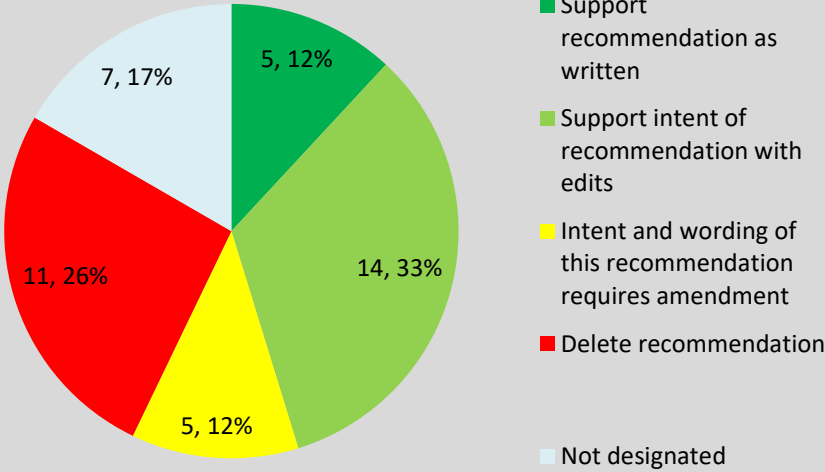


RECOMMENDATION 2

#	Comment	Contributor	EPDP Response / Action Taken																		
	<p>Per the EPDP Team Charter, the EPDP Team is committed to considering a system for Standardized Access to non-public Registration Data once the gating questions in the charter have been answered. This will include addressing questions such as:</p> <ul style="list-style-type: none"> • What are the legitimate purposes for third parties to access registration data? • What are the eligibility criteria for access to non-public Registration data? • Do those parties/groups consist of different types of third-party requestors? • What data elements should each user/party have access to? <p>In this context, amongst others, disclosure in the course of intellectual property infringement and DNS abuse cases will be considered.</p>  <table border="1" data-bbox="705 662 996 1141"> <caption>Survey Results for Recommendation 2</caption> <thead> <tr> <th>Response</th> <th>Count</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Support recommendation as written</td> <td>5</td> <td>12%</td> </tr> <tr> <td>Support intent of recommendation with edits</td> <td>14</td> <td>33%</td> </tr> <tr> <td>Intent and wording of this recommendation requires amendment</td> <td>5</td> <td>12%</td> </tr> <tr> <td>Delete recommendation</td> <td>11</td> <td>26%</td> </tr> <tr> <td>Not designated</td> <td>7</td> <td>17%</td> </tr> </tbody> </table>	Response	Count	Percentage	Support recommendation as written	5	12%	Support intent of recommendation with edits	14	33%	Intent and wording of this recommendation requires amendment	5	12%	Delete recommendation	11	26%	Not designated	7	17%		
Response	Count	Percentage																			
Support recommendation as written	5	12%																			
Support intent of recommendation with edits	14	33%																			
Intent and wording of this recommendation requires amendment	5	12%																			
Delete recommendation	11	26%																			
Not designated	7	17%																			
Support recommendation as written																					
1.	No comment	<ul style="list-style-type: none"> • David Martel • Etienne Laurin • Evin Erdoğan; ALAC • Ashley Heineman; NTIA 	<p>Support EPDP Response: none Action Taken: none [COMPLETED]</p>																		

#	Comment	Contributor	EPDP Response / Action Taken
2.	<p>SSAC considers the creation and implementation of a standardized access system that will provide reliable and timely access to registration data to parties with legitimate interests under the law to be of vital importance. We emphasize that this work should begin as soon as it is possible to do so.</p> <p>Much of the work to identify, investigate, and remove threats to the DNS is conducted by 3rd party cybersecurity professionals. The current system under the Temp Spec does not allow for sufficient or reliable access such that this work can continue to be as effective. Work to replace this with a scalable access model should begin without delay.</p>	Ben Butler; SSAC	<p>Support</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
Support intent of recommendation with edits			
3.	<p>Per the EPDP Team Charter, the EPDP Team is committed to considering a system for DIFFERENT CATEGORIES of Standardized Access to non-public Registration Data</p> <p>If not intended already, standardisation needs to be considered as NOT a single standard for access to all non-public data by all legitimate requests, but different standards for access with different privilege levels to different data elements by differentiated legitimate requests; for instance requests by International Law and Order Agencies and a Commercial third party, both making legitimate requests may NOT access data by a single standard of access, NOT by the same level of privileges.</p>	Sivasubramanian Muthusamy; Internet Society India Chennai	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
4.	<p>Per the EPDP Team Charter, the EPDP Team is committed to considering a system for Standardized, predictable, consistent and lawful Access to non-public Registration Data once the gating questions in the charter have been answered.</p> <p>Minor language tweaks for sake of clarity and being more explicit.</p>	DR. JAIDEEP KUMAR MISHRA ; DIRECTOR MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
5.	<p>Per the EPDP Team Charter, the EPDP Team is committed to considering a system for Standardized Access to non-public Registration Data once the gating questions in the charter have been answered. This will include addressing questions such as:</p> <ul style="list-style-type: none"> • What are the legitimate purposes for third parties to access registration data? • What are the eligibility criteria for access to non-public Registration data? • Do those parties/groups consist of different types of third-party requestors? • What data elements should each user/party have access to? <p>In this context, amongst others, disclosure in the course of legal and DNS abuse cases will be considered.