Early Input Categories – Table of Contents

Purposes for Accessing Data

#	Comment	Contributor	WG Response / Action Taken
(a) Purposes for Accessing Data – What are the unanswered policy questions that will guide implementation? a1) Under applicable law, what are legitimate purposes for third parties to access registration data? a2) What legal bases exist to support this access? a3) What are the eligibility criteria for access to non-public Registration data? a4) Do those parties/groups consist of different types of third-party requestors? a5) What data elements should each user/party have access to based on their purposes? a6) To what extent can we determine a set of data elements and potential scope (volume) for specific third parties and/or purposes? a7) How can RDAP, that is technically capable, allow Registries/Registrars to accept accreditation tokens and purpose for the query? Once accreditation models are developed by the appropriate accreditors and approved by the relevant legal authorities, how can we ensure that RDAP is technically capable and is ready to accept, log and respond to the accredited requestor's token?			
1.	a1) It is impossible to pre-define what legitimate purposes exist for third parties to access data. Legitimate purposes are limited to the specific circumstances of a particular request, including the type of data involved, the data elements required, the legal basis, the requestor, the purpose stated etc. The RYSG sees merit in perhaps identifying high level commonalities, however this does not mean we support a 'check box' exercise of Legitimate Purposes, where one size seems to fit all. This would be simply legally unsound. The RySG also notes that this may vary depending on the jurisdiction and who the requestor is.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
2.	a1) The answer to this question is highly dependent on who the third party is and the jurisdiction in which they operate and the jurisdiction in which other parties, including the data subject, are resident in. The NCSG does not consider it appropriate for the EPDP team to attempt to tackle this question, because the activities of third parties fall well and truly outside of our knowledge and control. We stress that simply because third parties have expressed their need to access personal information does not justify disclosure. Under the GDPR and other data protection laws and regulations,	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	the legitimate interest of the third party should be interpreted narrowly and established with a clear and specific outcome in mind. Rather, the NCSG recommends that the following questions instead be asked: ● Over the past 12 months, have the legitimate interests enumerated by third parties been used by registrars to disclose the personal information of domain name registrants? ● Do the use cases that involve third parties processing personal information provide a concrete outcome or benefit? ● Can the outcome of disclosure be achieved through other means?		
3.	a1) Determining purposes for data processing is work that the EPDP team needs to do. These purposes must follow the criteria in the GDPR, in particular they must be lawful and sufficiently narrow. The EPDP team needs to answer the policy question regarding what disclosure scenarios are eligible for a system supporting (semi) automated processing of requests based on accreditations. Only clear-cut cases are likely cases that qualify for such system, which in itself is a concept that is not foreseen in the GDPR. Processing requests to investigate, defend against or pursue civil claims with respect to trademark infringements are amongst those.	ISPCP	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	a1) Consistent with views expressed by the GAC, BC and others (including legal opinions obtained by and made available to ICANN), the IPC has long maintained that access to personal data is necessary and justified in order for right holders and their duly authorized agents and representatives, to investigate, enforce and prevent infringement of intellectual property rights. [1] --- [1] "Protecting the public in the context of the DNS requires taking into account the equally important issues of data protection and the legitimate and lawful practices associated	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	with protecting the public, including to combat illegal conduct such as fraud and infringement of intellectual property, cyber-security, promoting user confidence and consumer trust in the Internet, and protecting consumers and businesses. Prior GAC Advice and the ICANN Bylaws recognize these vital interests." See: https://gac.icann.org/briefing-materials/public/icann64-gac-briefing-whois-and-data-protection-policy-v2-8mar19.pdf		
	a2) Legal bases are limited to those identified in Article 6 of the GDPR.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
4.	ADD: e.g. does a legal right or entitlement to request and receive disclosure exist for the third party under ble law?	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
5.	Legal bases are specified in Article 6 of the GDPR. They are limited and specific, and do not apply to each requesting entity every time (a particular conflation that we have argued against multiple times). We have gone over this at some length already in the EPDP. We will not repeat ourselves here, except to stress that there is no blanket clause that can be used to create a simple, unified access engine.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
6.	There needs to be a legal basis both for disclosure as well as for requesting non-public registration data. While the EPDP team's work needs to focus on the legal basis for the disclosure, it is important also to look at the legal basis the requestor may have. disclosure, the legal basis must be taken from the catalogue in Art. 6 GDPR. It is likely only Art. 6 I c and f GDPR are applicable for the system. For the requestor, legal basis will likely be Art. 6 I f GDPR for civil claims. For public requestors, the matter is	ISPCP	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	more complex as the legal basis may vary depending on the requestor and national laws. unanswered question is whether public authorities may request data based on Art. 6 I f GDPR where there is no European or domestic legal basis that would allow for disclosure according to Art. 6 I c GDPR. This question is relevant for cross-border requests inside the EU as well as for requestors outside the EU.		
8.	a2) The protection of intellectual property is internationally recognized as a human right for the benefit of the public as well as authors and IP owners.[1] The legal bases for access include Article 6(1)(e) (public interest) and (f) necessary for the purposes of a legitimate interest), among others.[2] --- See Article 15 of the International Covenant on Economic, Social and Cultural Rights which specifies that countries that have ratified or acceded to this covenent ,"recognize the right of everyone" both "to enjoy the benefits of scientific progress and its applications" and "to benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author." The Convention underscores that protection of IP is necessary both for protection of individual as well as the public interest. See April 17 2019 Comments from the European Commission: "For instance, an IPR rightholder might have a legitimate interest to gain access to WHOIS personal data in order to ensure his/her IP right is protected and not abused. The existence of such a right needs to be substantiated and the necessity/proportionality of accessing that data ascertained. This IPR rightholder might rely on Art. 6(1) (f)."	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

