purposes identified herein." ICANN's mission is to ensure the stable and secure operation of the Internet's unique identifier systems, and this requires that ICANN ensure access to domain registration data for criminal law enforcement, cybersecurity investigations, consumer protection, and intellectual property protection. (Note that we do not ask for ICANN's active involvement in any such investigation, dispute, or litigation. Rather, we submit that ICANN's role has always been to ensure that the mechanisms exist which enable domain registration data to be made available for those who need it for legitimate purposes.) Microsoft and others are empowered by law in many jurisdictions to protect themselves, and their customers, through the filing of civil cases stemming from cybersecurity investigations. US federal legislation (e.g. the Lanham Act and the Computer Fraud and Abuse Act) has introduced civil causes of actions or claims for private litigants to bring actions. In UK Common Law, the concept of trespass to chattels has been similarly applied. Certain causes of action are specifically tailored for civil cybersecurity cases. In the Rustock investigations, Lanham Act civil seizure warrants were required to take malware servers offline. Brand protection is inextricably linked to consumer protection and the possible harm to consumer is exacerbated by the availability of pirate and counterfeit goods online and the ease with which they can be obtained /purchased. When brand abuse is also used as a mechanism for cybercrime, the consumer risk is increased. Our ability to protect consumers by using these existing statutes and adapt them into the cybersecurity realm has been extremely successful. The original wording does not accurately reflect this. Key to these statutes is the concept of notice. For us to bring any type of case, we must show the court that there has been a legitimate attempt to provide Notice of Process. If we can't provide this to the court, the case may be dismissed. We will discuss some implications of this elsewhere where publication of email addresses is discussed, but it should be apparent that many types of civil actions and dispute resolutions depend on identifying and contacting registrants. Therefore, we believe that more specificity is required to clarify that legitimate third-party interests play an important role maintaining the security, stability and resiliency of the domain	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 **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	name system, a role which has been impaired since the registrars and registries began making registration data unavailable to these legitimate third parties. In this regard, we are encouraged by the recent opinion of the ICANN Security and Stability Advisory Committee. Microsoft has relied on registration data for many types of investigations, both reactive (identifying bad actors after known attacks) and proactive (using registration data to prevent future attacks by these same actors), and our work provides important support to law enforcement. A few Microsoft investigative efforts using registration data are documented here: • Anti-Phishing Working Group's study • Cybersecurity Tech Accord study Finally, in cases where Microsoft trademarks and intellectual property have been abused, and related cybersecurity issues have not been identified, it is often the case that a letter or email from Microsoft informing a registrant of the problem is enough to resolve the issue. This desirable outcome benefits all parties and depends on access to accurate data.		
13.	The U.S. proposes Purpose 2 be edited to include a reference to ICANN's "commitments and core values." The U.S. believes this purpose is consistent with the EPDP Charter and European Data Protection Board guidance. Purpose 2 is narrowly tailored to the purpose and processing activities of ICANN and does not address the specific interests and purposes of third parties, subjects to be addressed at a later date. The U.S. strongly believes that for ICANN to meet its fundamental purpose of maintaining the security, stability, and resiliency of the DNS there are legitimate interests internal and external to ICANN necessary for ICANN to achieve this. To reflect this, the U.S. proposes Purpose 2 be edited to include a reference to ICANN's "commitments and core values." With this edit, Purpose 2 becomes the baseline necessary for ICANN and the community to develop and implement an access model at a later date that includes legitimate third party interests such as law enforcement, cybersecurity, and intellectual property enforcement.	Ashley Heineman; NTIA	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