</p> <p>We support disclosure of Registration Data in the course of investigation of DNS and legal abuse. We do not find it necessary to call out specific types of legal abuse. Accordingly, we propose the edited version provided above.</p> <p>We have proposed this modification as we support the exploration of a Standardized Access model that complies with legal and regulatory obligations, but it should be noted such a model ought not be construed to be policy as it has not completed a true PDP nor was it contemplated to be a policy when it was entered into the EPDP charter. We further note that a “system” for Standardized Access need not be a technical system but could also be a procedure. Finally, data that is distributed must be limited data that there was a legal basis to collect and that the distribution is not, itself, a legal basis.</p>	Tu cows Domains Inc.	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
6.	<p>The NCSG asks that the term “Standardized Access to nonpublic Registration Data” be replaced with the term, “Lawful disclosure of personal and sensitive registration data to third parties with legitimate interests.”</p> <p>In essence, Recommendation 2 is simply a restatement of one aspect of the EPDP’s charter. We note that later on in this report, the wording change we proposed here was accepted.</p>	Ayden Férdeline; NCSG	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
7.	<p>Yes, we recommend the final line in Recommendation #2 be edited to read:</p> <p>“In this context, amongst others, the ePDP Team will develop a policy that prescribes the method for disclosing non-public registrant data to third parties that have established legitimate interest in viewing registrant data, such as intellectual property rights holders, cybersecurity firms, organizations that mitigate DNS abuse, and law enforcement agencies.”</p> <p>This change will ensure that the policy developed by the EPDP meets the needs of all the stakeholders whose actions the successful maintenance of the stability, security and resiliency of DNS system rely.</p> <p>Failure to provide adequate access for all the stakeholders who have a role in preserving the stability, security and resilience, including intellectual property rightsholders, cybersecurity firms and other organizations that mitigate DNS abuse as well as law enforcement agencies runs the risk of undermining that security and furthering distrust of the Internet ecosystem. It would also be contrary to the longstanding purposes of the WHOIS system, which have always included these parties as evidenced in the earliest protocol for a directory service published in 1982 by the Internet Engineering Task Force that included contact information of anyone transmitting data across the ARPANET in order to “serve the needs of different stakeholders such as domain name registrants, law enforcement agents, intellectual property and trademark owners, businesses and individual users.” (History of WHOIS, ICANN WHOIS, https://whois.icann.org/en/history-whois).</p> <p>Moreover, providing reasonable access to all relevant stakeholders is clearly the expectation set by the European Data Protection Board in its May 27 communication to ICANN -- (ICANN is “to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data”).</p>	Sajda Ouachtouki; The Walt Disney Company	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
8.	<p>The BC recommends that the final line of the recommendation should be edited to read: “In this context, amongst others, the ePDP Team will develop a policy that prescribes the method for disclosing non-public registrant data to third parties that have established legitimate interest in viewing registrant data, such as intellectual property rights holders, cybersecurity firms, organizations that mitigate DNS abuse, and law enforcement agencies.”</p> <p>Now that the EPDP team’s gating questions have been sufficiently addressed, the BC strongly supports a recommendation that the EPDP Team contribute to ICANN Org’s development of a standardized, or “unified,” system for access to non-public registration data. Thus, the BC proposes edits to this recommendation to ensure that the protection of intellectual property and other rights are expressly recognized as a legitimate interest under GDPR and therefore understood to be within scope of the final policy. In the Article 29 Working Party’s letter to ICANN dated April 11, 2018 (https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-11apr18-en.pdf), the A29WP “welcome[d] the decision of ICANN to propose an interim model which involves layered access, as well as an “accreditation program” for access to non-public WHOIS data.” This communication signaled A29WP’s support for a standardized access program. This support is further emphasized in a May 27 communication to ICANN (https://www.icann.org/en/system/files/files/statement-edpb-whois-27may18-en.pdf), in which the European Data Protection Board reiterated its expectation that ICANN is “to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data.”</p>	Steve DelBianco; BC	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