7.	a3) “Access” may only be granted to those who have obtained the fully informed and freely given consent of the data subject. “Access” may also be granted to specific entities under EU law or Members State law. “Disclosure” eligibility criteria depend on the stated legal basis of the request: 6(1)a - Consent of the data subject (freely given and fully informed) 6(1)b - disclosure “necessary” to give effect to contract between the data subject and the data controller (in this instance the requestor) 6(1)c - Establishment of a legal obligation on the disclosing controller, i.e. The disclosing controller is required under an EU law / Member State law to disclose the data to a specified requestor. 6(1)d - The requester has established that disclosure is necessary to protect the vital interests of the data subject or another natural person, (NOTE: ICO guidance has confirmed that vital interest is an exceptionally high bar usually equated to immediate threat of loss of life. 6(1)e - The requester, who must verify their request is in the course of their exercising an official authority therein vested, must require disclosure for the performance of a task carried out in the Public Interest. The basis of this processing must be also established in EU or Member State law (Art 6(3)). The requester must establish necessity, legal basis and provide a valid legitimate interest for disclosure. Eligibility for disclosure is based on the receiving controller’s assessment of the request, and the review of all such requirements. The controller may only disclose where the interests and legal basis of the requester are not overridden by the competing interests, rights and freedoms of the relevant data subject, vis a vis the protection of their data.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
8.	ADD: What comparable processes exist for requesting disclosure in comparable situations?	RrSG	Concerns Divergence Agreement New Idea **WG Response:**

	For example, how would these parties obtain personal customer data from internet access providers, hosting providers, etc?		**Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
9.	This is not a precise question. A party is not by its very identity eligible or ineligible, it depends on the purpose and whether that purpose is legitimate and proportional. The purposes are described in Article 6, thus a legitimate, authenticated third party who qualifies to request under one of these purposes is "eligible". Then the request must be evaluated for scope and proportionality. We caution against using consent. Many Jurisdictions are finding that consent it difficult to manage, as individuals who data is requested are unlikely to be capable of fathoming the extent of onward transfer and use, in an age of big data.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
10.	ADD: A3.5) "What comparable processes exist for requesting disclosure in comparable situations? For example, how would these parties obtain contact details regarding property ownership or business ownership where these data are not already publicly available?"	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
11.	a3) There should be general eligibility criteria that all requestors must meet to ensure that data is not used in a manner that is incompatible with the purpose of the request. Such eligibility criteria can be found in the use case documents that have been discussed already by the EPDP team. Moreover, disclosure must only take place if additional safeguards are met. The most important one is a balancing of rights of the requestor against the rights of the data subject in anticipated balancing tests per use case. That means that disclosure must not take place where there is no substantial interest by the requestor as – in such cases – the rights of the data subject in its privacy will likely prevail. Also, disclosure must not take place where disclosure might lead to a threat of health and life of the data subject. As a consequence,	ISPCP	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	disclosure must be limited to cases where the rights of the requestor in the disclosure outweigh the rights of the data subject. Additionally, there must be eligibility criteria depend on the nature request, such as providing evidence of trademark ownership in cases related to trademark infringement of a particular mark. Finally, eligibility just encompass the acceptance of accountability mechanisms, such as documenting what requests have been made and how cases have been worked on.		
12.	a3) In order to gain access to such data, the requestor would need to demonstrate that they are acting in pursuance of the legitimate purpose of protecting intellectual property rights, such as where they are the owner of intellectual property which is the subject of enforcement, or are acting on behalf of such owner.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
12.	Eligibility is not tied to specific groups of people; eligibility is tied to the legal basis and a consideration of the elements of the individual request. There is a higher degree of viability of such a 'per group' eligibility for those legal bases which require 'official authority'. In such situations it is envisaged that there is potential that where such a legal authority / official authority is sufficiently established, the disclosing controller may not retain discretion in such a disclosure.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
13.	The disclosure of personal information to a third party requestor is variable and dependent upon the stated legal basis of the request. It is vital that the disclosing party determine the identity of the requestor, and assures that this requestor in fact represents the organization or entity that he/she purports to represent, and that the purposes for disclosure of personal data are accurately stated. Obviously, given that anyone can request access to personal data if they have a valid and legitimate purpose to request it,	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	and the DNS does have a public function and impact (as opposed to, for instance, someone requesting access to somebody else's health or financial data), there could be an infinite number of types of individuals or groups requesting access to data. We do not see the value in attempting to forecast the scope of the potential user group.		
14.	Group(s) - a user group or user groups represent a collection of entities/individuals that logically have common cause. To date, the GAC has identified, inter alia, law enforcement, cybersecurity practitioners, and intellectual property rights holders as obvious user groups that could collectively be represented by a known and eligible/recognized third party for purposes such as accreditation, developing agreements for terms of use and other vehicles that work to bring accountability and accredibility to an access/disclosure system. Simply being represented in a user group does not equate to a presumption of obtaining information.	GAC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	a4) Requestors seeking to access data for these purposes have in common that they are all acting in their interests as owners or representatives of owners, or IP. Therefore, despite the fact that there may be differences between them, such as regarding the specific IP they are enforcing, these differences are not material for the purposes of considering their access privileges.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
15.	The required data elements per request must rely upon the specific circumstances of the individual request. At a high level, we do not hold any personal data that might not be potentially released to a 3rd party who has met with the disclosure requirements. Blanket disclosure, however, cannot be permitted based on purpose alone, as necessity for the release of each data element must be established.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
16.	The data elements that would be released to a third party would depend on the nature of the specific request and would vary from case to case. The NCSG supports the	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:**

