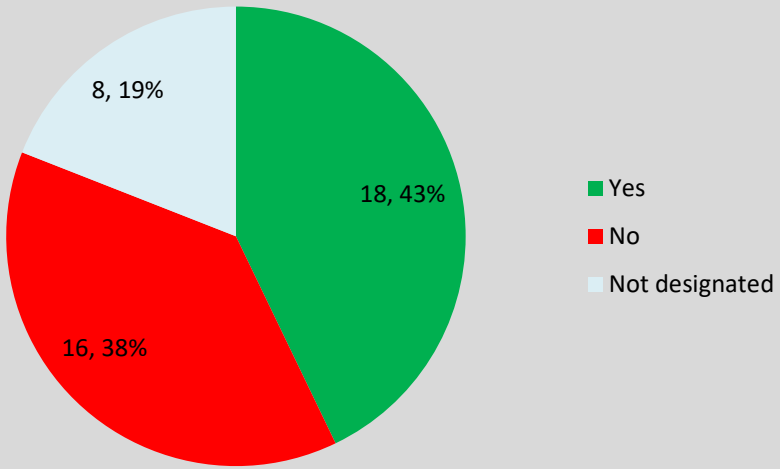
RECOMMENDATION 8 – Redaction

#	Comment	Contributor	EPDP Response / Action Taken

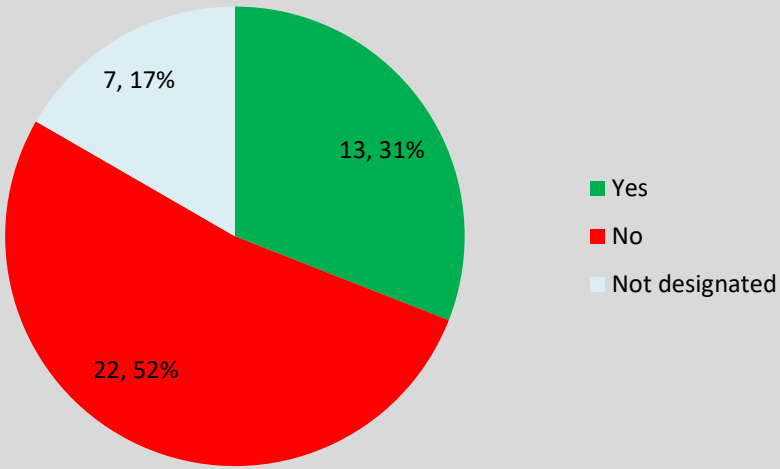
The EPDP Team recommends that redaction must be applied as follows to the data elements that are collected. Data elements neither redacted nor anonymized must appear in a freely accessible directory.

Refer to bottom of this document for the list of data elements Not Redacted / Redacted.

Do you agree that all of these data elements should be redacted?



The EPDP Team is of divided opinion as to whether "Organization" should be redacted for reasons stated in the Initial Report. Please see the Initial Report, beginning on p. 42. Should the "Organization" field be redacted?



#	Comment	Contributor	EPDP Response / Action Taken
Yes data elements redacted	**Yes Organization should be redacted**		
1.	No comments provided in support of this recommendation	Domain.com, LLC & affiliates	Support **EPDP Response:** The EPDP appreciates the support **Action Taken:** none [**COMPLETED**]
2.	RE: Organization: yes, yes, a thousand times yes. Organization should not be visible. Many people operate small organizations, home-based businesses. Mom-owned business, and hobby, research and educational groups from their homes, and the contact data in their domain registration is indistinguishable from that of an individual residence (because it is an individual resident!). Also, some organizations that are not doing anything illegal might be targeted merely because of their legal political, religious, or social affiliations (and these groups, as noted below, and those who work for them), are specially protected by the GDPR as noted in other parts of this comment. Combining the "Organization" field with others fields, including state or city would certainly make a domain name registrant more identifiable and more targetable.	A. Mark Massey; Domain Name Rights Coalition	Support **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
3.	The RySG supports the recommendation that the fields designated in Recommendation 8 should be redacted in the registration data directories that Contracted Parties are required to operate. However, the requirement to publish the remaining data elements in a "freely accessible directory" raises concerns for the RySG given the open-ended and imprecise nature of the language. The RySG proposes changing this language to "appear via free public based query access." Further, the RySG recommends refining Recommendation 8 to include a provision that, in the event a Contracted Party collects additional data elements not included in the list enumerated in the recommendation, the Contracted Party should be permitted to redact those data elements, at its discretion RE: Organization: The RySG notes that there are a great many instances where the Organization field of a domain registration record contains personal data of natural persons, such as the name of registrant. There is no way for Contracted Parties to understand the Registered Name Holder's intention or motivation behind inputting this type of data in such cases. Given the hundreds of millions of existing domain registrations, requiring contracted parties to publish the Organization field in publicly accessible domain registration databases would inevitably result in the publication of personal data that could result in violations of the GDPR. At this point in time, Contracted Parties cannot rely on domain registrants to only provide the names of legal organizations, rather than personal data, in the Organization field. The RySG understands that the EPDP is seeking additional legal guidance on this topic, and once that guidance is received, we may be willing to revisit this position. However, at this time, the RySG believes that the policy should allow registries to take a conservative approach to compliance by allowing the Organization field to be redacted.	Wim Degezelle ; RySG	Support **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
4.	RE: Organization: The "Organization" field should not only be redacted but DELETED as I have already addressed previously above. The "Organization" field should be deleted as redundant, unnecessary, confusing, and duplicative. The correct and accurate "name" of the "registrant" of facebook.com is Facebook, Inc. NOT "Domain Admin" or some other "anonymized" fictional title of an otherwise nameless person or entity. When the registrant is an organization, the name of the organization should go in the data field "Registrant Name."	John Poole; Domain Name Registrant	Support **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
5.	This question is badly designed. We select "yes" because we think these data must be redacted but, in addition, that MORE data elements should be redacted beyond what are listed here: Organization, State, and Country should also be redacted; there are NO data elements that need to be publicly displayed. The data can be provided to those third parties with a legitimate legal basis to access it without publicly displaying these fields. RE: Organization: In a sampling of the Organization field for registrations sponsored by our family of registrars, we found that the Organization field is most likely to match the registrant name or be completed with placeholder data (such as "NONE" or "—"). We did not find substantial indication that it was useful to determine the status of the registrant as either a natural or legal person. As such, using its to existence attempt to determine the status of the registrant is inappropriate and displaying the data it may contain risks revealing personal data. It should be redacted by default.	Tucows Domains Inc.	Support **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
6.	RE: Organization: In a perfect environment registrant org would not be redacted. However, because there is 20+ years of legacy WHOIS data in circulation that was obtained (often in violation of WHOIS terms of use), resold, and archived, the registrant org field is being used as an "index" to match redacted records to unredacted archives. Because of this ability to indirectly identify subjects, many of whom may be nature persons, we believe the existence of these archives means we must treat registrant org as personal data.	Sara Bockey; GoDaddy	Support **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
7.	RE: Organization: Registration of domain names is carried out using many different systems, business models etc., there is a very high risk that personal information is in the org field, as there has never been any real validation of what was being put in it.	Michele Neylon; Blacknight Internet Solutions Ltd	Support **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
8.	RE: Organization: ORGANIZATION: The publication of the ORGANIZATION field would be possible only if it did not contain personal data relating to private individuals. Regretfully, this is usually not the case as registrants have put that field to various non-intended uses, not the least of which is the repetition of the first and last name fields. Further, certain organizational structures of legal entities contain personal information in the name of the entity and while such data would not be protected under the GDPR as the entity name, the personal data contained therein would be protected. As the possibility of unintended publication of personal data could not be prevented in case of publication of the ORGANIZATION field, contracted parties need to be able to determine on their own whether they need to redact this field. Additionally, because there is 20+ years of legacy WHOIS data in circulation that was obtained (often in violation of WHOIS terms of use), resold, and archived, the registrant org field is being used as an "index" to match redacted records to unredacted archives, leading to the ability to indirectly identify data subjects, many of whom may be natural persons. We therefore propose that the redaction of this field be optional.	• Zoe Bonython; RrSG • Volker Greimann; Key-Systems GmbH	Support **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
