Additional comments for RECOMMENDATION 1 and additional purposes

#	Comment	Contributor	EPDP Response / Action Taken
Additional comments for recommendation #1 & additional purposes for processing registration data			
Additional comments for recommendation #1			
1.	No additional comments, except to note that this exercise (catalog of purposes) was part of RDS PDP. Note duplication of effort and compare/contrast outcomes	• 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.]
2.	The ALAC sees that activities like the WHOIS Accuracy Reporting System (ARS) and the use of the WHOIS registration data by the office of the chief technology officer (OCTO) for training and outreach are not fulfilled through the aforementioned purposes. In addition ICANN needs to continuously advance its operational and administrative role in relation to the stability, reliability, and security of the Internet and to do so research is needed. Therefore ALAC recommends adding additional purposes that can address the aforementioned needs.	Evin Erdoğdu; ALAC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
3.	The EPDP Team must revisit each of the workbooks and conduct a proper and thorough analysis of all processing activities and each data element identified as being required to fulfill every purpose. Because of the extensive interrelationship among issues and data elements, it will be important for the EPDP Team to conduct consistency reviews to ensure that any changes arising from the public comment period are applied consistently. In addition, the RySG continues to advocate for a data audit and mapping approach to determining purposes and the roles and responsibilities of involved parties. This important analysis is still absent.	Wim Degezelle ; RySG	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
4.	The GDPR defines data controllers and data processors in Art. 4 as: (7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal	Steve DelBianco; BC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:**

#	Comment	Contributor	EPDP Response / Action Taken
	data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; (8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; Under the Registrar Accreditation Agreement between registrars and ICANN, ICANN determines the purposes and means of the processing of personal data, in some instances for the purpose of WHOIS, by mandating data collection, transfer, storage, and display through minimum contractual terms that registrars maintain in contracts with Registered Name Holders (the data subjects). While there may be other terms in these contracts with Registered Name Holders aimed at allowing registrars to maintain a customer relationship (process payments in exchange for domain names), where ICANN determines the purposes and means of the processing of personal data for, things like WHOIS or escrow, ICANN is clearly a controller and the registrar a processor for the control. This does not exclude registrars as controllers of the same data where that data is collected for the registrar's purposes (e.g., maintaining a customer relationship with the Registered Name Holders). Indeed, the eco (Association of the Internet Industry) GDPR Domain Industry Playbook V. 1.0 (https://www.eco.de/wp-content/uploads/2018/02/eco-domain-industry-playbook-v1.0-en.pdf) at page 61 notes that: "The main purpose of any data processing operation in connection with domain registration is the provision of the services associated with domain registration within the scope of the contractual relation. However, the activity of the enterprise participating in domain registration cannot be reduced to this singular purpose. Rather, the registration of domains is a service, which - jointly with the services of other companies - guarantees the overall functionality of the Internet (namely conveying content available in the World Wide Web). The special roles of registrar and registry within this technical ecosystem is also reflected e.g. in the fact that they are subject to certain duties as operators of critical infrastructures. The activity of registry and registrar - in this light - also serves other purposes beyond the mere domain registration for customers, in particular also with regard to the functionality of the technical infrastructure as such. Registrar and registry therefore also have to a certain extent a regulatory function, which for example may include participation in the prosecution of legal infringements committed under usage of this ecosystem. Against this background we would consider processing of data for the purpose of maintaining security measures or technical analysis (also operated by third party providers) as likely (depending on the individual case) being justified under Art. 6 (1) lit. f) GDPR." (emphasis added)		[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
5.	We are concerned that the list of purposes is neither sufficiently complete, nor sufficiently detailed. We have attempted to address these concerns by suggesting edits to some of the recommended 7 purposes as well as suggesting additional purposes below.	Brian King; IPC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