14.	The GAC is still considering possible edits to clarify this purpose. The GAC supports the purpose of ICANN to maintain the security, stability and resiliency of the Domain Name System in accordance with ICANN's mission, but would also reference ICANN's commitments and core values as set forth in the Bylaws. The GAC recognizes that the EPDP spent considerable time trying to take into account the opinion received from the EDPB on the need for ICANN distinguish between its own processing activities and the purposes pursued by other stakeholders. However, the GAC is still considering the wording of this purpose and how to best emphasize that it focuses on ICANN purposes only. Making such a distinction should not exclude processing for legitimate purposes pursued by other stakeholders; as stated in the GAC's recent comments on the Unified Access Model, ""the GAC considers the development and implementation of such a unified and reliable access model to be of the utmost importance"" and has called on ICANN and the community ""to develop a comprehensive, harmonized, reliable, and scalable model that allows access to non public WHOIS data for authenticated users with a legitimate purpose in a manner that is consistent with the EU's General Data Protection Regulation (GDPR)."" The GAC is still considering possible edits to clarify this purpose. The GAC believes that it would then be useful to consider this item as part of the scope of legal guidance that the EPDP would be seeking.	Fabien Betremieux; GAC	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
Significant change required: changing intent and wording			

15.	ENSURING THE SECURITY, STABILITY, AND RESILIENCY OF THE DOMAIN NAME SYSTEM IN ACCORDANCE WITH ICANN'S MISSION, COMMITMENTS AND CORE VALUES THROUGH THE ENABLING OF LAWFUL ACCESS FOR LEGITIMATE THIRD-PARTY INTERESTS OF LAW ENFORCEMENT, CYBERSECURITY, COMBATTING DOMAIN NAME SYSTEM ABUSE, CONSUMER PROTECTION AND INTELLECTUAL PROPERTY RIGHTS PROTECTION TO DATA ELEMENTS COLLECTED FOR THE OTHER PURPOSES IDENTIFIED HEREIN Although we do not object in principle to the Purpose 2 statement, the IPC hopes to clarify that the purpose includes as a component the recognition of protection of intellectual property rights (as the universally, legally defined recognized rights of: trademark, copyright and patent) and by extension consumer protection and consumer trust within the meaning of "maintaining the security, stability, and resiliency of the Domain Name System in accordance with ICANN's Mission" particularly given that part of ICANN's Mission includes: "resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names, but including where such policies take into account use of the domain names); … reservation of registered names in a TLD that may not be registered initially or that may not be renewed due to reasons reasonably related to (i) avoidance of confusion among or misleading of users, (ii) intellectual property…." Accordingly, assuming this is the case, we hope to confirm that "lawful access for legitimate third-party interests" as used in this purpose statement includes the implicit recognition that intellectual property enforcement related investigations and actual enforcement measures conducted by intellectual property owners and their agents would therefore be considered "legitimate third-party interests" and thus permitted "lawful access" to the requisite data elements collected for other purposes as outlined elsewhere in the Initial Report. Note that while we suggest the addition of "Commitments and Core Values" to the purpose statement, these additions may not be necessary if the above can otherwise be clarified and confirmed. In addition, Article 13(1) of the GDPR states Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: . . . (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;	Brian King; IPC	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;" (emphasis added) The current list of purposes would benefit by greater specificity as embodied in the proposed new purpose. ICANN's purposes with respect to WHOIS data and registry directory services include, according to ICANN'S Bylaws "whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust, security, stability and resiliency, malicious abuse issues, sovereignty concerns and rights protection." (ICANN Bylaws Section 4.6). Purpose #2 from the Initial Report only addresses "security, stability and resiliency" and does not address the other ICANN purposes and concerns as articulated in Section 4.6 of the Bylaws. Article 13(1) of the GDPR requires that at the time personal data are collected, data subjects be given information about both the purposes for the processing and legal basis for the processing AND the legitimate interest pursed by the controller or by a third party. The proposed new purpose seeks to address both of these requirements by enumerating more specific purposes as well as identifying the legitimate interests of ICANN (as a joint controller) and as pursued by third parties that may seek access to the personal data. In its letter of 11 April 2018, to Goran Marby, the Article 29 Data Protection Working Party stated that "purposes specified by the controller must be detailed enough to determine what kind of processing is and is not included . . . ." The letter also stated that the WP29 "stresses the importance of explicitly defining legitimate purposes in a way which comports with the requirements of the GDPR." The new proposed Purpose seeks to do just that.		