9.	The NCSG requests the redaction of an additional data element: the State/Province field. RE: Organization: Many natural persons operate small organizations or businesses and contact data in their domain registration will be indistinguishable from that of an individual residence. Also, some organizations might be targeted merely because of their legal political, religious, or social affiliations. Legal advice provided to the GNSO Next-Generation RDS to replace WHOIS PDP Working Group explained that any data element that assists in making a natural person (RNH) identifiable, in conjunction with other data elements, should be treated as personal information, even if the data element does not appear to be personal information in itself. Combining the "Organization" field with others such as state or city would certainly make a Registered Name Holder more identifiable.	Ayden Férdeline; NCSG	Support Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
10.	RE: Organization: There is consensus that the registrant field shall be redacted. As the registrant field is populated with the same data as the organization field, it is only straightforward also to redact the organization field. This issue is closely linked to the distinction of natural and legal persons. If and when a compliant way to make a distinction between natural and legal persons can be found, the organization field can be published where no personal data is revealed. However, such mechanism does not exist (yet).	• Wolf-Ulrich Knoben; ISPCP Constituency • Lars Steffen; eco – Association of the Internet Industry	Support **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
11.	RE: Organization: Many natural persons operate small organizations or businesses and contact data in their domain registration will be indistinguishable from that of an individual residence. Also, some organizations that are not doing anything illegal might be targeted because of their political, religious or social affiliations.	Farzaneh Badii; Internet Governance Project	Support **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
Yes data elements redacted		**No Organization should not be redacted**	
12.	RE: Organization: GDPR clearly states that it is not applicable to Legal persons. So clearly, Organization field signifying a legal entity should not be redacted. However, it should be clearly mentioned/ advised to Registrant by Registrar at the time of Registration to avoid putting name of an individual (natural person) in Organization field.	DR. JAIDEEP KUMAR MISHRA ; DIRECTOR MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA	Support Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
13.	RE: Organization: Further guidance should be south from rNH.	Monica Sanders; i2Coalition	Support Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
14.	No comments provided in support of this recommendation or opposition to Organization redaction	Etienne Laurin	**EPDP Response:** The EPDP appreciates the support **Action Taken:** none [**COMPLETED**]
15.	RE: Organization: There are a number of reasons it should not be redacted. - For web sites (and other Internet resources) that are nominally commercial, Internet users should have SOME ability to know who is behind it (or if it is being hidden by Privacy/Proxy). Without the Organization field, there is NOTHING. - It is possible that the EPDP recommendations may allow all registrants to be treated as EU Natural Persons with significant redaction. - The Temp Spec has required the Organization filed to be displayed and there has not been any evident major issue about it. - It is an OPTIONAL field to fill in and Registrants can be warned that it will be displayed if filled in. So there is no reason to NOT display it.	Evin Erdoğdu; ALAC	Support Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
16.	It is essential to protect the privacy of the customer RE: Organization: It is not personal data	David Martel	Support Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
No data elements redacted		**Yes Organization should be redacted**	
17.	No submissions contained no support of redaction, but supported redaction of the Organization field.	none	**EPDP Response:** No submissions contained no support of redaction, but supported redaction of the Organization field. **Action Taken:** none [**COMPLETED**]

#	Comment	Contributor	EPDP Response / Action Taken
No data elements redacted	**No Organization should not be redacted**		
18.	No. Registrant Email and City should not be redacted Because time often is of the essence during security and law enforcement investigations, there must be an immediate method for contacting domain registrants that is more precise and affirmative than a web form or anonymous link. Unfortunately, experience with registrars following implementation of the Temp Spec (and further previous experience with Privacy/Proxy services) confirms that responsiveness to reveal requests is slow and unpredictable at best and entirely absent at worst. Email addresses, especially for Legal Persons, do not have to reveal personal data. The BC believes that, in order to serve the investigatory needs of law enforcement, security authorities and brand protection interests, registrars should, at a minimum, provide a uniquely hashed email string. In addition, the EPDP Charter (Part 1(f)) relates to publication of data. Registrars should give registrants the option to opt in to having their WHOIS Contact Data published rather than be redacted. The Temporary Specification 7.2.1/ Appendix C – Section 2.3 contains this requirement: As soon as commercially reasonable, Registrar MUST provide the opportunity for the Registered Name Holder to provide its Consent to publish the additional contact information outlined in Section 2.3 of Appendix A for the Registered Name Holder. Legal entity registrants such as corporations should not have any WHOIS data redacted. Natural person registrants may wish to display their information to ensure that their customers can confirm the authenticity of their website and prevent phishing and other impersonations. Domain owners may wish to be easily contactable in order to solicit interest in secondary market sales of their domain names. Enabling the consent feature is consistent with the accountability principles laid out in GDPR. RE: Organization: No. An Organization by definition refers to a Legal Person, and Legal Persons are exempt under GDPR and most other national privacy laws. No registrant data collected for a Legal Person should be redacted. The Registrant Organization field is included in the Temp Spec, as it should be, and it is the duty of parties to demonstrate that it should be redacted, not the reverse. (This was established in the email of Nov 19 in which ICANN responded to this very question by confirming the legal standing of Registrant Organizations under Article 6(1)(f).)	Steve DelBianco; BC	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