9.	<p>Prefer the final paragraph to read "In this context, amongst others, disclosure in the course of law enforcement, cybersecurity, DNS abuse, and intellectual property protection activity will be considered."</p> <p>simply adding more detail and color by listing legitimate purposes which are specifically mentioned in the GDPR text (security and LEA)</p>	Tim Chen; DomainTools	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
10.	<p>The EPDP WG needs to state clearly in the report that it will not have the time to really consider this charter subject before it completes its final report. Between now and the final report due date, the EPDP WG has to consider public comments, measure consensus levels, and more, and likely will not break new ground.</p>	Greg Aaron; iThreat Cyber Group	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
11.	<p>INTA requests that the general comment in Recommendation #2 be edited to read as follows: “In this context, amongst others, the EPDP Team will develop a policy that prescribes the method for disclosing non-public registrant data to third parties that have established legitimate interest in viewing registrant data including intellectual property rights holders, cybersecurity firms, organizations that mitigate DNS abuse, and law enforcement agencies, among others.”</p> <p>INTA strongly supports this recommendation for the EPDP Team to develop a standardized, or “unified,” system for access to non-public registration data after the gating questions have been answered.</p> <p>INTA proposes edits to this recommendation to ensure that the protection of intellectual property rights is expressly recognized as a legitimate interest under GDPR and therefore understood to be within scope of the final policy. The term “legitimate” implies that the interest is bolstered by recognition of a legal right, which in the case of intellectual property is the reason for its very existence. Intellectual property rights are regarded as third generation human rights and are duly recognized as human rights under Article 27 (2) of the Universal Declaration of Human Rights. The Article provides that ‘Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.’</p> <p>In the Article 29 Working Party’s letter to ICANN dated April 11, 2018, the A29WP “welcome[d] the decision of ICANN to propose an interim model which involves layered access, as well as an “accreditation program” for access to non-public WHOIS data.” This communication signaled A29WP’s support for a standardized access program. This support is further echoed, in a May 27 communication to ICANN, in which the EPDB reiterated that it expects ICANN “to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data.”</p> <p>With respect to the reference to “relevant stakeholders,” ICANN has identified “intellectual property rights holders as being such stakeholders with a legitimate interest in having access to registrant data.</p> <p>For the reasons expressed above and in deference to the statements provided, INTA recommends the edits provided above.</p>	Lori Schulman Senior Director, Internet Policy; International Trademark Association (INTA)	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
12.	<p>Per the EPDP Team Charter, the EPDP Team is committed to answering the additional gating questions in the charter and recommending a system for Standardized Access to nonPublic Registration Data no later than submission of its Final Report.</p> <p>“In this context, amongst others, the EPDP Team will develop a policy that prescribes the method for disclosing non-public registrant data to third parties that have established legitimate interest in accessing registrant data including intellectual property rights holders, cybersecurity firms, organizations that mitigate DNS abuse, and law enforcement agencies.”</p> <p>These additions reflect that the protection of intellectual property rights is expressly recognized as a legitimate interest under GDPR and therefore understood to be within scope of the final policy.</p> <p>The charter calls for the EPDP team to deliver an Initial Report outlining a proposed model of a system for providing accredited access to non-public Registration Data, not to “consider” doing so. The EPDP fails to fulfill its charter if it does deliver a model for a system for standardized access to non-public data. At a bare minimum the team should commit to a time certain to complete this work, and no consensus policy superseding the Temporary Specification should be adopted without it.</p> <p>In the Article 29 Working Party’s letter to ICANN dated April 11, 2018, the A29WP “welcome[d] the decision of ICANN to propose an interim model which involves layered access, as well as an “accreditation program” for access to non-public WHOIS data.” This communication signaled A29WP’s support for a standardized access program. This support is further echoed, in a May 27 communication to ICANN, in which the EPDB reiterated that it expects ICANN “to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data.”</p>	<p>Brian King; MarkMonitor, Inc., a Clarivate Analytics company</p>	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