Purpose should be deleted			
16.	First, this is not needed, as legitimate and lawful access is not prohibited by GDPR and other privacy laws, nor ICANN policies, etc. Second, the EDPB already warned ICANN against conflating third-party interests with its own, see https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf, and that is exactly what this Purpose #2 does--read this quote: "In effect, Purpose 2 says that ICANN is ordering registries and registrars to collect data from domain name registrants in order to disclose that data to third parties. That is just wrong. The whole principle of collecting and processing data for the sake of unspecified third parties and unspecified uses contravenes basic privacy and data protection norms ... Coming up with terms and conditions of access is step 2 in the EPDP process. We ... need to resist the notion that providing third party access is one of the purposes of Whois, as that points us backwards to the pre-GDPR system of open public Whois."--source: https://www.internetgovernance.org/2018/11/25/whois-privacy-reform-hits-its-first-milestone/	John Poole; Domain Name Registrant	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
17.	3rd party access to registration data is not part of ICANN's mission.	Michele Neylon; Blacknight Internet Solutions Ltd	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
18.	GoDaddy concurs with the RrSG position that ICANN's mission does not explicitly include enabling third party access to registration data. Third party access may be found to be a legitimate secondary purpose. GoDaddy reminds ICANN that it received guidance from the EDPB on this topic in a letter dated 5 JUL 2018, which cautioned against conflating "its own purposes with the interests of third parties." https://edpb.europa.eu/sites/edpb/files/files/news/icann_letter_en.pdf	Sara Bockey; GoDaddy	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
19.	Lawful access for legitimate, GDPR -compliant third party interests has nothing to do with maintaining the SECURITY, STABILITY, AND RESILIENCY OF THE DOMAIN NAME SYSTEM. This is essentially an attempt to fit third party purposes into an alleged ICANN purpose which does not exist in this form. ICANNs interests and the interests of third parties should be kept separate.	Volker Greimann; Key-Systems GmbH	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
20.	At the time of the preparation of the report the question of access to data has neither been fully discussed nor has the lawfulness of responses to disclosure requests been assessed exhaustively. It is difficult to assess the lawfulness of such purpose in the absence of knowing the parameters for disclosure, should any such recommendations be made. Additionally, even without the definition of a related purpose, information may be provided to respond to lawful disclosure requests, such as requests from competent law enforcement authorities. As a consequence, no definition of a purpose needs to be defined for these cases. It is questionable whether data may lawfully be kept to enable those holding the data to disclose it to third party beyond such cases. Therefore, a purpose relating to disclosure of data to third parties may be unlawful and it should only be included in the final report conditional to affirmative confirmation by either a competent authority or legal counsel.	• Lars Steffen; eco – Association of the Internet Industry • Wolf-Ulrich Knoben; ISPCP Constituency	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
21.	ICANN's mission does not explicitly include enabling third-party access to registration data. Third-party access may be found to be a legitimate secondary purpose. Additionally, the EDPB has already cautioned ICANN against conflating its purposes with that of third-party interests. https://edpb.europa.eu/sites/edpb/files/files/news/icann_letter_en.pdf	Zoe Bonython; RrSG	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
22.	Enabling third-party access to data elements is not within ICANN's mission. Further, "enabling" third-party access is not a legitimate purpose for collecting data. It is instead is instead a right where under certain circumstances where and when allowed by law.	Domain.com, LLC & affiliates	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
23.	We are sympathetic to the needs of law enforcement, and understand that WHOIS is an important (but far from the only available) tool to investigate wrongdoing. However, we wish to be clear that third party access to registration data is not part of ICANN's mission. Moreover, this overbroad application of what 'security, stability, and resiliency' means, as stated in this purpose - a slippery slope that could lead to the inclusion of just about anything being considered in-scope. Further, we draw attention to Article 6(1)(f) where release of data for legitimate interests is more rightly considered a legal obligation for data controllers. This view is consistent with that of the Internet infrastructure community on this issues and many others which consider the clear and blurred lines around the control and release of data."	Monica Sanders; i2Coalition	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
24.	The core of this recommendation is a suggestion that Contracted Parties collect registration data for the purpose of disclosure. Contracted Parties do not and it is submitted that this is not a shared purpose of ICANN and Contracted Parties. Furthermore, the text of the recommendation simply mirrors that of article 6(1)f of the GDPR. This amounts to a legal obligation on all data controllers i.e. the controller shall consider a disclosure request regarding the data processed by them; insofar as the disclosing controller is satisfied, as per under article 6(1)f, that the requesting 3rd party holds a legitimate purpose for such disclosure and such a disclosure is weighed appropriately against the data subject's rights. This is entirely separate from a 'purpose', and in fact is applicable regardless of purpose. it is our belief that Purpose 2, at most is mere restatement of a legal basis for processing, and not a valid "purpose" for either ICANN or the Contracted Parties. It is submitted that the inclusion of Purpose 2 is therefore a fundamental misunderstanding and misinterpretation of Art. 6(1)f, and absent affirmative confirmation as to the legality of this purpose, it should be deleted in its entirety, as it does not add anything to the data processing review.	Wim Degezelle; RySG	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