19.	Email fields should not be redacted. Organization Field should not be redacted. City should not be redacted. Privacy / Proxy data should not be redacted. The registration of a legal person registrant should not be redacted. Please note that our responses assume that processing shall be lawfully disclosed to the registrant at the time of data collection. Email addresses are important for both identifying and contacting registrants in the normal course of business, and not only during investigations. Registrants have the easy ability to create a new email address at no cost for the purpose of registrant communication which does not reference the registrant's name (if a natural person) or other personal identifiers. Organization names provide additional means for identifying and contacting registrants when the other fields are unreliable and is also indicative that the registrant is a legal person. Since organizations are not covered by GDPR, Organization fields should not be redacted anyway. The City field is used in resolution cases where determination of jurisdiction is needed to identify proper venue for litigation and understand which controlling law and procedure applies. Several states contain multiple districts with differing law and procedure. Proxy data is the data of a legal person (the proxy provider) and should never be redacted. Data which is redacted requires requests for disclosure. This impedes the normal course of business, and adds delay to investigations where time may be of the essence. In some cases, contact for Notice of Process is required; in some other investigations (and not just collaborations with law enforcement), it is sometimes best not to disclose to the registrant that they are being investigated, and over-redaction impedes this. Web forms are not an effective method to replace email addresses. When using a web form, there is no assurance that mail was transported to the contact, that it was received into the target mailbox, or that it was read. At minimum, a registrar must provide an account-level anonymized email address, consistent for all registrations by that registrant at that registrar, rather than a web form. Account-level anonymized identifiers have been investigated by SSAC and other parties and should be considered. See https://www.icann.org/en/system/files/correspondence/jevans-to-marby-et-al-04jun18-en.pdf for one such example. The effectiveness of email for contactibility cannot be overstated. As mentioned elsewhere, civil action requires proof of Notice. It is often the case that a bad actor will enter various inaccurate registrant data in order to resist detection, yet submit a working email address, if for no other reason than to use the notice presented to that email address as a trip wire alerting them to the need to start deleting accounts or otherwise covering their tracks. Note that an account-level anonymized email specific to a single registry or single registrar, though better than a web form, is still not as effective for contacting or identifying bad actors as a DNS-wide anonymized identifier applicable to all registrations by a registrant across all registrars. Such a DNS-wide anonymized identifier has also been discussed by SSAC and other parties and should be considered. In response to arguments that anonymized email addresses are also personal data which can be used to identify a data subject when combined with other data, and which therefore must also be redacted: GDPR does not require absolute anonymization, and we assert that pseudonymized email addresses satisfy the requirements of the GDPR. RE: Organization: Since organizations are not covered by GDPR, Organization fields should not be redacted.	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	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
20.	Registrant email address should not be redacted. City should not be redacted. Email has been recognized as most important data element for law enforcement as well as DNS abuse, consumer protection, and IP rights violation investigations. In the balance of privacy and other rights and interests, it is appropriate that this data element remain unredacted and publicly accessible. This is particularly the case because a registrant has the ability to create, at no cost, an email address that contains no personal data, such as the registrant's name. We recommend that in addition to the registrant's email address remaining unredacted, that registrars inform registrants that their email address will not be redacted, will be publicly accessible and that the registrant may create a valid e-mail address for purposes of registering the relevant domain name which email address contains no personal data. The disclosure of a registrant's email address in a public WHOIS system is essential for the legitimate purpose of expeditiously contacting the registrant in case of possible infringements or illegal actions. The email address serves as a prime data point for both notifying a potential victim and communicating with a potential infringer in an objective manner without necessarily identifying the domain name holder. The legal basis of article 6.1 (f) GDPR and the corresponding balancing exercise favour the rights and interests of several third parties, including law enforcement, commercial entities and intellectual property rights holders. The publication of the email address has a limited impact on the registrant. A registrant always retains the ability to register a domain name with an unidentifiable email address (example: info@organisation.com). There are numerous free email address providers available and a registrant may even opt to use a privacy or proxy service when registering the domain name. Additionally, at the registration of a domain name, a registrant is (and can always be) sufficiently informed about the publication and possible further use of essential "personal" information. In this regard, the data subject will have reasonable expectations that this information will be accessible in relation to the registered domain name. The risk for the registrant receiving unsolicited emails cannot outweigh the accountability and transparency necessary when operating a website or email address related to a domain name. Masking the email address of registrants unduly restricts the protection of consumers, and enforcement of intellectual property and commercial rights and prevents parties from amicably settling disputes related to potential online infringements. Should it be considered that the registrant's privacy interest in keeping his (freely chosen) email address hidden overrides the provided legitimate third party interests, than at least an effective and standardised policy for replacing the email address with a pseudonymised email must be implemented. A pseudonymised email address would redact any information potentially identifying the registrant by providing a unique registrant-specific replacement email address which is non-identifiable. Taking into account the balancing exercise of article 6.1 (f) GDPR, such pseudonymisation, together with the limited impact on the data subject, would tilt the balance sufficiently in favour of the legitimate third party interests for having a reliable measure of contact which can be associated to multiple domain names belonging to the same owner. [Please refer to Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC of the Article 29 Working Party (currently the European Data Protection Board), p. 42-43.] Further, pseudonymising consistently across registrars in such a way that enables connecting registrants for research and dispute resolution expediency would prove prohibitively difficult. Web forms do not provide the same evidence of delivery as can be established by sending an email in the absence of subsequently receiving a "bounceback," and web forms can impose unreasonable and unrealistic character limits. City is needed to serve legal process, identify proper venue for litigation, and understand which controlling law and procedure applies. For example, "San Francisco" would indicate that controlling