	proportionate release of personal information in justified circumstances, and would not support more personal information than necessary being shared with a third party. We note Article 6(f) requires that "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." This requires that, in appropriate cases, the "purposes" of the requestor be weighed against the danger to the data subjects (registrants), especially when their fundamental rights and freedoms are involved. We note that complexities for processing of Whois requests are likely to arise in cases involving "sensitive data" under Article 9 -- where the "processing of personal data" "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" as well as "data concerning health or data concerning a natural person's sex life or sexual orientation." Accordingly, for certain human rights, LGBTQ, minority political and religious organisational registrants, their members (often named as contacts in the Whois with their addresses) will require a more thorough evaluation prior to disclosure of data that may well impact their rights and freedoms. As discussed above, the jurisdiction of the requestor may raise issues and possible dangers. An EU resident serving as a webmaster/Whois contact/member of a LGBTQ group may also be a Nigerian or Kenyan citizen (countries where LGBTQ activities are now banned and heavily penalized). What danger exists in relation to the disclosure of data, and danger to "fundamental freedoms and rights" should the request arise in Nigeria or Kenya? Similar concerns arise in response to requests of Whois data from countries which engage in collective punishment against family members (e.g., even if		[**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	the organization's registrant is unreachable, family members might be reachable once a member's name is disclosed). The danger to minority religious and political groups by a third party in a jurisdiction hostile to that minority -- dangers of arrest, death, persecution for association with the protected organization -- would require an inquiry beyond the "stated legal basis of the request." In addition to noting this concern during this discussion of developing a UAM, we wish to note that there is very scanty information available to domain name registrants currently with respect to who has access to their personal or confidential data, and how. This needs to change drastically under the GDPR.		
17.	a5) Disclosure must be restricted to those data elements that are necessary to achieve the purpose of the requestor. This may vary from use case to use case and also include the provision of pseudonymized data.	ISPCP	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
18.	a5) Redacted Data elements: To keep the work of the EPDP at a reasonable level, the ALAC suggests that, where applicable, instead of dealing with redacted data on an element-by-element basis for each class of request any category of requester, that the data elements be grouped together based on similar characteristics and impact. Specifically, the ALAC suggests that the EPDP group fields together in 4 categories: a) Registrant Name and Organization (if redacted) b) Registrant contact fields c) Tech name and contact fields d) Other redacted fields (Registry Domain ID, Registry Registrant ID	ALAC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	a5) The data elements necessary for such requests include: name, postal address, email address, phone number (since often, this element has been verified by the registrar as accurate through two-factor authentication), organization	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:**

	name, date of registration. These elements are all justifiably necessary and proportionate for the purposes and legal basis on which the request is based.		[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
19.	It may be possible to establish sets of data elements which may be a potential 'common' set of data elements based on specific type of requestors, which have identified a particular legal basis; however under the GDPR and in particular with art 6(1)of which shall likely be the basis for the vast majority of cases, there remains a requirement on the 'disclosing' controller to carry out an assessment in any given case of whether or not the legal basis and necessity has been established in that case. This remains a vital aspect of the 'balancing test'.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
20.	ADD: How can legitimate interests/ third party purposes be matched against disclosure levels? What ards exist against misrepresentation of purposes?	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
21.	a6) ADD: To what extent, if any, are contracted parties accountable when a third party misrepresents their intended processing, and how can this accountability be reduced?	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
22.	a6) This seems to be the wrong question. First, let's figure out who the data controller/joint controllers are. Then, let's do a data protection impact assessment (DPIA) for requestors who want access routinely to certain types of data. All we have heard so far is expressions of need/desire for continued access to data, not the demonstration of that need and estimated volumes. A comprehensive DPIA and associated risk assessment will need to assess the purpose for processing personal information and what data elements, if any, are justified in such a case. The NCSG suggests that the EPDP explore these questions – of fair evaluation of the Article 6(f) proportionality	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]

	protections for the interests or fundamental rights and freedoms of the data subject prior to disclosure as well as well as safeguards against the misuse of registrant data elements – as a matter of priority. We note that ICANN's ability to enforce against misuse of registrant data elements after disclosure in a global environment will be limited and, hence, protections prior to disclosure as mandated by GDPR for personal and sensitive data must be made. A comprehensive risk assessment should be done to determine means to measure the negative impact of information disclosures.		
23.	a6) That depends on the nature of the request. There must not be strict volume limitations. Trademark infringements may occur in a high, yet finite number of domain names. Researchers may need huge amounts of data, but only pseudonymized data.	ISPCP	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	a6) The data elements necessary for such requests include: name, postal address, email address, phone number (since often, this element has been verified by the registrar as accurate through two-factor authentication), organization name, date of registration. These elements are all justifiably necessary and proportionate for the purposes and legal basis on which the request is based. Overall volume (not specific to IP) is likely to be substantially higher than today under the Temporary Specification, though probably not as high as prior to the Temporary Specification.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
24.	The technical solution must follow the policy recommendations. The technical solution should support policy, not shape or drive that policy. The RySG recognizes that various work has already been done showing that RDAP is a flexible tool likely to be able to support policy recommendations that will ultimately come out of phase 2.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
25.	ADD: What purposes will accreditation ultimately serve? : How would RDAP function in case a review process is needed for each request, e.g. as a process that is not instantaneous?	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:**

			[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
26.	the EPDP team agrees to having an accreditation model, then we can discuss the best way to implement it. First, the relying parties (i.e. the data controllers/cocontrollers, assume we are talking about the contracted parties here for the sake of brevity) need to do a risk assessment of the accreditation processes. How can they be assured that an individual who claims to be a law enforcement agent, IP attorney, accredited cybercrime investigator etc. has been reliably accredited to receive a token? We do not think that accrediting a legitimate purpose will be easy, and are looking forward to discussing this separate problem once we get there.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
27.	That is a matter of implementation and it is premature to discuss this before knowing the policy recommendations.	ISPCP	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
	a7) Much work has gone into this in the Accreditation and Access Model outlined here: https://www.ipconstituency.org/accreditation In addition to the charter questions specified in (a), the EPDP team should also consider policy around response times (e.g. SLAs).	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
28.	ADD: a8) BC Proposes that the EPDP split Purpose 2 into two separate purposes: ● *Enabling ICANN to maintain the security, stability, and resiliency of the Domain Name System in accordance with ICANN's mission and Bylaws through the controlling and processing of gTLD registration data*	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]

