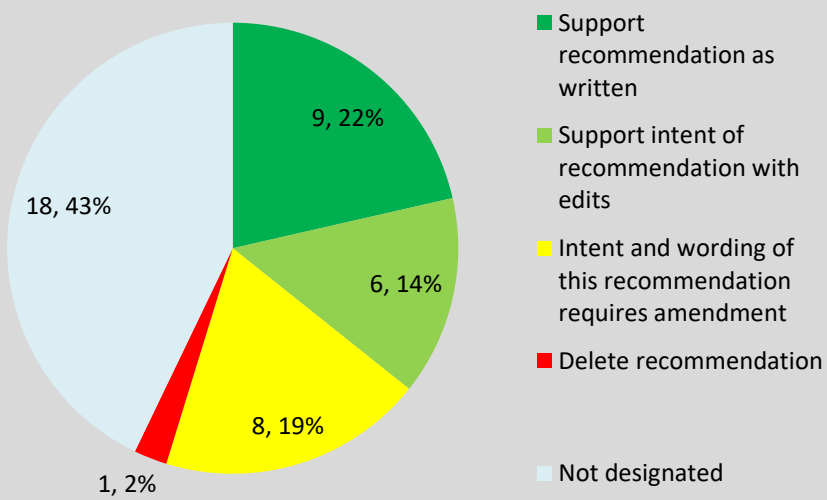
RECOMMENDATION 14

#	Comment	Contributor	EPDP Response / Action Taken
The EPDP Team recommends that the policy includes the following data processing activities as well as responsible parties: [See Initial Report pages 17-21]  			
Support recommendation as written			
1.	No comments provided in support of this recommendation	• DR. JAIDEEP KUMAR MISHRA ; DIRECTOR MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA • Lars Steffen; eco – Association of the Internet Industry	Support **EPDP Response:** The EPDP appreciates the support **Action Taken:** none [COMPLETED]

#	Comment	Contributor	EPDP Response / Action Taken
		• Wolf-Ulrich Knoben; ISPCP Constituency • Monica Sanders; i2Coalition • David Martel • Etienne Laurin • Ben Butler; SSAC	
2.	While we are generally OK with the proposed roles/responsibilities as currently written, it is with the caveat that responsibilities of the respective parties for all processing activities must be further defined, detailed and captured in the appropriate data processing agreements (i.e., a JCA).	Sara Bockey; GoDaddy	Support **EPDP Response:** The EPDP appreciates the support **Action Taken:** none [**COMPLETED**]
3.	The extensive list of processing activities, responsible parties and legal bases is a good first approximation. We support its broad outlines as proposed but are open-minded regarding comments proposing modifications.	Farzaneh Badii; Internet Governance Project	Support **EPDP Response:** The EPDP appreciates the support **Action Taken:** none [**COMPLETED**]

#	Comment	Contributor	EPDP Response / Action Taken
Support intent of recommendation with edits			
4.	MarkMonitor supports that the policy includes the data processing activities and the responsible parties. The policy should also note that the activities and parties outlined are as the EPDP team understands the facts and law to be now, and may be subject to change based on forthcoming legal advice, EDPB guidance, and future industry and policy development. Some of the specifics in the tables beginning on p. 63 may need some further clarification. In particular, on p. 66, under "disclosure" no party is listed in the context of facilitating DRPs like the UDRP. But disclosure generally occurs upon the filing of a "Doe" or P/P complaint, where the registrar provides the underlying contact details to the dispute resolution provider (DRP) and the DRP then discloses them to the complainant who then would typically file an amended complaint with the updated registrant information. Thus, we would suggest listing Registrar and DRP as responsible parties for disclosure for this purpose, with 6(1)(f) as the lawful basis. Similarly, for "data retention" in the same table, we would suggest the DRP as the "responsible party" in the sense that even where the underlying registration data may no longer be retained at the ICANN/registry/registrar levels, dispute resolution determinations and underlying materials containing the initially disclosed registration data would likely be considered retention of the data. Again, the lawful basis for data retention would be 6(1)(f). In the context of this purpose, both registrar and DRP should be considered as "processors" with ICANN being a controller given that the dispute resolution mechanisms are implemented pursuant to ICANN policies. MarkMonitor also calls the team's attention to footnotes 48-51 which cite instances where 6(1)(b) is a better lawful basis.	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
5.	Specifics in the tables beginning on p. 63 would benefit from further clarification. In particular, on p. 66, under "disclosure," no party is listed in the context of facilitating DRPs (like the UDRP). But disclosure generally occurs upon the filing of a "Doe" or privacy/proxy complaint, where the registrar provides the underlying contact details to the dispute resolution provider (DRP) and the DRP then discloses them to the complainant, who can then file an amended complaint with the updated registrant information. The BC therefore suggests listing Registrar and DRP as responsible parties for disclosure for this purpose, with 6(1)(f) as the lawful