precedent and procedure from the Northern District of California might apply to litigation concerning the domain name, where "San Diego" would indicate that completely different law and procedure from the Southern District of California would control. RE: Organization: GDPR is only to be applied as written to natural persons, not legal persons. To redact an organization name is not at all required or supported through application fo the GDPR. This is extremely valuable information to identify or contact the legal owner of the domain or to track abusive behavior by or against persons and entities, including against the RNH. When, in rare instances, and organization name includes personal data, such as a natural person's name, the person, in securing a license to do business under that name has provided clear consent in the use of that organization as a non-personal identifier. Redacting the "organisation" field in the public WHOIS would not only go beyond the GDPR remit, it would go against other important EU regulatory frameworks related to (online) accountability and transparency of businesses and e-commerce in the EU. Article 5 of Directive 2000/31/EC on electronic commerce for example requires that online service providers shall render easily and permanently accessible the following information: (i) their name, (ii) their geographic address, (iii) their contact details, including their electronic email address, (iv) their trade or commercial register number, etc. According to article 46 of Directive 2017/1132/EU relating to certain aspects of company law, Member States are also required to disclose the particulars of company officers in central national company registers. This personal data is specifically considered to be of public interest and may be accessed by any third party. The organisation field normally does not contain any personal information as it pertains to legal entities to which the GDPR is not applicable. In the rare cases that the organisation reflects the name of an identifiable natural person, this person is required by EU law to disclose his (personal identifying) company information anyway according to EU law. Redacting the organisation field would therefore go against other EU regulatory frameworks while not being necessary under the principles and obligations of the GDPR.	Brian King; MarkMonitor, Inc., a Clarivate Analytics company	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
21.	City should not be redacted City needed in order to serve legal process and city not a sensitive personal data element Email has been recognized as most important data element for law enforcement as well as DNS abuse, consumer protection and IP rights violation investigations. In the balance of privacy and other rights and interests, it is appropriate that this data element remain unredacted and publicly accessible. This is particularly the case because a registrant has the ability to create, at no cost, an email address that contains no personal data, such as the registrant's name. We recommend that in addition to the registrant's e-mail address remaining unredacted, that registrars inform registrants that their e-mail address will not be redacted, will be publicly accessible and that the registrant may create a valid e-mail address for purposes of registering the relevant domain name which e-mail address contains no personal data. Email: The disclosure of a registrant's email address in a public WHOIS system is essential for the legitimate purpose of expeditiously contacting the registrant in case of possible infringements or illegal actions. The email address serves as a prime data point for both notifying a potential victim and communicating with a potential infringer in an objective manner without necessarily identifying the domain name holder. The legal basis of article 6.1 (f) GDPR and the corresponding balancing exercise favour the rights and interests of several third parties, including law enforcement, commercial entities and intellectual property rights holders. The publication of the email address has a limited impact on the registrant. A registrant always retains the ability to register a domain name with an unidentifiable email address (example: info@organisation.com). There are numerous free email address providers available and a registrant may even opt to use a privacy or proxy service when registering the domain name. Additionally, at the registration of a domain name, a registrant is (and can always be) sufficiently informed about the publication and possible further use of essential "personal" information. In this regard, the data subject will have reasonable expectations that this information will be accessible in relation to the registered domain name. The risk for the registrant receiving unsolicited emails cannot outweigh the accountability and transparency necessary when operating a website or email address related to a domain name. Masking the email address of registrants unduly restricts the protection of consumers, and enforcement of intellectual property and commercial rights and prevents parties from amicably settling disputes related to potential online infringements. Should it be considered that the registrant's privacy interest in keeping his (freely chosen) email address hidden overrides the provided legitimate third party interests, than at least an effective and standardised policy for replacing the email address with a pseudonymised email must be implemented. A pseudonymised email address would redact any information potentially identifying the registrant by providing a unique registrant-specific replacement email address which is non-identifiable. Taking into account the balancing exercise of article 6.1 (f) GDPR, such pseudonymisation, together with the limited impact on the data subject, would tilt the balance sufficiently in favour of the legitimate third party interests for having a reliable measure of contact which can be associated to multiple domain names belonging to the same owner. [Please refer to Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC of the Article 29 Working Party (currently the European Data Protection Board), p. 42-43.] Further, pseudonymising consistently across registrars in such a way that enables connecting registrants for research and dispute resolution expediency would prove prohibitively difficult. Web forms do not provide the same evidence of delivery as can be established by sending an email in the absence of subsequently receiving a "bounceback," and web forms can impose unreasonable and unrealistic character limits. Finally, the IPC notes the letter from Dave Jevans to Göran Marby, Cherine Chalaby, and Rod Rasmussen sent on June 4, 2018 [https://www.icann.org/en/system/files/correspondence/jevans-to-marby-et-al-04jun18-en.pdf] that recommends "replacing plain text point of contact details with consistently hashed values, rather than redacting those POC details altogether. Consistently hashed values would allow an investigator or research to search registration data sets and to associate multiple domains that use the same POC details, while not disclosing the original POC data of a potential GDPR data subject." We believe this, and similar mechanisms, should be explored more thoroughly and encourages SSAC to review and comment on the viability and utility of the proposal as a replacement for redaction. City is needed to serve legal process, identify proper venue for litigation, and understand which controlling law and procedure applies. For example, "San Francisco" would indicate that controlling precedent and procedure from the Northern District of California might apply to litigation concerning the domain name, where "San Diego" would indicate