25.	Purpose 2 is not required in order to create and operate a domain name. It does not justify any real purpose for collecting and processing data about the registrant. It is related to disclosure of the data that has already been collected. Under the GDPR, this is not considered a legitimate purpose. Lawful access for legitimate third party interests should be handled under the policy for "access" or disclosure. It does not need to be declared a purpose, thus this should be deleted.	A. Mark Massey; Domain Name Rights Coalition	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
26.	"MAINTAINING THE SECURITY, STABILITY, AND RESILIENCY OF THE DOMAIN NAME SYSTEM IN ACCORDANCE WITH ICANN'S MISSION THROUGH THE ENABLING OF the necessary degree of transparency for all users of necessary data elements concerning personal Domain Names, relatively more information concerning commercial Domain Names, LAWFUL ACCESS FOR different classes of LEGITIMATE THIRD-PARTY INTERESTS qualifying for different levels of privileges TO pertinent additional / redacted DATA ELEMENTS COLLECTED FOR THE OTHER PURPOSES IDENTIFIED HEREIN" In this section, the Purpose is further clarified by the proposed text which emphasizes the preservation of Registrant Data by the earlier whois process which made data elements largely available for all users. Whois, by any other name, with fewer data elements where necessary, needs to exist for the benefit of all users; Some data fields may be designated as sensitive and redacted, but Lawful Access by Law and Order Agencies for part or all of the redacted data of all or requisitioned domain name registrations is to be defined; Same or lesser level of lawful access by Third Parties to be separately defined. The rationale for distinction between commercial and non-commercial Domain Names is further expanded in response to Question#1 and #87.	Sivasubramanian Muthusamy; Internet Society India Chennai	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
27.	Purpose 2 is vague and does not specify what is involved in "maintaining the security, stability, and resiliency of the domain name system in accordance with ICANN's mission". The NCSG has held the position from the start of the discussion on this purpose that what is interpreted to be within the scope of ICANN's mission in relation to SSR needs to be identified in order for this purpose to hold any true meaning. When the topic had been raised, there was significant disagreement within the EPDP on what the interpretation of the bylaws relevant to SSR includes, thus leading to disagreement on what the scope of this purpose should include. The current vague wording of this purpose seems to intentionally attempt to bypass this discussion (one on which there is likely to be no consensus), and leave the interpretation of the scope of ICANN's SSR duties to the implementation of this policy recommendation. The NCSG does not find this to be appropriate. Note that the need to be specific in identifying the scope of ICANN's mission when defining purposes was clearly communicated to the GNSO Next-Generation gTLD RDS to Replace WHOIS PDP WG by EU data protection experts in May 2017, when they said: "Purpose has to be defined in advance of the data processing. Purposes have to have a legitimate aim and the processing has to be necessary and proportionate to the legitimate aim pursued. Translating this to ICANN means the working group would want to take a look into ICANN role and its mission statement and separate out the legitimate data processing purposes, and determine which data are necessary for which purpose." https://community.icann.org/download/attachments/64078601/ICANN58-DataProtectionExpert-Responses-7April2017-plus-Intro.pdf	Ayden Férdeline; NCSG	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
28.	"Disclosure of personal information to the third party is not an ICANN purpose - ICANN does not process domain name registrants data to disclose it later. The only clause in which disclosure might be interpreted as in ICANN's mission and scope is elaborated in section 1.1 and G1 and G2. It reads as: ""ICANN's scope is to coordinate the development and implementation of policies: - [...] with respect to gTLD registrars and registries, policies in the areas described in Annex G-1 and G-2 ;[....][for example] maintenance of and access to accurate and up-to-date information concerning registered names and name server."" Nowhere in the bylaws ICANN directly is in charge of providing access nor facilitating access to registrants data. It is only in charge of developing consensus based, uniform and global policies and implementing them. Moreover, security stability and resiliency can only be interpreted in technical terms and in line with ICANN's narrow and technical mission. It cannot move beyond the narrow and technical definition and include non-technical interest such as protection of trademark."	Farzaneh Badii; Internet Governance Project	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
Not designated			

#	Comment	Contributor	EPDP Response / Action Taken
29.	No selection made and no additional comments submitted	• Steve Gobin; Corporate domain name management • Brian Beckham; Head, Internet Dispute Resolution Section, World Intellectual Property Organization • Ivett Paulovics; MFSD Srl URS Provider • Ashley Roberts; Valideus • Renee Fossen; Forum - URS and UDRP Provider • Stephanie Perrin	**EPDP Response:** none **Action Taken:** none **COMPLETED**