basis. Similarly, for "data retention" in the same table, the DRP can be listed as the "responsible party" -- even where the underlying registration data may no longer be retained at the ICANN/registry/registrar levels, dispute resolution determinations and underlying materials containing the initially disclosed registration data would likely be considered retention of the data. Again, the lawful basis for data retention would be 6(1)(f). In the context of this purpose, both registrar and DRP should be considered as "processors" with ICANN being a controller given that the dispute resolution mechanisms are implemented pursuant to ICANN policies. The BC also calls the team's attention to footnotes 48-51, where we cite instances where 6(1)(b) is a better lawful basis.	Steve DelBianco; BC	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
6.	Some of the specifics in the tables beginning on p. 63 may need some further clarification. In particular, on p. 66, under "disclosure" no party is listed in the context of facilitating DRPs like the UDRP. But disclosure generally occurs upon the filing of a "Doe" or P/P complaint, where the registrar provides the underlying contact details to the dispute resolution provider (DRP) and the DRP then discloses them to the complainant who then would typically file an amended complaint with the updated registrant information. Thus, we would suggest listing Registrar and DRP as responsible parties for disclosure for this purpose, with 6(1)(f) as the lawful basis. Similarly, for "data retention" in the same table, we would suggest the DRP as the "responsible party" in the sense that even where the underlying registration data may no longer be retained at the ICANN/registry/registrar levels, dispute resolution determinations and underlying materials containing the initially disclosed registration data would likely be considered retention of the data. Again, the lawful basis for data retention would be 6(1)(f). In the context of this purpose, both registrar and DRP should be considered as "processors" with ICANN being a controller given that the dispute resolution mechanisms are implemented pursuant to ICANN policies. See response to previous question.	Brian King; IPC	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
7.	The NCSG supports the intent of this recommendation, and the identification of the different processing activities and responsible parties (controllers and processors) for each. However, the NCSG maintains that we disagree with the inclusion of Purpose #2 and Purpose #7 as they are currently worded in the initial report, and therefore, cannot support any of the processing activities and responsible parties associated with them at this time.	Ayden Férdeline; NCSG	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
8.	Some of the specifics in the tables beginning on p. 63 may need some further clarification. In particular, on p. 66, under "disclosure" no party is listed in the context of facilitating DRPs like the UDRP. But disclosure generally occurs upon the filing of a "Doe" or P/P complaint, where the registrar provides the underlying contact details to the dispute resolution provider (DRP) and the DRP then discloses them to the complainant who then would typically file an amended complaint with the updated registrant information. Thus, we would suggest listing Registrar and DRP as responsible parties for disclosure for this purpose, with 6(1)(f) as the lawful basis. Similarly, for "data retention" in the same table, we would suggest the DRP as the "responsible party" in the sense that even where the underlying registration data may no longer be retained at the ICANN/registry/registrar levels, dispute resolution determinations and underlying materials containing the initially disclosed registration data would likely be considered retention of the data. Again, the lawful basis for data retention would be 6(1)(f). In the context of this purpose, both registrar and DRP should be considered as "processors" with ICANN being a controller given that the dispute resolution mechanisms are implemented pursuant to ICANN policies.	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.]