that completely different law and procedure from the Southern District of California would control. RE: Organization: The GDPR is only to be applied as written to natural persons, not legal persons. To redact an organization name is not at all required or supported through application of the GDPR. This is extremely valuable information to identify or get in touch with the legal owner of the domain or to track abusive behavior by or against persons and entities, including against the RNH. When, in rare instances, and organization name includes personal data, such as a natural person's name, the person, in securing a license to do business under that name has provided clear consent in the use of that organization as a non-personal identifier. This is clearly stated in Recital 14 of the GDPR. Redacting the "organisation" field in the public WHOIS would not only go beyond the GDPR remit, it would go against other important EU regulatory frameworks related to (online) accountability and transparency of businesses and e-commerce in the EU. Article 5 of Directive 2000/31/EC on electronic commerce for example requires that online service providers shall render easily and permanently accessible the following information: (i) their name, (ii) their geographic address, (iii) their contact details, including their electronic email address , (iv) their trade or commercial register number, etc. According to article 46 of Directive 2017/1132/EU relating to certain aspects of company law, Member States are also required to disclose the particulars of company officers in central national company registers. This personal data is specifically considered to be of public interest and may be accessed by any third party.	Brian King; IPC	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
22.	Registrant e-mail address should not be redacted. Registrant city should not be redacted. General consensus across law enforcement, cybersecurity experts, intellectual property rights holders and consumer protection organizations exists that this is the most important WHOIS data element to support investigations and combat a wide range of illegal activity online, including DNS abuse. Registrants should be informed that this data element will remain unredacted and that they have the option of creating an e-mail address for their domain name registrations that contains no personally identifying information. That is a simple thing for any registrant to do and they can do so at no cost. We note that the GAC in its consensus advice issued in its ICANN61 San Juan Communique urged ICANN "to reconsider the proposal to hide the registrant email address as this may not be proportionate in view of the significant negative impact on law enforcement, cybersecurity and rights protection." The city of the registrant is required for serving legal process. If the street address of the registrant is redacted, then the city of the registrant should not be considered personal data warranting redaction. RE: Organization: The GDPR only applies natural persons, not legal persons. Therefore to redact an organization name actually runs counter to the GDPR rather than serving as a privacy protection that is either required or supported by the GDPR. Redacting the “organisation” field in the public WHOIS would not only run counter to the GDPR, but it would also go against other important EU regulatory frameworks related to (online) accountability and transparency of businesses and e-commerce in the EU. Article 5 of Directive 2000/31/EC on electronic commerce for example requires that online service providers shall render easily and permanently accessible the following information: (i) their name, (ii) their geographic address, (iii) their contact details, including their electronic email address , (iv) their trade or commercial register number, etc.	Dean S. Marks; Coalition for Online Accountability	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
23.	ALL elements should not be redacted. Under the proposed recommendation, registrants would be unable to easily demonstrate via the WHOIS that they are the owners of their own assets! This would greatly degrade the value of domain name assets, and expose domain names to issues like identity theft (where others can pretend, with impunity, that they are the owners of a domain name, when in fact they are not). If you're going to permit redaction, please ensure that registrants can OPT OUT of redaction, and OPT-IN to full publication of their own WHOIS data. The purported reason for the GDPR is to give owners of data control over it, but the current recommendation doesn't allow me, as a registrant, to make it public! (it appears, reading the text as is, that the registrar has no choice and must redact!). Here's another possible solution (that others might not have considered), namely allow registrants to run their own WHOIS service for their own domain names. In the case of .com (a thin WHOIS registry), we essentially have the main WHOIS info become the responsibility of the registrar to publish. Thus, the registry essentially redirects those seeking full WHOIS to the registrar. Why not add one new level of redirection to this? We can make the registrar also be a "thin WHOIS" provider, who would redirect requests for full WHOIS output to the registrant. Thus, the registrant can have control over publication of their data. Using digital signatures, the published WHOIS output from the registrant's WHOIS server would publish both the data and a signature. Since the registrar has all the data too (but doesn't publish it), all the registrar needs to do is publish a cryptographic signature (without the data). If the cryptographic signature from the registrar matches the signed data published by the registrant, then one can be assured that the WHOIS contact data is valid (and matches what the registrar isn't itself publishing). In other words, by delegating the task of publishing the WHOIS to the registrant themselves, many of the legal liability issues generated by GDPR of registrars and registries disappear. RE: Organization: A registrant who wants to prove they are the owner of their own domains *wants* to have these fields published.	George Kirikos; Leap of Faith Financial Services Inc.	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
24.	All registrant fields MAY be displayed. Registrant City. Technical Contact Name, Technical Contact Phone, Technical Contact Email 1) The report seems to make a HUGE change to the current Temp Spec. The current Temp Spec says that Registry Operator and Registrar MUST redact ONLY WHERE the data subject or processing activity is covered under GDPR. They MAY publish registrant data such as name and address where the data subject or processing activity is NOT covered under GDPR. That protects parties under GDPR and is fine. But Rec #8 now says that registrant fields such as name and address MUST ALWAYS be redacted. That is a huge expansion of blocking. The current Temp Spec's qualifications and guidelines for redaction are missing, and without them the recommendation is an immense change. This many not have been the intent of WG, but it's what the plain language of Rec 8 says. Rec 8 needs to at least go back to the the Temp Spec's qualifications. 2) It would be preferable if contact fields such as name and address are redacted ONLY IF protected by GDPR or another applicable privacy law. Along with that needs to be a program to provide some surety. But so far we don't think the data protection authorities are going to penalize any registrar or registry operator if a registrant mi-identifies its country of residence, natural-versus-legal status, etc. The risk is on the registrant there, and legitimate interests balance it. It is not ICANN's role to create a blanket base privacy regime of the world; it is ICANN's role to facilitate compliance but not to force parties to go beyond it. 2) The entire point of collecting a Tech Contact is to DISPLAY it, so tit can be seem by the public. So there needs to be better discussion of why the Tech fields would be redacted from publication. If the data is provided, then there can be a mechanism for the registrant to attest that the data has been provided with the data subject's permission. The GDPR was not designed to make such things impossible. 3) It is strained to claim that Registrant City is personally identifiable. RE: Organization: The GDPR does not protect the data of legal persons. The existing data in teh field should not be displayed yet but there should be a requirement put in place to get registrants to tell them that ht field is for legal person info, and review what is in this field going forward.	Greg Aaron; iThreat Cyber Group	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