	• *Enabling third parties to address consumer protection, cybersecurity, intellectual property, cybercrime and DNS abuse involving the use or registration of domain names*		
29.	ADD a9) Can legal counsel be consulted to determine if the restated purpose 2 (as stated above) is possible under GDPR? If the above language is not possible, are there suggestions that counsel can make to improve this language?	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
30.	ADD a10) Could the EPDP review the approach taken by ccTLDs in the EU, with regard to the purposes identified, examples of how to inform the registrants, and other relevant info?	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
31.	ADD a11) Could ICANN summarize key aspects of the ccTLD approaches to purposes, and provide a briefing to the EPDP?	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
32.	ADD a12) Can legal analysis be provided on how the balancing test under 6(1)(f) is to be conducted, and under which circumstances 6(1)(f) might require a manual review of a request?	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
33.	ADD a13) If not all requests benefit from manual review, is there a legal methodology to define categories of requests (e.g. rapid response to a malware attack or contacting a non-responsive IP infringer) which can be structured to reduce the need for manual review.?	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
34.	Given timing and resource constraints, the IPC offers the following statement in response to the issues raised by the questions above. Specific responses to each question can be provided in due course, as necessary. Consistent with views expressed by the GAC, BC and others (including legal opinions obtained by and made available to ICANN), the IPC has long	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	maintained that access to personal data is necessary and justified in order for right holders and their duly authorized agents and representatives, to investigate, enforce and prevent infringement of intellectual property rights. [1] The protection of intellectual property is internationally recognized as a human right for the benefit of the public as well as authors and IP owners.[2] The legal bases for access include Article 6(1)(e) (public interest) and (f) necessary for the purposes of a legitimate interest).[3] In order to gain access to such data, the requestor would need to demonstrate that they are acting in pursuance of the legitimate purpose of protecting intellectual property rights, such as where they are the owner of intellectual property which is the subject of enforcement, or are acting on behalf of such owner. Requestors seeking to access data for these purposes have in common that they are all acting in their interests as owners or representatives of owners, or IP. Therefore, despite the fact that there may be differences between them, such as regarding the specific IP they are enforcing, these differences are not material for the purposes of considering their access privileges. The data elements necessary for such requests include: name, postal address, email address, phone number (since often, this element has been verified by the registrar as accurate		

[1] "Protecting the public in the context of the DNS requires taking into account the equally important issues of data protection and the legitimate and lawful practices associated with protecting the public, including to combat illegal conduct such as fraud and infringement of intellectual property, cyber-security, promoting user confidence and consumer trust in the Internet, and protecting consumers and businesses. Prior GAC Advice and the ICANN Bylaws recognize these vital interests." See: https://gac.icann.org/briefing-materials/public/icann64-gac-briefing-whois-and-data-protection-policy-v2-8mar19.pdf

[2] See Article 15 of the International Covenant on Economic, Social and Cultural Rights which specifies that countries that have ratified or acceded to this covenent ,"recognize the right of everyone" both "to enjoy the benefits of scientific progress and its applications" and "to benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author." The Convention underscores that protection of IP is necessary both for protection of individual as well as the public interest.

[3] See April 17 2019 Comments from the European Commission: "For instance, an IPR rightholder might have a legitimate interest to gain access to WHOIS personal data in order to ensure his/her IP right is protected and not abused. The existence of such a right needs to be substantiated and the necessity/proportionality of accessing that data ascertained. This IPR rightholder might rely on Art. 6(1) (f)."

	through two-factor authentication), organization name, date of registration. These elements are all justifiably necessary and proportionate for the purposes and legal basis on which the request is based. In addition to the charter questions specified in (a), the EPDP team should also consider policy around response times (e.g. SLAs).		

Credentialing

#	Comment	Contributor	WG Response / Action Taken
b) What are the unanswered policy questions that will guide implementation? b1) How will credentials be granted and managed? b2) Who is responsible for providing credentials? b3) How will these credentials be integrated into registrars'/registries' technical systems?			
1.	b) It is as of yet unclear as to the meaning of 'credentialing' in the context of disclosure. It is accepted that in certain instances, such as under the legal basis of Art 6(1)c , credentialing will be a very efficient manner in which to establish the authenticity of the request and source, and thus the availability of a specific legal power to obtain disclosure. We will, however, caution that under legal basis such as Art 6(1)f, credentialing will be useful to remove the need for the disclosing controller to verify identity, the identity of the requestor is merely one element in the balancing test. Legal basis, necessity and an assessment of all the circumstances of a specific and individual request cannot be circumvented by a credential.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
2.	b) We first need to ask what is the best way of having a harmonized disclosure policy in place, and whether or not credentialing is even necessary? We do not accept the concept of credentialing if it means a kind of access where, for instance, every law enforcement officer or IP attorney gets a token to get access to a stream of data. We acknowledge the utility of providing credentials for contact points in different agencies or governments, and in certain entities. But it is not clear that we have defined and constrained these terms closely as yet.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
3.	b) The biggest question is whether a credentialing system, which is not explicitly mentioned in the GDPR, can be made work from a legal point of view. It is therefore necessary to obtain feedback from the EDPB or the EC as soon as practically possible. This is also to get feedback whether or not such system would likely be accepted in the context of a	ISPCP	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	code of conduct according to Art. 40 GDPR. Another question to be answered, if the first one is answered in the affirmative, is how narrow the accreditation must be, i.e. whether it must be for use cases or whether one accreditation can be used for various use cases if the eligibility criteria for all those use cases are met. We would envisage that there is a central hub that conducts the administrative part of managing credentials. The vetting of requestors and the accreditation itself, however, does not necessarily have to be conducted centrally, but there can be certification authorities for different sectors, such as the trademark "community" or law enforcement, to name but two examples.		
4.	b1) Should credentialing be deemed appropriate by the working group, credentials must be based upon a well-defined system of applications, verification of applications, and continuing audit. Depending upon the weight to be afforded to the 'credential', there should be scope for suspension and censure for misuse of the credential. Credentials must not be shared by the credentialed person or entity.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
5.	b1) ADD: (including requestor demonstration of affiliation, and revocation or adjustment of credential)? NOTE: An appointed organization shall have procedures, and these procedures will vary from sector to sector and country to country. It is perhaps out of scope for the EPDP team to address the specifics; international guidance should be sought from international accreditors with experience in similar processes. Validity of a demonstration of affiliation or status should be verified by a group with appropriate ability to do so. Once credentials are granted, they should be tracked and periodically audited for continued relevance. Credentials that are no longer required should be suspended so that access is appropriately limited.	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