13.	<p>Per the EPDP Team Charter, the EPDP Team is committed to developing a system for Standardized Access to non-public Registration Data once the gating questions in the charter have been answered, such as the proposal from ICANN for a unified access model, or through other means that ICANN has suggested exploring, including ICANN assuming legal responsibility for providing access as a sole controller. See Göran Marby, ICANN President and CEO, ICANN GDPR and Data Protection/Privacy Update, ICANN (Sept. 24, 2018), https://www.icann.org/news/blog/icann-gdpr-and-data-protection-privacy-update. In this context, amongst others, this will include disclosure to law enforcement authorities and third parties in the course of intellectual property infringement and DNS abuse cases will be considered.</p> <p>The two instances of the word “considering” suggests the ePDP might conclude that no such standardized model should be created, and that disclosure is not necessary in intellectual property infringement cases.</p> <p>Failure to adopt a standardized model is contrary to the ePDP Charter, which states that work on a standardized model “shall begin once the gating questions above have been answered and finalized in preparation for the Temporary Specification initial report.” ePDP Charter at 7 (emphasis added), https://gnso.icann.org/sites/default/files/file/field-file-attach/temp-spec-gtld-rd-epdp-19jul18-en.pdf.</p> <p>Similarly, failure to disclose to law enforcement authorities and third parties in intellectual property infringement cases would be contrary to the longstanding purpose of the WHOIS system to thwart such infringement. 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. (emphasis added).</p>	Neil Fried; The Motion Picture Association of America	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
14.	<p>“In this context, a method for promptly and predictably disclosing non-public registrant data to third parties who have demonstrated legitimate interest in viewing registrant data such as those that perform cybersecurity investigations, intellectual property enforcement, consumer protection, DNS abuse mitigation, and law enforcement will be developed.”</p> <p>The existing text seems to imply that intellectual property infringement and DNS abuse cases are only worth being “considered” and are not first-class legitimate purposes for performing disclosure. We disagree with this assertion and suggest the edits above to clarify any ambiguity about this. As stated elsewhere, brand abuse is increasingly an enabling mechanism for cyber abuse. It should be clear that consumers can be harmed when what seems to be a branded pharmaceutical good is actually a low-quality counterfeit, but many are not aware that fake branded digital goods may actually contain malware or connect to phishing sites which are used to harvest credentials or drop malicious payloads.</p>	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	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
15.	<p>Intellectual property infringement and DNS abuse cases will be recognized as legitimate purposes for disclosure.</p> <p>A right holder must be able to contact the registrant of a domain in order to send a notification of infringement and the registrar/registry must facilitate this basic level of communication. This is especially the case where domain operators mask their registration information.</p> <p>As a representative of right holders whose rights are systematically infringed on a commercial scale, VAP's right of information is regularly ignored or rejected with the argument that the infrastructure provider is not liable for content of a domain. Thereby registrars/registries ignore their own terms and conditions which purportedly prohibit the use of domains for illegitimate purposes.</p>	Monique A. Goeschl; Verein für Anti-Piraterie der Film- und Videobranche (VAP)	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
Intent and wording of this recommendation requires amendment			
16.	<p>DNRC strongly recommends replacing the term “Standardized Access to nonpublic Registration Data” with the term “Lawful disclosure of nonpublic registration data to third parties with legitimate interests.”</p> <p>In essence, Recommendation 2 is simply a restatement of one aspect of the EPDP’s charter. Later in this report, the wording change proposed above was accepted.</p>	A. Mark Massey; Domain Name Rights Coalition	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