25.	Tech Fields collected (as optionally provided by data subject) should be the same fields as those fields collected for Registrant contact. If the tech contact data is collected from the Registrant, to the extent allowable by law, said data should not be redacted. See 44, 45 above RE: Organization: Efforts should be made to provide educational material such that the data provided in the Org field can be relied on to not contain personal data, or else that the data is provided with proper informed consent by the data subject. With these conditions in place, the publication of the Org field can be useful.	Ben Butler; SSAC	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
26.	In the case of Registrants registering domain names for commercial webspaces, none of the data elements to be redacted; more data elements may be necessary. RE: Organization: None.	Sivasubramanian Muthusamy; Internet Society India Chennai	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
27.	INTA supports publication of Registrant Email, Organization, and Registrant City. None of these data elements should be redacted. In order to minimize consumer harm, it is important that swift action is taken in instances of suspected malicious activity. Malicious sites support a range of harmful bad practices including offering counterfeit goods or services, infringing trademarks or supporting some other illegal purpose like the support of malware. Typically, when a rights holders begins an investigation into whether a website is malicious, the email address is the first line of inquiry. Knowing the Registrant's city is another data point used to determine whether the site may be controlled by a bad actor or, instead, a business partner or other friendly entity. As important as it is to find bad actors, it is equally important to identify authorized users and avoid unnecessary enforcement actions including UDRP filings or other means of enforcement. Access to accurate and timely information can help rights holders avoid bringing registrants into the UDRP process unnecessarily. From a privacy perspective, oftentimes a Registrant's Email address will not have sufficient identifying information to be able to decipher personal information, while still giving others an opportunity to correspond directly with the Registrant. Practically speaking, Registrants may provide email addresses without any personally identifying information. The implications of using email with personally identifiable information could be explained to Registrants during the domain name registration process. Therefore, Registrants will have full notice as to the accessibility of the email address and the ability to provide an email address with non personally identifying information. The legal basis of GDPR Article 6.1 (f) and corresponding balancing tests support the exercise of rights and furtherance of interests of third parties including law enforcement and intellectual property rights holders. The risk of the Registrant receiving unsolicited emails must be weighed against the risk of perpetuating online abuse and consumer fraud. As explained in INTA's response to Purpose 1 above, Registrants have rights and obligations within the domain name system. The risk of the Registrant receiving unsolicited communication cannot outweigh the accountability and transparency necessary when operating a website or email address related to a domain name. Alternatives like communicating through an anonymized email address or web form are not sufficient to overcome the challenges of redacted email. This is because communications from anonymized email addresses or web forms may either be marked as spam or never be properly forwarded. The net effect is that a third party attempting to get in contact with a Registrant would not be able to know if the email failed or if the Registrant is simply not responsive. Redacting or masking the email address of Registrants unduly restricts law enforcement, enforcement of intellectual property rights and consumer protection. It also prevents parties from amicably settling disputes related to potential online infringements and may trigger unnecessary legal actions based on the failure to properly identify a party prior to a legal filing. Many of these harms are rightfully avoided by publishing an accurate, contactable email address. The rationale for publishing organization information is more thoroughly explained below. RE: Organization: None.	Lori Schulman Senior Director, Internet Policy; International Trademark Association (INTA)	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
28.	City and organization The U.S. wants the organization name and city fields to remain public and not be redacted. There is no evidence that indicates that publication of these fields is in violation of GDPR or is personally identifiable in combination with other published fields. In fact, there are other public online resources that make these fields (and others) available. Most notably are the business registers that are maintained and published by most European countries and consolidated by the European Business Register. The U.S. appreciates that the organization field has been incorrectly filled in by some registrants in the past and that in some cases they have included personally identifiable information. The U.S. does not see previous inaccurate information as justification to stop publication of these fields, but rather an opportunity to better inform registrants for new registrations and to clean up historical records in a phased in manner (e.g., including through annual notices to registrants, etc.). RE: Organization: Same entry as above.	Ashley Heineman; NTIA	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
29.	Registrant Organization. Email Address. Registrant Organization: The Temp Spec does not redact this field. No arguments have yet been communicated that merit overriding the correct decision to publish a data field that is meant for Legal Persons. Email Address: The single most useful field for cybersecurity research and the resulting protection of the security and stability of DNS. There are ways to handle this data field that protect both its viability for this purpose and the privacy of the Natural Person registrants. RE: Organization: see above.	Tim Chen; DomainTools	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