6.	b1) If it is determined by this working group that credentialing is necessary, and that is not a given, we will need to explore what auditing functions are required to ensure that credentials are not abused, misused, stolen, or shared with someone other than the credentialed party. Credentials must not be issued permanently but for a time-limited period with regular re-verification that the party has a need to or is authorized by an entity to request registration data. Credentials must be issued to individuals and not to entities.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
7.	b1) IPC submits that these are important practical questions. IP ownership is not complicated to verify, and therefore the simplest and most efficient means towards credentialing a requestor is self-attestation, and agreement of the requestor to abide by reasonable terms and conditions which include a representation as to the accuracy of their status as an IP owner, and their use of the data for the purposes of enforcement of the IP which they have attested they own. This can be managed through whatever entity is controller of the access system. In addition, credentialing users based on a well-defined Accreditation scheme will allow for system automation when possible. This automation will allow for a predictable process for requestors and allow responders to minimize costs.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
7.	b2) This is impossible to speculate upon at this time. Regardless, there will, however, need to be a strong legal authorization or agreement which includes adequate, indemnity and a full system of redress between the controller(s)(disclosing) and the certification body.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
8.	ADD: and managing credentials? NOTE: This may fall to ICANN, as an overseeing body already present in the industry. However, ICANN may not be able to appropriately discern if a requestor's affiliation or other group membership is valid and applicable to the situation at hand (e.g. ICANN may not have awareness about the inter-relationship between various law enforcement agencies in an unfamiliar jurisdiction). In that case, credential	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	management may need to reside with industry bodies who coordinate with ICANN to be designated as the approved credentialing group for a given industry.		
9.	b2) Who is responsible for providing ADD: and managing credentials?	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
10.	b2) It would be premature of us to respond to this question at this time. This is a big policy question. Who will take on the responsibility for vouching for the use of credentials by an entity? There is your answer, and there are many associated policy questions, such as who is auditing these processes, what is the fail rate, etc.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	b2) Credentials should be provided and managed by whatever entity is controller of the access system.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
11.	b3) This is impossible to speculate upon at this time. This may not even be necessary in a centralized solution.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
12.	b3) NOTE: This will depend on several other factors that have to be determined first. But from a high level the EPDP Team could come up with a setup where ICANN for example has a set of master credentials that connect to registries to registrars where the assumption is that the credentialing on a micro level prior is done through a system that connects to ICANN first or a web portal that connects to ICANN. If all flags are checked there it could technically in an easy manner pull the data from CP's.	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
13.	b3) We defer to the registrars and registries to answer this question. Liability hangs from the answers to b2 above.	NCSG	Concerns Divergence Agreement New Idea **WG Response:**

			Action Taken: [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	b3) The credentials themselves need not be integrated into contracted parties' technical systems. We should not assume that the contracted parties will be involved in credentialing.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
14.	ADD: b4) What process should be followed for a data controller to dispute a credential? NOTE: The controller should contact the credentialing body and provide information as to why it disagrees with the issued credential. The credentialing body should have a designated point of contact and/or process for reviewing these disputes.	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
15.	ADD: B4) The BC is aware of at least two different systems for WHOIS that have been built to address the GDPR concerns (WIPO/InfoNetworks system, and the PWC model). Can ICANN Org evaluate and prepare a summary comparison of the features/approaches of each system to inform the EPDP's work regarding what is technically feasible?	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
16.	B5) Has ICANN Org explored whether insurance or bonding can be utilized as a means of mitigating risk to the contracted parties and ICANN? If not, can ICANN explore these risk-mitigation techniques?	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
17.	ADD b4) Will there be an audit process to ensure the credentials are being managed properly by registrars'/registries and their systems? b4) What is the process for when a credential is corrupted or compromised? b5) Will log records for each credential be saved and stored? Whom will have access to these records?	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

18.	IPC submits that these are important practical questions. IP ownership is not complicated to verify, and therefore the simplest and most efficient means towards credentialing a requestor is self-attestation, and agreement of the requestor to abide by reasonable terms and conditions which include a representation as to the accuracy of their status as an IP owner, and their use of the data for the purposes of enforcement of the IP which they have attested they own. In addition, credentialing users based on a well-defined Accreditation scheme will allow for system automation when possible. This automation will allow for a predictable process for requestors and allow responders to minimize costs.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	WG Response / Action Taken
(c) Terms of access and compliance with terms of use – What are the unanswered policy questions that will guide implementation? c1) What rules/policies will govern users' access to the data? c2) What rules/policies will govern users' use of the data once accessed? c3) Who will be responsible for establishing and enforcing these rules/policies? c4) What, if any, sanctions or penalties will a user face for abusing the data, including future restrictions on access or compensation to data subjects whose data has been abused in addition to any sanctions already provided in applicable law? c5) What kinds of insights will Contracted Parties have into what data is accessed and how it is used? c6) What rights do data subjects have in ascertaining when and how their data is accessed and used? c7) How can a third party access model accommodate differing requirements for data subject notification of data disclosure?			
1.	c) As discussed above, we assume one-time access each request. If there are other assumptions, they need to be interrogated, we suggest a DPIA and complete risk assessment.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
2.	c) The answers to these questions can partially be found in the answers above. In order to answer the additional points above, we need answers to the gating questions mentioned above. One scenario is that Rys, Rrs and ICANN are joint controllers that have granted functional responsibility for the system to ICANN, so ICANN would enforce the policies. However the technical operations could be outsourced to third party acting as a processor on behalf of the joint controllers and additional certification authorities could be independent controllers. Requestors that do not follow the policies / rules, can loose their accreditation and they have to indemnify the other parties involved. In order to ensure that there is no risk of indemnification claims that cannot be enforced given the credit standing of the requestor or the jurisdiction the requestor is based in, it is possible to charge an accreditation fee, a renewal fee for accreditation, a fee per request and a security to cover penalties that needs to be paid. It is possible to structure this differently, but the idea is to make the	ISPCP	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	requestor pay for the accreditation, for the use of the system and pay into an "insurance pool" out of which the contracted parties and ICANN can finance cases where legal defense or sanctions are concerned.		
3.	c1) The EPDP Team must address the question of when the purpose associated with a given request for data disclosure (i.e., the user's reason for requesting access to that data) will be assessed. The existing RDDS query process does not currently account for the need to express and assess this data point. The EPDP Team may wish to consider if certain potential users should be excluded from participation based on prior bad conduct or conduct demonstrating an inability to properly secure personal data.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
4.	c1) NOTE: Should be only applicable laws	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
5.	c1) Foremost, applicable law. There must be an enforceable attestation that the third party will protect the data in compliance with applicable law, particularly in cases where there is no data protection law in the jurisdiction receiving the data. This includes verification that a third party requestor has the capacity to transmit and store personal information in a secure fashion. There must also be penalties and sanctions in place for third parties that request registrant data for illegitimate purposes or where it is later found to be unnecessary.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	c1) Users' access to the data should be subject to agreement to process the data in compliance with applicable law. Any rules governing the terms and conditions for access to data should be uniform and standard across contracted parties. Contracted parties shall not be permitted to alter them, unless such alteration is required by national law.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