17.	<p>The IPC requests that the general comment in Recommendation #2 be edited to read as follows: “In this context, amongst others, the ePDP Team will develop a policy that prescribes the method for disclosing non-public registrant data to third parties that have established legitimate interest in accessing registrant data including intellectual property rights holders, cybersecurity firms, organizations that mitigate DNS abuse, and law enforcement agencies.” Per the EPDP Team Charter, EPDP Team is committed to answering the additional gating questions in the charter and recommending a system for Standardized Access to nonPublic Registration Data no later than submission of its Final Report. In this context, amongst others, disclosure in the course of intellectual property infringement and DNS abuse cases will be considered.</p> <p>The charter calls for the EPDP team to deliver an Initial Report outlining a proposed model of a system for providing accredited access to non-public Registration Data, not to “consider” doing so. The EPDP fails to fulfill its charter if it does not deliver a model for a system for standardized access to non-public data. At a bare minimum the team should commit to a time certain to complete this work, and no consensus policy superseding the Temporary Specification should be adopted without it.</p> <p>The IPC strongly supports this recommendation for the EPDP Team to develop a standardized, or “unified,” system for access to non-public registration data after the gating questions have been answered.</p> <p>The IPC proposes edits to this recommendation to reflect that the protection of intellectual property rights is expressly recognized as a legitimate interest under GDPR and therefore understood to be within scope of the final policy.</p> <p>In the Article 29 Working Party’s letter to ICANN dated April 11, 2018, the A29WP “welcome[d] the decision of ICANN to propose an interim model which involves layered access, as well as an “accreditation program” for access to non-public WHOIS data.” This communication signaled A29WP’s support for a standardized access program. This support is further echoed, in a May 27 communication to ICANN, in which the EPDB reiterated that it expects ICANN “to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR, without leading to an unlimited publication of those data.”</p> <p>With respect to the reference to “relevant stakeholders,” ICANN has identified “intellectual property rights holders as being such stakeholders with a legitimate interest in having access to registrant data.</p> <p>For the reasons expressed above and in deference to the statements provided, the IPC recommends the edits provided above.</p>	Brian King; IPC	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
18.	<p>Per the EPDP Team Charter, the EPDP Team is committed to answering the additional gating questions in the Charter and developing and recommending a system for Standardized Access to non-public Registration Data no later than the submission of its Final Report. This will include addressing questions such as:</p> <ul style="list-style-type: none"> • What are the legitimate purposes for third parties to access registration data? • What are the eligibility criteria for access to non-public Registration data? • Do those parties/groups consist of different types of third-party requestors? • What data elements should each user/party have access to? <p>In this context, amongst others, the EPDP Team will develop a proposal that sets forth the method and process for disclosing non-public Registration data to third parties that have established legitimate interest in accessing non-public Registration data, including intellectual property rights holders, cybersecurity firms, organizations that mitigate DNS abuse, consumer protection organizations and law enforcement agencies.</p> <p>In order to fulfill its Charter, the EPDP Team must develop and deliver a proposal to address standardized access to non-public registrant data. The edits to Recommendation #2 submitted here recognize this as a requirement of the Charter that must be fulfilled by the EPDP Team no later than the submission of its Final Report.</p> <p>Moreover, specific guidance from the European Data Protection Board has been received by ICANN in the Board's May 27 communication wherein it stated that it expects ICANN "to develop and implement a WHOIS model which will enable legitimate uses by relevant stakeholders, such as law enforcement, of personal data concerning registrants in compliance with the GDPR . . . "</p> <p>The suggested edits offered above further clarify "relevant stakeholders" by specifically calling out intellectual property rights holders, cybersecurity firms, organizations that mitigate DNS abuse, consumer protection organizations and law enforcement agencies</p>	Dean S. Marks; Coalition for Online Accountability	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
19.	<p>Registrars or registry operators should put in place a data disclosure process, which allows any third party that can evidence a legitimate right to a domain name to obtain the complete whois data of a domain name.</p> <p>The temporary Specifications currently only require Registrar and Registry Operator to provide reasonable access to Personal Data in Registration Data to third parties on the basis of a legitimate interests pursued by the third party. The definition of "reasonable access" is vague and may be subject to interpretation.</p> <p>A lot of ccTLD registry operators such as EURid have already put in place procedures where a third party that wants to obtain the complete whois data of a domain name have to submit a form duly completed, signed and stamped together with evidences of its legitimate right to the concerned domain name (e.g. trademark certificate, BRC...) to the registry operators. Such procedures are compliant with the GDPR.</p>	Steve Gobin; Corporate domain name management	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