30.	Regarding the undecided redaction or non redaction of the Organization field The AG IS opposes the redaction of the Organization field, which is important for cybersecurity, and is a legal person under GDPR Recital 14A. Here, it is important for the EPDP to recognize that the Organization field is not private information and is in fact consistent with business record requirements from many EU member states as well as European Directive 2000/31/EC. Accordingly, in analyzing interests and rights, the Organization field should not be equated with other fields containing personal data under the GDPR. Regarding the redacted City field The AG IS opposes the redaction of the City field, which is not personal data, and which is a useful field for cybersecurity. Regarding the redacted Email field The AG IS opposes redaction of the Email field without a suitable replacement. Some European ccTLDs publish entire Whois records, including a registrant's email address and other personal data, consistent with GDPR. Nonetheless, if the community chooses to redact this field as a matter of policy then it is important to ensure that another universal, cross-TLD identifier, whether generated through anonymization or tokenization, exist in its place. An email form is not suitable for cybersecurity purposes. Regarding the redacted "Tech Fields" The AG IS opposes the fragmentation of Tech Contact fields. Since the inception of Whois, the Tech Contact field has been a useful means for reaching those best able to resolve technical issues as well as for reaching victims for DNS abuse. Accordingly, this should continue to be available as an option for all registrants of gTLDs. RE: Organization: The AG IS opposes the redaction of the Organization field, which is important for cybersecurity, and is a legal person under GDPR Recital 14A. Here, it is important for the EPDP to recognize that the Organization field is not private information and is in fact consistent with business record requirements from many EU member states as well as European Directive 2000/31/EC. Accordingly, in analyzing interests and rights, the Organization field should not be equated with other fields containing personal data under the GDPR.	Greg Mounier on behalf of Europol AGIS; Europol Advisory Group on Internet Security	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
31.	City and Email should not be redacted. City of residence is not sensitive personal information. Email addresses are critical data points for combatting illicit activity and DNS abuse—including intellectual property infringement—as well as for purposes of consumer protection and public safety. Combatting the harm to consumers and businesses posed by illicit use of domain names outweighs the slight privacy interest in an email address of a domain name holder, especially since the domain name holder is willingly engaging in public-facing activity. Significantly, a registrant can easily select an email address that does not disclose sensitive information, if he or she chooses. For purposes of notice, registrars should inform registrants that their email address will not be redacted. RE: Organization: The GDPR applies only to information about "natural persons." See GDPR, art. 1 (describing the subject matter and objectives of the regulation as relating to the protection of natural persons), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. The GDPR thus imposes no obligation to obfuscate information about businesses or other legal entities. Because access to such information is necessary to promote the transparency, accountability, and trust that is critical to promote commerce, communications, and creativity online, as well as for purposes of consumer protection, law enforcement, and enforcement of intellectual property and other rights, such information should remain available. This is also consistent with ICANN President and CEO Göran Marby's comments making "it a high priority to find a path forward to ensure compliance with the GDPR while maintaining WHOIS to the greatest extent possible." Data Protection and Privacy Update—Plans for the New Year, ICANN Blog (Dec. 21, 2017), https://www.icann.org/news/blog/data-protection-and-privacy-update-plans-for-the-new-year.	Neil Fried; The Motion Picture Association of America	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
32.	Regarding the redacted City field The City field should not be redacted as an individual cannot be identified nor is identifiable either directly or indirectly from this identifier or with all the identifiers otherwise non-redacted. Regarding the redacted Email field The lack of a consistent approach by all Contracted Parties could create a fragmented system. The GDPR allows for anonymisation techniques to protect personal data. Consistent with its previous views shared with the ICANN Community, as well as its previous Advice to the ICANN Board, the GAC believes that email addresses should be anonymized as the preferred path forward (rather than a web form) as it would prevent identification of the data subject via all likely and reasonable means, while providing a special email per registrant that is unique across all domains and TLDs. This unique but anonymized identifier is needed for investigative and other legitimate uses. This view is consistent with the Opinion of the Art. 29 Working Party which recognized "that anonymisation techniques can provide privacy guarantees" so long as there is sufficient regard given to "to all the means 'likely reasonably' to be used for identification (either by the controller or by any third party)." See Art. 29 WG Opinion 05/2014 on Anonymisation Techniques. Regarding the redacted "Tech Fields" The GAC is concerned that the EPDP is considering making the collection of this data "optional" for registrars without thoroughly and thoughtfully considering what impact this would have in terms of data transfer, registry practices, as well as impact on the consumer. Regarding the latter, the GAC does not think it is appropriate for registrars to unilaterally decide for registrants that they do not need to identify a technical contact. Registrants may see value in providing a technical contact to resolve issues with their domain in a timely and most direct manner, among other reasons. The provision (and therefore collection) of a technical contact should remain an option for the registrant. RE: Organization: Regarding the undecided redaction or non redaction of the Organization field The Organisation field should not be redacted as this is clearly a field whereby any personal data contained within the entry would fall under that of a legal person as defined within rectial 14A. The Contracted Parties have noted there may be historic data in this field which is not an Organisation name as some registrants may have incorrectly provided information. This could be rectified by a number of means, the first to provide clear advice on what this field is for and the implications of entering data into here. Second, to provide the registrant with the ability to rectify this field if it is not correctly filled out and by confirmation at renewal point. The GAC would like to point out that there are many European countries who publicly publish business details (including organization name) and even a network of these national registers (European Business Registrar). Also the European Directive 2000/31/EC states "Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information: (a) the name of the service provider; (b) the geographic address at which the service provider is established; (c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;" Where there are concerns over how to handle this information, we recommend that ICANN contracted parties consider these as potential models to inform the decisions made by the EPDP.	Fabien Betremieux; GAC	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