6.	c2) At a minimum, a user to whom data has been disclosed must not (i) use that data for or in connection with any reason other than the reason provided by the user in stating its legal basis and legitimate interest; (ii) disclose that data to any other person not encompassed by the user's credential, legal basis and legitimate interest except in submissions in administrative, regulatory, or judicial proceedings; (iii) use that data beyond any time period stated as a condition of disclosure.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
7.	c2) NOTE: Should be dictated by applicable laws and best practices and be only for the original purpose.	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
8.	c2) Foremost, applicable law. Requested data must only be used for the purpose that the user stated was their reason for requesting the data, as supported by a legal basis and, if necessary, their enumerated legitimate interest. Data must not be retained beyond an agreed retention period (to be determined). The data controller needs to inform the individual concerned that his/her data have been released, in compliance with the applicable DP law.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	c2) Users' access to the data should be subject to agreement to process the data in compliance with applicable law. Any rules governing the terms and conditions for access to data should be uniform and standard across contracted parties. Contracted parties shall not be permitted to alter them, unless such alteration is required by national law. Users may contribute towards this by defining for their user group, a set of agreed norms governing their use of data following access, which can be incorporated by reference into the standard terms.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

9.	c3) It is premature to determine who will be responsible for establishing and enforcing these rules/policies, but users should not be responsible for doing so.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
10.	c3) NOTE: The question is who or what can legally enforce the rules/policies globally and how would it work? Currently the only international legal body is the Hague International Court of Justice, which is not recognized by all countries in the world. Therefore, unless the SSAD is jointly operated by governments, enforcement could be a deal breaker/show stopper. If ICANN takes on any of this liability, what guarantees do CPs get?	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
11.	c3) The data controller(s) are responsible for establishing the terms and conditions of the disclosure, in compliance with relevant law. The recipients must comply with the same provisions, regardless of jurisdiction. It is not the responsibility of the domain name registrant to police this. He/she will have access rights when the data is being held by the recipient, but it should not be simply left to the registrants to manage this.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	c3) ICANN or its designee in the role of the controller responsible for providing access should establish and enforce these terms, but only to the extent necessary to comply with the controller's legal obligations.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
12.	c4) Graduated sanctions, including prohibitions on requesting further disclosures, termination of credentials and financial penalties, should apply to users who abuse the data.	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
13.	c4) ADD: and/or data processors whose data has been abused in addition to any sanctions already provided in applicable law? ADD: How can enforceability of sanctions and payment of compensation be ensured to avoid contracted parties being left with the responsibility?	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

14.	c4) Significant financial penalties against the requesting third party, and significant financial compensation to the domain name registrant whose personal information has been misused should be considered. Other sanctions, including restrictions on further disclosure requests, may be justified.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	c4) Breach of the terms can result in consequences such as termination of access but should be proportionate and limited in accordance with the balance that must be struck between the legitimate interests of the third party and data subject. Future restrictions on access may be necessary where a third party requestor has repeatedly breached the terms and conditions of access, in a substantive and not purely procedural or technical manner.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
15.	c5) Data subjects are the customers of Contracted Parties. Contracted Parties must have full visibility into what data has been disclosed, to whom, and in furtherance of what identified interest. Establishing such an 'audit trail' is also a basic requirement under the GDPR (Art 15(1)(c)), and the relevant contracted party in this instance, must be in a position to fully inform the data subject of such a disclosure.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
16.	c5) NOTE: CPH should discuss this within their respectives SG's and supply the EPDP WG with a procedure and requirements. The data subject has a direct relationship with the CP, and so the CP needs visibility into all queries, with the ability to deny requests.	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
17.	c5) There must be a complete audit trail available to any data controller or co-controller.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	c5) We should not assume that the contracted parties are involved in the accessing of the data. In any event, neither the contracted party nor the access controller should have	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	insights into how the data is used. Visibility could increase liability for the controller, which is to be avoided.		
18.	c6) The entire basis of Data Protection law is to ensure transparency for the data subject regarding the manner in which processing of their personal data occurs. Controllers MUST be able to demonstrate to whom and for what reason any of their personal data was disclosed to any 3rd party. See Art 15, GDPR "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: … (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;"	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
19.	c6) NOTE: In general best practices should be used. Data protection law requirements and applicable law need to be complied with and could involve several different procedures. This question is very complex as there might be scenarios where LEAs request data but the data subject cannot be informed as that could compromise the investigation. As always, the LEA must follow due process, and the data subject's rights must be protected.	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
20.	c6) All rights guaranteed as per applicable law, including in particular those referenced in Article 15 of the GDPR. Data subjects must also be notified if and when their data is accessed by a third party, with a rationale offered for the disclosure of their personal information.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	c6) Data subjects should have the rights provided under applicable law. We note that some access by its nature should not be ascertainable by the data subject (e.g. investigations under seal).	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