6.	Your Google Form prevents me from entering additional comments, this is the message I get: "Your response is too large. Try shortening some answers."	John Poole; Domain Name Registrant	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
Proposed additional purposes & rationale			
7.	There are no additional purposes we would like to suggest. Our comment relates to the purposes as defined in this document. We regard it as necessary to test the language of the purposes against the overall package of recommendations that the EPDP will come up with to ensure that all recommended processing activities are adequately reflected in a purpose that passes the test of GDPR requirements. Also, it shall be noted and made explicitly clear in the final report that the purposes and related processing activities only cover those areas that shall be governed by ICANN's policies and thus be made part of ICANN's contracts and be enforced accordingly. However, there may be additional purposes pursued by contracted parties and ICANN that are out of scope of this EPDP or ICANN's governance. Nothing in the EPDP's findings shall prevent the contracted parties or ICANN from conducting additional processing activities, which certainly must be compliant with applicable laws.	• Lars Steffen; eco – Association of the Internet Industry • Wolf-Ulrich Knoben; ISPCP Constituency	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
8.	1. A new purpose to address the needs and benefits provided by DNS security and stability research conducted through publication of reports on threats to the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS, and on the accuracy of WHOIS. 2. A new purpose to enable ICANN to conduct operations, facilitate activities, and implement consensus policies (adopted in accordance with the ICANN Bylaws) consistent with its mission of furthering the operational stability, reliability, global interoperability, resilience and openness of the DNS.	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
	1. Research is a legitimate basis for processing, per GDPR Article 6(1)f, with specific safeguards defined in Article 89. It is also squarely within ICANN's mission and mandate, as the requirement for research derives from Section 1.2a (Commitments) of the ICANN bylaws: (i) Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet; (ii) Maintain the capacity and ability to coordinate the DNS at the overall level and work for the maintenance of a single, interoperable Internet; This purpose exists to ensure that ICANN may continue to use registration data in support of its mission, whilst maintaining the privacy of data subjects through appropriate safeguards such as pseudonymisation. In addition, this purpose enables ICANN to continue to operate its Accuracy Reporting System (ARS), which publishes periodic reports on accuracy, using full WHOIS contact fields. The ARS is an important program approved by the ICANN Board in response to the recommendations from the first WHOIS Review Team. 2. Prior to May 25, and consistent with its mission and mandate under the Bylaws, ICANN used full WHOIS data as part of operational security-related activities via the Office of the CTO -- this included collaborating with public/private sector investigators, training law enforcement agencies in techniques for mitigating cybersecurity threats (such as CONFICKER), and working with a compliance related complaint. ICANN also used WHOIS as it implemented consensus policies involving the use of WHOIS data fields (for example, transfer policy processes or Thick WHOIS). It is important that ICANN retain the ability to provide these services in order to fulfill its role in safeguarding the DNS.		
9.	1. Mitigation of Domain Name Abuse. 2. To improve consumer trust in the Domain Name System The rationale is the same as provided in answer to the question on differentiation between legal and natural persons	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
10.	1) ARS (Accuracy Reporting System) 2) The Office of the Chief Technology Officer (OCTO) research and threats analysis/prevention Both of these are topics which are just starting to be discussed in the EPDP, but this will serve as an introduction: ARS: The ARS was instituted in response to a recommendation of the WHOIS Review Team related to the accuracy of registration contact data. Studies had shown that there was a significant issue with data accuracy. Every 6 months (pre the Temp Spec) the ARS samples randomly selected gTLD registrations and tests the contact information for accuracy using a number of criteria. Those failing accuracy tests are passed to Contractual Compliance. In recent cycles, about 40% of all records samples have at least one contact entry that fails validation. Under the 2013 RAA, new registrations, those transferred to a new registrar, or those where there is a voluntary change of contact information must pass specific validation and verification test, but the vast majority of registrations have not been subject to such tests (an estimated 180,000,000). Under GDPR data must be accurate for the purpose under which it is processed. Purpose 2 and 6 both pass contact data to parties who have an expectation of accuracy and there is no way to understand whether this is being done without accuracy monitoring. OCTO Research: ICANN is responsible for the DNS which includes fully understanding all aspects of it. Activities may include addressing DNS threats and potentially developing an evolution of it or a dissimilar replacement. To do that it needs to have access to all aspects of the DNS. If ICANN were a typical controller, it would have access to all of the data to begin with, and this would be covered under Recital 50 (secondary processing provisions), but since ICANN is not in possession of the data, we must make sure that it has suitable access.	