9.	P 63: The DNS requires that IP addresses must also be disclosed in applicable cases. The remaining thin gTLD registries should be required to move to thick status, per the Thick WHOIS Consensus Policy and Board Resolution 2014.02.07.08.	Greg Aaron; iThreat Cyber Group	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
Intent and wording of this recommendation requires amendment			
10.	The Initial Report indicates which actors are "Responsible Parties" for the data processing activities that correspond to each Purpose. However, the term "responsible party" is not a defined term under the GDPR and does nothing to indicate which party is the controller or processor, or whether the parties may be joint controllers, for each processing activity. The EPDP Team did not specifically discuss and analyze the roles and responsibilities of each party for any of the processing activities required for any of the Purposes. It must do so, and revise the recommendation as appropriate. The RySG is willing and available to contribute to this analysis as the EPDP Team needs. A party's involvement in a given processing activity – or whether it has some "responsibility" with regard to that processing activity – does not automatically indicate its role and responsibility under the GDPR. The EPDP Team must analyze each processing activity required for each purpose to determine which party determines the means and purposes of processing to identify which party is the controller (or potentially which parties are joint controllers, or independent controllers). This level of analysis has not yet been conducted by the EPDP Team, and as such, this recommendation cannot yet be finalized	Wim Degezelle ; RySG	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
11.	A lot of this needs to be in the form of a JCA to capture it all correctly; a clear determination of the responsibilities hinges on the role of ICANN ORG. The ICANN ORG position as to their role in data processing seems to change according to blog posts, correspondence and other publications. It is imperative that this be documented and consensus achieved on this point so that we can proceed with setting up the appropriate data sharing agreements. The EPDP team did not engage much in discussing the high number of accredited registrars with resellers who also process data. It may not be feasible to list all the processing activities of the resellers in such a JCA, but it is imperative for the registrants/data subjects we capture it all correctly. For example: The right of rectification should be done at a reseller level in the case of wholesale registrars. The temp spec states this should be done by registrars (this is incorrect in some registrars opinion). The reseller acts as a starting point to correct the data in the entire DNS chain (registrar, registries, data escrow). However, it is not limited to the DNS chain: the chances are that the registrant has obtained more services through the reseller which are not part of the DNS, but which require data correction also.	• Volker Greimann; Key-Systems GmbH • Zoe Bonython; RrSG	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	In this specific example/purpose, the reseller is the data controller and not ICANN, and we should not create situations where registrants instruct ICANN to correct their data even though ICANN will be the ultimate data controller for many purposes. Also, it is worth discussing something which has not been considered by the EPDP team so far:he disclosure of registrant data by resellers. Due to the lack of correct agreements with ICANN and registries, most registrars act as a data processor for many purposes and are limited by the contracts from certain resellers who operate as a data controller (hosting companies, ISP's, telecom providers, etc.). The legal basis might be different from a reseller point of view. As such the JCA will be a tremendous and complicated task, but it needs to be done if we want to serve the registrant correctly regarding his or her fundamental rights.		
12.	[No rationale or amendment provided]	Domain.com, LLC & affiliates	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
13.	Data processing agreements need to be kept out of policy. They're contractual and subject to change when new processors etc., are added or others are taken away. Putting this into policy is a bad idea	Michele Neylon; Blacknight Internet Solutions Ltd	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
14.	somewhat duplicative question The data processing activities enumerated in the Initial Report appear to include actions against the registrant's second level domain name, e.g., UDRP and URS, and also to include actions against the registry and its generic top level domain, e.g, PDDRP and RRDRP. It's completely ambiguous and unknown in which category (or another) "future-developed domain name registration-related dispute procedures" may fall. Accordingly, and consistent with our lengthy response to Purpose 6 above (which we ask Staff to transfer in full to any comment summary), we have to object strongly anything as vague,	A. Mark Massey; Domain Name Rights Coalition	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	broad, undefined and dangers as -- “the following data processing activities.” We note above that we have strongly objected to various collection activities, processing activities, transmission of personal and sensitive data from Registrars to Registries (the largest in countries not even deemed “adequate” by GDPR for data protection laws and activities). DNR has objected to Purpose 2 above, “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,” for all the reasons set out above. DNRC objects to giving up, absent much more proof of registry involvement, the RDDS data of registrants in disputes involving registries (e.g., PDDRP, RRDRP and future disputes where registrants are not even a party! (Purpose 6 above.) We have strongly stated that Purpose 7 should be deleted, namely: “ENABLING VALIDATION TO CONFIRM THAT REGISTERED NAME HOLDER MEETS OPTIONAL GTLD REGISTRATION POLICY ELIGIBILITY CRITERIA VOLUNTARILY ADOPTED BY THE REGISTRY OPERATOR” (and we noted, among other rationales, see above: “Data required for validation could include a wide range of sensitive personal data enabling the identification of individuals or protected groups such as religious, political, ethnic, gender and sexual orientation organizations. There is absolutely no need for this kind of data to be in the RDDS. Registry Operators can and currently do collect and validate this data on their own. Since each specialized registry (including brand registries) have different criteria for validation, this purpose risks openings the door to potentially hundreds of new data elements. Further, it is dangerous and inappropriate for this data to be placed in a global directory that can be accessed by third parties. GTLD validation processes should be limited to individual registries only, and the data needed to do that should not be placed in the RDDS.” So no, asking the same questions as above, blurring the detail in the question, and calling for support of “data processing activities” unenumerated above does not suddenly make them acceptable :-).		