21.	c7) The answer to this question really depends on the level of disclosure that occurs. The creation of any centralized platform for access will likely, from a privacy by design standpoint, necessitate full disclosure of the existence of such an entity whose purpose is the disclosure of registrant data to third parties. Such a notification will have to occur prior to collection of data (i.e. prior to the processing occurs). Expected disclosure on such an organized scale outside of the purpose for which the data is collected, so much so that it necessitates a separate entity to manage, is exceptionally rare and is frankly unusual (this is as opposed to those registers which find a basis in law e.g. company registers, register of directors, electoral registers).therefore the RySG would recommend, if not insist, that any disclosure made via a centralized platform should always be notified to the data subject.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
22.	c7) NOTE: As we have little to no experience with this, it is best that at first everything is manually evaluated. At a certain point automation can kick in. This approach, while possibly labor intensive at first, at least gets the project going as opposed to trying to automate and predict the unknowns, which usually stalls entire projects. Also new technology might emerge during the operational phase which cannot be predicted by the WG.	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
23.	c7) Exemptions to the disclosure requirements are routinely managed by countries with data protection law; we can figure this out when we get there. Research is being done on secure untraceable requests, but the rationale for such secure untraceable requests is very restricted in use. It would be premature for us to respond further to this question.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
	c7) The unified access model should facilitate cases with differing requirements for data subject notification, such as investigations under seal.	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

24.	ADD: c8) What requirements, if any, should be implemented to processing of disclosed data by third (security, deletion timeframes, prohibitions on further transfers, etc)?	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
25.	n legal counsel be consulted to determine whether GDPR prevents higher volume access for properly credentialed cybersecurity professionals, who have agreed on appropriate safeguards? If such access is not prohibited, can counsel provide examples of safeguards (such as pseudonymization) that should be considered?	BC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
26.	ADD: c8) Will data subjects have access to logs of users that have requested access to their own data and seek clarification as to how their data is being used? If so, to whom will these users seek this data? c9) Wholesale focused Registrars, how will they manage contracted Resellers' access and purposes associated with WHOIS data access and elements under their separate and unique Registrar to Reseller contracts? c10) Will an ICANN audit process being created in order to ensure contracted parties are complying with their new responsibilities?	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
27.	Any rules governing the terms and conditions for access to data should be uniform and standard across contracted parties. Contracted parties shall not be permitted to alter them, unless such alteration is required by national law. Users may contribute towards this by defining for their user group, a set of agreed norms governing their use of data	IPC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

	following access, which can be incorporated by reference into the standard terms. Breach of the terms can result in consequences such as termination of access but should be proportionate and limited in accordance with the balance that must be struck between the legitimate interests of the third party and data subject. Future restrictions on access may be necessary where a third party requestor has repeatedly breached the terms and conditions of access, in a substantive and not purely procedural or technical manner.		

Annex: Important Issues for Further Community Action

#	Comment	Contributor	WG Response / Action Taken
1. Pursuant to Section 4.4, continuing community work to develop an accreditation and access model that complies with GDPR, while recognizing the need to obtain additional guidance from Article 29 Working Party/European Data Protection Board. 2. Addressing the feasibility of requiring unique contacts to have a uniform anonymized email address across domain name registrations at a given Registrar, while ensuring security/stability and meeting the requirements of Section 2.5.1 of Appendix A. 3. Developing methods to provide potential URS and UDRP complainants with sufficient access to Registration Data to support good-faith filings of complaints. 4. Consistent process for continued access to Registration Data, including non-public data, for users with a legitimate purpose, until the time when a final accreditation and access mechanism is fully operational, on a mandatory basis for all contracted parties. 5. Distinguishing between legal and natural persons to allow for public access to the Registration Data of legal persons, which are not in the remit of the GDPR. 6. Limitations in terms of query volume envisaged under an accreditation program balanced against realistic investigatory cross-referencing needs. 7. Confidentiality of queries for Registration Data by law enforcement authorities.			
1.	1) NOTE: The WG should bring itself up to speed with the latest/final version of the Guidelines on Certification, following public consultation of Annex 2. Which is available at the EDPB website: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en	RrSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
2.	NCSG believes that the contracted parties should be permitted to differentiate between legal and natural persons if they so desire, but they should not be obliged to do so, as it is unfeasible in many circumstances.	NCSG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

Items deferred from phase 1

#	Comment	Contributor	WG Response / Action Taken
a. Feasibility of unique contacts to have uniform anonymized email address b. Legal vs. Natural persons c. Additional purpose for ICANN's OCTO d. Display of information of affiliated vs. accredited privacy / proxy providers e. City Field f. Data Accuracy and the WHOIS Accuracy Reporting System			
1.	a) The RySG maintains its viewpoint that an anonymized email address continues to be both an email address and personal data. Creation of an 'anonymized' address therefore does not really create any additional protection for the data subject, merely creates an additional responsibility to protect a new element of personal data, that was created by us. As such the RySG is opposed to this unnecessary endeavor, as it does not solve, it merely compounds the matter.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
2.	b) The RySG maintains its support for the first part of Recommendation #17 from Phase 1 and believes that Registrars and Registry Operators should continue to be permitted to differentiate between registrations or legal and natural persons, but not be obligated to do so.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
3.	c) During Phase 1 of the EPDP, ICANN specifically stated that OCTO does not presently require or use personal registration data in its research. The RySG reiterates the comment it made on the Phase 1 draft Final Report, where we noted that the EPDP Team's inclusion of a Purpose for potential future uses of personal data by OCTO would directly contradicts GDPR requirements that Purposes not be speculative. We believe this matter should be given a very low priority in the Phase 2 work.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
4.	c) For OCTO (Office of the Chief Technology Officer), subject to requirements to keep data confidential, OCTO should have access to any data it requests for research and threat analysis.	ALAC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:**