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
11.	A. A new purpose to address the needs and benefits provided by DNS security and stability research conducted through publication of reports on threats to the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS, and on the accuracy of WHOIS. B. A new purpose to enable ICANN to conduct operations, facilitation activities, and implement consensus policies (adopted in accordance with the ICANN Bylaws) consistent with its mission of furthering the operational stability, reliability, global interoperability, resilience and openness of the DNS. A. Research is a legitimate basis for processing per GDPR Article 6(1)f, with specific safeguards defined in Article 89. It is also squarely within ICANN's mission and mandate, as the requirement for research derives from Section 1.2a (Commitments) of the ICANN bylaws: (i) Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet; (ii) Maintain the capacity and ability to coordinate the DNS at the overall level and work for the maintenance of a single, interoperable Internet; This purpose exists to ensure that ICANN may continue to use registration data in support of its mission, while maintaining data subject privacy through appropriate safeguards such as pseudonymisation. In addition, this purpose enables ICANN to continue to operate its Accuracy Reporting System (ARS), which publishes periodic reports on accuracy, using full WHOIS contact fields. The ARS is an important program approved by the ICANN Board in response to the recommendations from the 1st WHOIS Review Team. B. Prior to the adoption of May 25th, and consistent with its mission and mandate under the Bylaws, ICANN used full WHOIS data as part of op/sec related activities of the Office of the CTO to collaborate with public/private sector investigators, to train law enforcement agencies in techniques for mitigating cybersecurity threats such as CONFLICKER, or to work with a compliance related complaint. It also used WHOIS as it implemented consensus policies that involve the use of WHOIS data fields (such as in transfer policy processes or Thick WHOIS). It is important that ICANN continue to provide these services to enhance the DNS.	• Brian King; MarkMonitor, Inc., a Clarivate Analytics company • 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.]
12.	Additional Purpose 1: Promoting the transparency, accountability, and trust necessary to ensure a safe, secure, and supportive environment online for communication, commerce, innovation, and creativity—such as by combating illicit online conduct and ensuring public safety, consumer protection, law enforcement, dispute resolution, protection of intellectual property, prevention of domain name abuse, and enforcement of rights—as well as to provide access to third-parties and law enforcement authorities for such purposes.	Neil Fried; The Motion Picture Association of America	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:**

#	Comment	Contributor	EPDP Response / Action Taken
	Additional Purpose 2: To facilitate analysis regarding misuse of domain names in deciding whether to create additional gTLDs, as well as to create or amend policies regarding the misuse of gTLDs. Rationale for Additional Purpose 1: Since before the dawn of the commercial internet, access to WHOIS data has been a cornerstone of the transparency, accountability, and trust necessary to ensure a safe, secure, and supportive online environment for communication, commerce, innovation, and creativity. As ICANN itself notes, the Internet Engineering Task Force began publishing a protocol for a directory service in 1982 that listed the contact information of anyone transmitting data across the ARPANET. See History of WHOIS, ICANN WHOIS, https://whois.icann.org/en/history-whois (last visited Dec. 11, 2018). "As the Internet grew," that system "began to serve the needs of different stakeholders such as domain name registrants, law enforcement agents, intellectual property and trademark owners, businesses and individual users." Id. Access to WHOIS information is critical to creating the transparency, accountability, and trust that is fundamental to the multistakeholder model of internet governance, and that all internet users need to be comfortable interacting online. Without reliable and timely access to WHOIS data, individuals and businesses will have