#	Comment	Contributor	EPDP Response / Action Taken
15.	The transfer of data elements from Registrar to Registry and ICANN needs to be total and not partial; Attention is also drawn to the suggestion to collect registration data using the same simple technology as used by credit card companies to collect card data from customers across merchant websites.	Sivasubramanian Muthusamy; Internet Society India Chennai	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
16.	ICANN indicates that the “Responsible Party" for the collection of data is “ICANN”, “Registrars", and “Registries”. As a practical matter, only registrars collect these data. Some of that data is for a lawful basis related directly to the relationship between the registrar ad the customer and some of that data is also related to current ICANN contractual requirements. If ICANN believes that these data must be collected by the registrar for any reason, ICANN must provide justification for each data element. We note that ICANN has yet to demonstrate a legitimate interest in much of the data collected by registrars. ICANN indicates that the “Responsible Party" for the transmission of data from a registrar to a registry is “Registrars” and “Registries”. As a practical matter, registries are not a responsible party for the transmission of data from the registrar to the registry but may be a contractually-responsible party for such data elements as they require. Each registry must provide justification for each data element. We note that this is not a process that ICANN may simply demand. Some registries, for example, have jurisdictional requirements that allow them to demand certain locational data. We note that the long-time existence of thin Whois outputs such as .com indicate that, in practice, the majority of registries do not require many of the personal data that ICANN has, in the past, indicated are necessary to thick Whois. ICANN indicates that the “Responsible Party" for the disclosure of data is “Registrars” and “Registries". It is not clear to whom this disclosure refers. Registrars and registries have legal requirements under their local laws to disclose what data they have to certain parties upon request (such as subpoena or warrant). However, they cannot be required to collect this data simply to disclose it. ICANN indicates that the “Responsible Party" for the retention of data is “ICANN”. We note that this party is, in fact the Data Escrow provider and not ICANN. This function is solely for backup and EBERO purposes—to protect against the catastrophic failure of a registry or registrar. Registrars and registries are, of course, responsible for their own backups and may also have data retention responsibilities but none of that is falls under ICANN’s purview. The EPDP recommends that the seven identified purposes for processing gTLD Registration Data	Tucows Domains Inc.	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
	form the basis of the new ICANN policy, however only analyzes the purpose in each case and not the data element. As expressed above, the purpose is necessary but not sufficient (and in many cases not necessary) but also necessary is an analysis of whether each piece of personal data included in a data element is necessary to that purpose. We have analyzed each of these above and note that most of them see that ICANN has no purpose for collecting much of these data. Page 89 of the EPDP Initial Report analyzes each data element and comes the wrong conclusions, as each element is simply indicated as being "necessary". As previously noted, the long-time existence of thin Whois outputs such as .com indicate that ICANN has does not need the majority of these data elements—which we note include personal data—to protect the security, stability, and resiliency of the Internet, ICANN's stated goal.		
Delete recommendation			
17.	See my response to Recommendation #13.	John Poole; Domain Name Registrant	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
Not designated			
18.	No selection made and no additional comments submitted	• Evin Erdoğdu; ALAC • Dean S. Marks; Coalition for Online Accountability • Lori Schulman Senior Director, Internet Policy; International Trademark Association (INTA) • George Kirikos; Leap of Faith Financial Services Inc. • Tim Chen; DomainTools • Steve Gobin; Corporate domain name management • Ashley Heineman; NTIA	**EPDP Response:** none **Action Taken:** none [**COMPLETED**]

#	Comment	Contributor	EPDP Response / Action Taken
		• Neil Fried; The Motion Picture Association of America • Sajda Ouachtouki; The Walt Disney Company • Greg Mounier on behalf of Europol AGIS; Europol Advisory Group on Internet Security • Monique A. Goeschl; Verein für Anti-Piraterie der Film- und Videobranche (VAP) • Fabien Betremieux; GAC • Brian Beckham; Head, Internet Dispute Resolution Section at WIPO • Theo Geurts • Ivett Paulovics; MFSD Srl URS Provider • Ashley Roberts; Valideus • Renee Fossen; Forum - URS and UDRP Provider • Stephanie Perrin	