20.	<p>With six months of GDPR experience behind us, it is obvious that ICANN needs to turn its concerted attention to addressing the need for a unified/standardized system for reasonable access to non-public registrant data.</p> <p>Failure to provide a solution is harming a range of legitimate causes.</p> <p>As stated by the Interpol representative at the ICANN Meeting in Barcelona, “investigations are affected by [and] have been slowed down or have been challenged by WHOIS.”</p> <p>Decisive action in developing a unified/standardized access model would foster predictability, in all stakeholders’ interests, and to this end WIPO remains willing to assist in a potential accreditation body capacity.</p> <p>Even if this reflects the EPDP Charter, we find Recommendation No. 2 troubling in that it suggests the EPDP will “turn its attention to considering a system for Standardized Access to non-public Registration Data once the gating questions in the charter have been answered”.</p> <p>Not only does this fail to commit to actually coming up with a solution, it proposes to only begin “considering” one once the “gating questions” have been answered.</p> <p>We see no compelling reason why work on a unified/standardized system for reasonable access to non-public registrant data cannot commence immediately in parallel with the EPDP effort.</p>	Brian Beckham; Head, Internet Dispute Resolution Section, WIPO	<p>Concerns</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
Delete recommendation			

#	Comment	Contributor	EPDP Response / Action Taken
21.	<p>Delete</p> <p>1) There is no "recommendation" provided, just a statement that the "EPDP Team is committed to considering a system for Standardized Access to non-public Registration Data once the gating questions in the charter have been answered."</p> <p>2) Read EPDP Charter p.9: "Work on recommendations for a System for Accredited Access to Non-Public Registration Data should NOT commence until all gating questions have been answered. Similarly, delivery of the Final Report on the EPDP Team's recommendations on issues relating to the Temporary Specification for gTLD Registration Data to the GNSO Council and subsequently the ICANN Board (before 25 May 2019) should NOT be held up by work that may still be ongoing in relation to the EPDP Team's recommendations for a System for Accredited Access to Non-Public Registration Data."</p> <p>The EPDP working group needs to answer the gating questions before addressing and making any "recommendations" about "access" to non-public Registration Data."</p>	John Poole; Domain Name Registrant	<p>Divergence</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
22.	Disclosure of registration data to 3rd parties is not a "purpose" for its collection.	Michele Neylon; Blacknight Internet Solutions Ltd	<p>Divergence</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
23.	This is a statement of something already in the charter. It is not a recommendation. As such, it should be removed. We welcome the opportunity to explore this topic further after the EPDP has concluded.	Sara Bockey; GoDaddy	<p>Divergence</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
24.	The recommendation shall only be supported conditional to confirmation that such processing is possible in a legally compliant fashion. One way of doing this is to recommend the preparation of a code of conduct according to Art. 40 of the GDPR and enact the recommendation only if and when such code of conduct is approved.	Lars Steffen; eco – Association of the Internet Industry	<p>Divergence</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
25.	<p>While we understand this language was compromise language within the ePDP team, the RrSG does not believe it is appropriate to consider this a policy recommendation at this time. As stated in the ePDP charter and reinforced in the initial report, the topic of Standardized Access to non-Public registration Data should only be considered once all of the gating questions have been answered. The access discussion was clearly going to be one of the most challenging issues for the ePDP team to address and it was very deliberate of the GNSO council to structure the Charter in this manner so as to head-off the possibility of this topic derailing the work of the group. It is crucial the team be allowed to address and lock down solid policy recommendations based on the gating questions before addressing the issue of access to non-public Registration Data.</p> <p>Members of the RrSG participating in the ePDP team have been consistent in voicing their openness to participating in the discussion surrounding access once the gating questions have been addressed and we reinforce that sentiment in these comments. At such time that the working group has resolved all of the gating questions, we look forward to moving on to the discussion around access.</p>	<ul style="list-style-type: none"> • Zoe Bonython; RrSG • Volker Greimann; Key-Systems GmbH 	<p>Divergence</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