difficulty determining—when necessary—whom they are engaging with online, whether to verify the identity of the entity; to find a contact for purposes of conveying information, preferences, questions, and concerns; or to seek redress for mistakes and harms. Moreover, law enforcement and other entities will have a harder time investigating, preventing, and mitigating illicit behavior online. Promoting a safe and secure online environment—as well as the collection, processing, and sharing of registration data to accomplish that purpose—is perfectly consistent with the European Union's General Data Protection Regulation. WHOIS data had been publicly available prior to the May 2018 adoption of the Temporary Specification, and domain name registrants have long been on notice that they must provide certain information that will be publicly disclosed, including for matters of public safety, consumer protection, law enforcement, dispute resolution, protection of intellectual property, and enforcement of rights—reducing expectations of privacy. Moreover, the GDPR acknowledges that a variety of interests can warrant collection and disclosure, such as public safety, law enforcement and investigation, enforcement of rights or a contract, fulfillment of a legal obligation, cybersecurity, and preventing fraud. See GDPR, arts. 2(2)(d), 5(1)(b), 6, 23, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. See also ICANN, GOVERNMENTAL ADVISORY COMMITTEE, Communiqué—San Juan, Puerto Rico (Mar. 15, 2018) (stating that the GDPR allows for access to data for legitimate purposes), https://gac.icann.org/advice/communiques/20180315_icann61%20gac%20communique_finall.pdf. Promoting a safe and secure online environment is also consistent with ICANN's Bylaws. Section		[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	1.1, for example, provides that ICANN's mission includes coordinating the development and implementation of policies with respect to gTLD registrars and registries in the areas described by annexes G-1 and G-2. See ICANN Bylaws, Sec. 1.1(i)(a), https://www.icann.org/resources/pages/governance/bylaws-en/. Annexes G-1 and G2, in turn, include "issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, security and/or stability of the Internet"; "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)"; and "reservation of registered names in a TLD … that may not be renewed due to reasons reasonably related to … intellectual property" (emphasis added). Similarly, Section 4.6(e)(ii) provides that ICANN will periodically "assess the effectiveness of the then current gTLD registry directory service and whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust and safeguarding registrant data" (emphasis added). Thus, it is in ICANN's remit to ensure WHOIS data remains accessible to promote the safety and the security of the internet itself, not just the safety and security of the domain name system, as well as to protect intellectual property. To be clear, these purposes have nothing to do with curbing or discriminating against particular internet expression, but rather are related to combatting illegal conduct, including unauthorized dissemination of copyrighted material. Detailing these purposes 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. Rationale for Additional Purpose 2: ICANN's mission includes adopting policies regarding the creation of additional gTLDs. Misuse of gTLDs's is relevant in determining whether to create such additional gTLDs, and whether to expand existing policies or create new ones regarding misuse. Analysis of misuse will require collection and processing of data as part of the WHOIS system, including sharing with third parties.		
13.	As discussed earlier, establishing the provenance and ownership history of a domain name is critical. Thus, "transfer" and "recovery" should be explicitly added within the aforementioned text (need not be a separate purpose, but can be appended to existing points). Research and Journalism should also be explicitly permitted uses. 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	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
	electricity which are fungible and where no historical record is needed). If an overly-restrictive interpretation of GDRP and privacy interests is made, that erasure of historical ownership records will have a severe impact on the ability of a registrant to demonstrate to others that they were a past registrant (for domain recovery purposes), and also to demonstrate to others that they're a legitimate current registrant (as opposed to a domain name thief who happens to have their data in the current WHOIS). It is imperative that these historical records be maintained, for the benefit of the current registrant, past registrants (through domain recovery), and future registrants (who can demonstrate proper ownership, by referencing an audit-trail of the historical ownership). Furthermore, research and journalism are important in a free society, to help uncover matters of public interest. ICANN should not "accredit" journalists, either, because citizen journalism is a part of journalism too.		