	If ICANN were a typical data controller, it would automatically have such data without any further consideration.		[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
5.	d) There is neither sufficient delineation nor detail in the use of P&P providers to ensure that the CPHs are not knowingly facilitating personal data breaches. There is no uniformity in the data elements that are populated as a result of the use, by a data subject, of a P&P service. Some instances rely on anonymized outputs (e.g. privacycustomer87687634@Privacy.com) whereas some rely on a generic and single contact. (e.g. Privacyprovider@provider.com). There remains no manner in which all such contacts may be 'published' as to do so would be to knowingly invite breach. The RySG reiterates our position that this is a matter for a separate PDP or similar to remedy, and not for the EPDP to encroach upon. Such a PDP may then, as necessary with Privacy by default and design in mind, create or impose a system to ensure such an option of publication can be achieved without a high potential for personal data breach.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
6.	e) The RySG, noting the legal opinion of Bird & Bird, accepts that there is a heightened risk in the publication of the 'City' field, and would be supportive of redaction until such a time as the risk is lessened.	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
7.	f) The RySG would like to note that data accuracy and the WHOIS Accuracy Reporting System are completely separate matters. With regards to the data accuracy (as is referred to Art 5(1)d), we defer to and accept the legal opinion of Bird & Bird, and note that the concept of accuracy under the GDPR is that data must be accurate for the purpose to which such data are to be used, and methods to ensure "accuracy" must be commensurate to that use and purpose, including whether or not the accuracy of the data has a noted impact on the data subject's rights, thus, necessitating a higher degree of	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]

	verification. In the domain industry, as agreed by Bird & Bird, the use for the data is to ensure contactability. Bird & Bird have concluded that the required verification steps upon registration and the annual requirement to re-verify contact data ensure ongoing contactability. Unless there are specific limitations as to the class of registrants (eg. certain TLD eligibility requirements), where registration is dependant on a heightened degree of verification, then the expected level of accuracy for the registration (i.e. contactability of the registrant) is met. Where contactability is not established, then there is a process for requiring update, and a consequence (suspension) for a failure to do so. The RySG reminds the EPDP that accuracy of data subject data, is as per the instruction of the data themselves. Should a data subject express to the controller that data held is inaccurate, then under the right to rectification (also Art 5(1)d), then the controller must ensure that the data held is updated to reflect the instruction of the data subject. We do not retain any additional or heightened expectations of 'accuracy' as is claimed by some members.		
8.	For the questions remaining from Phase 1, our previous comments stand.	ISPCP	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

Additional Input

#	Comment	Contributor	WG Response / Action Taken
1.	Design and implementation of standardized, centralized model must be cost neutral for Contracted Parties. Users of the model must bear some costs for using the model. The RySG believes that any standardized model must be legally compliant and not place a significant operational burden on Contracted Parties. The RySG acknowledges the necessity of some level of automation but believes it will not be possible to develop a fully automated model that is legally compliant. It is worth noting that not all automation has to be on the "back end" of responses to requests. Opportunities exist for automation on the front end that can help the disclosing party process requests more quickly or efficiently. We must also note that the creation of a centralized model is not a legal requirement for any contracted party. As controllers, we have legal obligations to meet with regards to data protection and we undertake to meet our legal obligations, lest we are censured by the proper authorities. The RySG are engaging in this process in utmost good faith, so as to attempt to make to process more streamlined and predictable for the community as a whole. We will not however merely accept any situation whereby we are forced to accept a system, where we have reason to believe that such a system only serves to unnecessarily heighten our liability, for the 'ease' of others. We also remind the EPDP team that our goal is to establish a process which is compatible with the law. The existence an indemnity as a 'cushion' against potential illegal action is not an acceptable result. Any contractual obligation which may be agreed c between the contracted parties and ICANN Org, must remain, at a minimum, compatible with applicable law, lest it be rendered unenforceable. The RySG will continue to strive in good faith towards the creation of such a system, but	RySG	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]

	where such a system is not legally possible, we may have to accept that such a system may not be ultimately recommended by the team.		
2.	The ALAC is not in a position to provide detailed guidance on the specific issues to be addressed during phase 2 in response to this consultation. Our previous applicable statements still stand and the ALAC and its representatives on the EPDP of course reserve the right to provide input and comment as the work progresses.	ALAC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
3.	Access vs. Disclosure - the GAC has historically used the word "access" versus "disclosure" simply because that is a term that has been used when third parties want to "access" information. Even more plainly, when a party wants something, they will use the term that most accurately reflects their need (ie: getting access to information) and not the action taken by another party (disclosing the information). There is no other meaning or motivation behind the GAC's use of the word "access." Specifically, using the term "access" is not intended to presume access to a complete data set or to data for a period of time beyond that of the associated specific legitimate request. However, in recognition of others concerns around the use of "access," the GAC may consider using the term "disclosure" for the sake of broader discussions moving forward provided that making such request is understood as a privilege of the requesting third party even though actual disclosure is subject to adherence to GDPR .	GAC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
4.	Unified Access Model (UAM) - the GAC does not attribute this term to any specific model, but rather views it as a catch all term for any model that is streamlined, standardized, and unified. The GAC's already stated support and expectation for a UAM is based on our assumption that it would be the most efficient approach.	GAC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
5.	Centralized - the GAC uses this term to denote a single access point for directing and receiving responses to information requests. However, should that centralized access point be ICANN Org, there needs to be appropriate accountability	GAC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:**

	measures put in place for ICANN Org to the ICANN Community.		[COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
6.	Accreditation - the GAC views this as a critical component to an access/disclosure model whereby parties linked by common cause can be "accredited" by a known and eligible/recognized third party. The accreditation provider would be responsible for managing and policing the groups of entities/individuals it accredits for purposes of providing rigor and accountability on the requestor side of the house. By no means does the GAC equate accreditation with automatic or assumed access to disclosed information.	GAC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]
7.	The GAC is of the view that there remain a number of outstanding policy issues regarding user groups, purposes, and legitimate interests - including making sure we are as the EPDP being consistent in how we use these terms and discuss them. Further, it is worth noting here that the GAC has on numerous occasions recognized law enforcement, cybersecurity and intellectual property rights enforcement as legitimate interests and we hope these will be quickly and effectively be recognized in the work of the EPDP. The GAC emphasizes that any kind of misuse of a UAM shall be prevented by inclusion of necessary safeguards in the system.	GAC	Concerns Divergence Agreement New Idea **WG Response:** **Action Taken:** [COMPLETED / NOT COMPLETED] – [Instruction of what was done.]