26.	No comment supplied	Domain.com, LLC & affiliates	<p>Divergence</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
27.	The recommendation shall only be supported conditional to confirmation that such processing is possible in a legally compliant fashion. One way of doing this is to recommend the preparation of a code of conduct according to Art. 40 of the GDPR and enact the recommendation only if and when such code of conduct is approved.	Wolf-Ulrich Knoben; ISPCP Constituency	<p>Divergence</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
28.	Third party access to registration data is not part of ICANN's mission.	Monica Sanders; i2Coalition	<p data-bbox="1630 140 1751 165">Divergence</p> <p data-bbox="1630 172 1809 197">EPDP Response:</p> <p data-bbox="1630 236 1787 261">Action Taken:</p> <p data-bbox="1630 300 2020 325">[COMPLETED / NOT COMPLETED] –</p> <p data-bbox="1630 331 1975 357">[Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
29.	<p>All WHOIS should essentially be public, and not gated. My company wants to always opt-in to public WHOIS for our own data, and mechanisms should be in place to require registrars to permit this opt-in (some have not yet done so, despite the temporary spec!)</p> <p>But, I do respect that some seek privacy (opting in to that). I don't think ICANN should be developing that system, but instead there is an alternative, namely putting it in the hands of the courts, using a mechanism like we have in Canada for "Norwich Orders", see: https://www.lerners.ca/lernx/norwich-orders/ or https://en.wikipedia.org/wiki/Norwich_Pharmaceutical_order or search Google "Norwich Orders" to find more.</p> <p>I believe an ICANN-developed system will be ripe for abuse (i.e. overreach by trademark interests, for example), and would have limited penalties, whereas abusers of a Norwich-type order could be penalized by the courts. Furthermore, courts recognize that intermediaries (e.g. registrars/registries) would be entitled to reasonable cost recovery, as per the recent judgment in the recent Supreme Court of Canada involving Rogers and Voltage Pictures, see: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/17254/index.do</p> <p>Again, I emphasize that I want the WHOIS to be public, but if folks are going to insist on privacy for some of that data, the courts (of a competent jurisdiction) are the right place, not ICANN. To be clear, a competent jurisdiction should be the jurisdiction of the entity holding the data (e.g. location of registrar or registry, as the case may be, depending on whether it's a thin or thick WHOIS system in place). As an aside, returning to thin WHOIS might be best, to allow those who are concerned about privacy to choose a registrar in an appropriate jurisdiction that suits their own needs.</p> <p>ICANN has long been subject to gaming, and taking this out of ICANN's hands seems best. Otherwise, various camps will do their best to create a policy that includes themselves, to gain an advantage, and to exclude others.</p> <p>Once a policy is adopted, it would be nearly impossible to change it (as seen by past policy mistakes by ICANN), as a party used to gaining an advantage eventually considers it an entitlement.</p>	George Kirikos; Leap of Faith Financial Services Inc.	<p>Divergence</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>

#	Comment	Contributor	EPDP Response / Action Taken
30.	<p>The RySG doesn't believe that the purpose of recommendations is to reiterate that work in the Charter will be done. Unless the recommendation is to 1) amend the Charter, or 2) alter the implementation of the Charter, then it should be assumed that the ePDP will address all in scope issues during its period of work.</p> <p>The RySG is committed to continuing to work with the EPDP Team on the topic of how to provide access to non-public registration data, including the consideration of the questions included in the text of Recommendation #2, once the Phase 1 work and completion of answers to the gating questions in the Charter, is complete.</p> <p>Should the EPDP see fit not to accept our recommendation to delete, then we remind the Team that the proper terminology that should be used, and as discussed by the EPDP team, is "request for disclosure" and not "access."</p>	Wim Degezelle ; RySG	<p>Divergence</p> <p>EPDP Response:</p> <p>Action Taken:</p> <p>[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]</p>
Not designated			
31.	No selection made and no additional comments submitted	<ul style="list-style-type: none"> • Farzaneh Badii; Internet Governance Project • Theo Geurts • Ivett Paulovics; MFSD Srl URS Provider • Greg Mounier on behalf of Europol AGIS; Europol Advisory Group on Internet Security • Ashley Roberts; Valideus • Renee Fossen; Forum - URS and UDRP Provider • Stephanie Perrin • Fabien Betremieux; GAC 	<p>EPDP Response: none</p> <p>Action Taken: none [COMPLETED]</p>