14.	COA recommends additional purposes for processing registration data concerning: (i) research, both research conducted by ICANN org and by third parties, and (ii) implementation of consensus policies by ICANN org and the undertaking of validation, facilitation and compliance activities consistent with its mission. Potential wording to capture such additional purposes: A. Enable research undertaken by ICANN and third parties concerning the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and threats to these criteria and values, and on the accuracy of WHOIS data. B. Enable the operations of ICANN consistent with its mission of furthering the operational stability, reliability, global interoperability, resilience and openness of the DNS via implementation of consensus policies, validation and compliance with policies and contracts, and facilitation activities. Article 5(1)(b) and (e) of the GDPR recognize research as legitimate and not "incompatible with the initial purposes." Given how important research-- undertaken both by ICANN org itself and by third parties, such as cybersecurity researchers--is to the core mission of ICANN of ensuring and furthering the stability, reliability and resiliency of the domain name system, this research purpose should be set forth explicitly. In addition, adding this explicit purpose furthers compliance with Article 5(1)(a) of the GDPR that personal data is processed "fairly and in a transparent manner in relation to the data subject" because setting forth this purpose clearly and explicitly enhances transparency. Finally, adding a specific reference to the accuracy of WHOIS data fulfills the accuracy requirement of the GDPR as set forth in Article 5(1)(d). This is the rationale that supports new Purpose A suggested above. In order to implement, fulfill and enforce both consensus policies and contractual obligations, as well as pursue operations critical to ICANN's core mission, ICANN will need access to and be able	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
	to process personal data of registered name holders in its role as a controller or joint controller. Setting forth this purpose explicitly furthers the accountability principle set forth in Article 5(2) of the GDPR. In addition, it adds greater clarity to the lawful processing activities of ICANN as set forth in Article 6 of the GDPR. Among other functions, this purpose permits ICANN to continue to operate its Accuracy Reporting System ("ARS") concerning WHOIS data. This is the rationale that supports new Purpose B suggested above.		
15.	Cybersecurity and anti-fraud purposes, such as those noted in Recitals 47 and 49 of the GDPR. As Whois serves as a public directory for the public databases central to the domain name system, there are many purposes for processing such data. The EPDP draft processing purposes articulate such purposes and their legal bases, including the GDPR's Art. 6.1(f) lawful purpose for the legitimate interest of the data controller or a third party. A GDPR legitimate interest analysis requires an assessment as to whether an interest is legitimate to begin with, and, if so, whether such an interest is overridden by the interests or fundamental rights and freedoms of data subjects. The AG IS recommends that the EPDP holistically consider all of the important interests and rights at stake with regard to cybersecurity, the security and stability of the DNS, and overall data protection risks posed by maliciously registered or hijacked domain name registrations. The EPDP should consider and articulate a true assessment of interests in rights considering the victims of DNS abuse, the security and stability of the DNS, the many GDPR recitals articulating overriding interests, and the GDPR's risk-based approach to appropriate safeguards for personal data. Whois data is used for cybersecurity purposes, and the processing of personal data for cybersecurity purposes is recognized in the GDPR. 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	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
16.	Echoing the explanation found on page 89 of the Initial Report, the RySG urges the EPDP team to ensure clarification as to the definition of 'ICANN purposes' as it applies to the report, as it remains unclear, and should not be relegated to a footnote. The RySG urges further clarification that the purposes as stated, are notwithstanding any established purposes of either ICANN or individual registries or registrars, who may design and establish their own additional purposes, in which they would be acting as sole controller.	Wim Degezelle ; RySG	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
17.	In support of cybersecurity research directly in line with ICANN's Mission to support the stable and secure operation of DNS. GDPR Article 6(1)f supports research as a legitimate purpose. It needs to be highlighted that a vast network of global security researchers, acting independently, directly support DNS security	Tim Chen; DomainTools	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:**

#	Comment	Contributor	EPDP Response / Action Taken
	efforts manifest at all levels including those of the individual, corporate, service-provider and nation-state. This is particularly evident in law enforcement work, which is one of the few arenas where such work is occasionally made public.		[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
18.	No additional purposes are required.	• Mark Massey; Domain Name Rights Coalition • Farzaneh Badii; Internet Governance Project • 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.]
19.	No additional purposes are required. The addition of new data elements to the RDDS is beyond the scope of the EPDP Team's work. The EPDP Team has a narrow charter, and was not chartered to create new features and purposes for processing gTLD Registration Data. The NCSG believes such an issue is best taken up in the GNSO Next-Generation RDS to Replace WHOIS PDP, should this PDP Working Group ever be reconvened, or alternatively to be addressed by any PDP Working Group that replaces it in determining RDS functions that fall outside of the scope of this EPDP.	Ayden Férdeline; NCSG	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
20.	Purposes should reference the need for processing for law enforcement, DNS abuse, IP infringement and consumer protection purposes. INTA also supports clarification of purposes to include research of DNS abuse since this falls squarely within ICANN's mission and is one of the primary bases for the obligation of registrars to collect registrant data insofar as ICANN is concerned. If these purposes cannot be clarified within the framework of the existing purposes enumerated above, then it may be necessary to include additional purposes. The list of purposes set forth above are integral to accomplishing ICANN's mission, and ensuring the health and welfare of the DNS system, for the benefit of individual registrants, as well as the many stakeholders who have an interest in the DNS system.	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.]
21.	SSAC supports the creation of an additional purpose for the processing of registration data (in deliberations referred to previously as Purpose O). This purpose would be for ICANN Org teams other than Contractual Compliance to be able to conduct research. ICANN teams (like OCTO and SSR) should have the ability to conduct research relating to security, stability and overall patterns affecting the DNS ecosystem. This may require them to be able to access pseudonymized registration data.	Ben Butler; SSAC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
22.	The GAC supports the intent of "Purpose O" that is being considered by the EPDP but not part of the initial report at this point:	Fabien Betremieux; GAC	Concerns Divergence Support New Idea **EPDP Response:**

#	Comment	Contributor	EPDP Response / Action Taken
	Research and publish reports on threats to the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS As detailed in the related Data Element Workbook (a working document of the EPDP Team last circulated on 15 November 2018), the legal basis for processing data under this purpose would rely on GDPR Article 6.1(f), "with specific safeguards defined in Article 89". Research might also be considered as a compatible purpose if the criteria in Article 6(4) GDPR are met and appropriate safeguards, which may include encryption or pseudonymisation, are implemented. Research activities by ICANN might provide trusted and verifiable information to the Internet community regarding the Internet's system of unique identifiers, helping in that way to preserve and enhance the administration of the DNS system, as well as to ensure its resilience, stability, security and openness. In that regard, the EPDP is recommended to explore how to best accommodate ICANN's research activities in line with EU GDPR requirements. Further, the GAC believes that Purpose O (or something similar) could and should capture the purpose of ICANN to process information associated with its registration data Accuracy Reporting System.		**Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
23.	The IPC supports the addition of purposes related to research - covering research performed by ICANN Org (as currently described in "Purpose O") but extending to any ICANN group also research performed by relevant and legitimate 3rd parties. 1. [Current Purpose O] - "Research and publish reports on threats to the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS." The IPC believes this purpose should encompass and enable all ICANN groups and divisions (OCTO, GDD, Compliance) to conduct operations, facilitation activities, and implement consensus policies (adopted in accordance with the ICANN Bylaws) consistent with its mission of furthering the operational stability, reliability, global interoperability, resilience and openness of the DNS. 2. ENABLE [RELEVANT AND LEGITIMATE 3RD PARTY] RESEARCH OF DNS ABUSE AND THE SECURITY, STABILITY AND RESILIENCY OF THE DOMAIN NAME SYSTEM 1. Research is a legitimate basis for processing per GDPR Article 6(1)f, with specific safeguards defined in Article 5(1)(e) and Article 89. It is also squarely within ICANN's mission and mandate, as the requirement for research derives from Section 1.2a (Commitments) of the ICANN bylaws: (i) Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet; (ii) Maintain the capacity and ability to coordinate the DNS at the overall level and work for the	Brian King; IPC	Concerns Divergence Support New Idea **EPDP Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	maintenance of a single, interoperable Internet; This purpose exists to ensure that ICANN may continue to use registration data in support of its mission, whilst maintaining the privacy of data subjects through appropriate safeguards such as pseudonymisation. In addition, this purpose enables ICANN to continue to operate its Accuracy Reporting System (ARS), which publishes periodic reports on accuracy, using full WHOIS contact fields. The ARS is an important program approved by the ICANN Board in response to the recommendations from the 1st WHOIS Review Team. 2. Research conducted by relevant and legitimate third parties with respect to DNS Abuse and the security, stability and resiliency of the Domain Name System is a fundamental and legitimate purpose consistent with ICANN's Bylaws and critical for ICANN to fulfill its mission. Since such research can and often does involve analysis of data associated with Registered Name Holders, this purpose is directly related to the collection and processing of such data.		