33.	Registrant email and city should not be redacted. City of residence is not sensitive personal information and is needed in order to serve legal processes effectively, identify proper venue for litigation and understand which controlling law and procedure applies. Additionally, email addresses are critical data points for combatting illicit activity, consumer protection, public safety or any DNS abuse. Email addresses are a necessary data point for both notifying a potential victim as well as alleged perpetrator without necessarily identifying the domain name holder. Registrants have the ability to register a domain name with an unidentifiable email address and also have the option to use a privacy or proxy service when registering the domain name. RE: Organization: The GDPR applies only to information about Natural persons, not Legal persons. Legal entity registrants such as corporations should not have any WHOIS data redacted.	Sajda Ouachtouki; The Walt Disney Company	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
34.	RE: Organization: Organisations are not covered by the GDPR	Steve Gobin; Corporate domain name management	Divergence **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
Not designated			

#	Comment	Contributor	EPDP Response / Action Taken
35.	No selection made and no additional comments submitted	• Ivett Paulovics; MFSD Srl URS Provider • Renee Fossen; Forum - URS and UDRP Provider • Brian Beckham; Head, Internet Dispute Resolution Section at WIPO • Monique A. Goeschl; Verein für Anti-Piraterie der Film- und Videobranche (VAP) • Theo Geurts • Ashley Roberts; Valideus • Stephanie Perrin	**EPDP Response:** none **Action Taken:** none [**COMPLETED**]

RECOMMENDATION 8 – Additional Comments

#	Comment	Contributor	EPDP Response / Action Taken
36.	This is a truly horrible recommendation, and would not allow registrants to publish their own data in the WHOIS, to demonstrate to others definitively that they are the owners of their own domains. Redaction should be optional, and not be forced upon those who want their data to be public. Adoption of this recommendation would diminish trust in the DNS. Imagine if you couldn't look up your own property records for real estate at the land registry, and allow others to see them publicly, for example, to prove to others that you're the owner of your own house? There are a lot of shady registrars, who would be able to seize the assets of a registrant, because the registrar could no longer prove that they are the owners of their own domain names! The public WHOIS provides an important verification benefit, to prevent this and other types of abuse. I simply fail to see how the other constituencies (outside the IPC and BC, who also oppose this recommendation) can justify mandatory redaction, even when the registrant themselves *doesn't* want the data redacted. If it's due to liability concerns (for registrars and registries), see the comments 2 fields above on this form, where I proposed allow registrants to run their own WHOIS servers to show their own contact details (which can be verified using digital signatures, and registries/registrars need only publish the signatures or a cryptographic hash, instead of the underlying data).	George Kirikos; Leap of Faith Financial Services Inc.	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
37.	The EPDP is mainly about evaluating and revising the Temp Spec. But the Initial Report makes it very hard for readers to figure out what a resulting Temp Spec might look like based on the recommendations. The EPDP must include a red-lined version of the Temp Spec in its next report, so the community can understand and comment on it. Right how the potential results and implications are pretty opaque. See comment #1 on Rec 8 above for an example.	Greg Aaron; iThreat Cyber Group	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
38.	This comment submission in various sections emphasises the importance of making a distinction between registrants registering a domain name for individual webspace (for instance a personal blog) and a registrant registering a domain name for commercial use (for instance a website with a payment gateway or bank account details); With such a distinction between personal and commercial domain names the "Organization" field is essential for commercial domain names, but non-essential for personal domain names. What is referred to as "commercial domain name" is usually domain names registered by business entities legally known as artificial persons, but also includes individuals carrying out commercial activity in the webspace linked to the domain name, and non-commercial legal entities raising funds.	Sivasubramanian Muthusamy; Internet Society India Chennai	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
39.	While the RySG supports the substance of Recommendation #8, we believe the wording could be more clear by stating upfront which data fields should be redacted in the public registration data output.	Wim Degezelle ; RySG	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]
40.	CITY: Non-redaction of the city field in connection with other available data such as the domain name itself may allow the identification of the registrant, especially for smaller cities or towns with only a few hundred inhabitants. We therefore propose that as a default the CITY field remain redacted. EMAIL: We support the EPDP recommendation. TECH: As the main concern of the TECH fields is to provide the ability to contact a knowledgeable party, it should be sufficient to provide only the necessary contact details to enable such contact. For such purposes, the identity of these contacts is not required. Furthermore, in legacy registrations many registrants filled this contact with their own details. Therefore, removal of redaction would expose their personal information. We therefore propose that the name and phone number remain redacted and the email contact be handled in accordance with the EPDP team recommendation.	• Zoe Bonython; RrSG • Volker Greimann; Key-Systems GmbH	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

#	Comment	Contributor	EPDP Response / Action Taken
41.	In this area, concerns about compliance with GDPR must guide the policy. Based on legal advice it received last year, ICANN org redacted most of the data fields regarding the registrant's contact information in its Temporary Specification. The EPDP recommended the same set of redactions as the Temp Spec. Disagreements are at the margins. Privacy advocates would like to see the State/Province field redacted. The Intellectual Property interests would like to see both the State/Province and the City fields published. The EPDP has agreed that the Administrative and Technical Contacts will no longer be required data elements to be collected. These ancient data fields go back to the origins of Whois before ICANN existed, and serve little purpose, yet for some reason they were required elements in registrar contracts. In a very large portion of domain name registrations, the Admin-C and Tech-C are the same as the registrant. Based on the principle of data redaction, Admin-C will no longer be required, and it will be optional for a registrant to provide a technical contact. The EPDP is still considering whether registrars should be required to offer a Technical Contact field. It should be noted that for all practical purposes, the default technical contact for any registrant is the registrar, and registrar contact info is already automatically included in the public Whois. However, another question to be considered is whether 'optional' also means 'optional' for the registrar to offer the ability to the Registered Name Holder to provide these data elements or whether the Registrants should continue to be required to offer this ability. In either case, if the Registrar optionally provides this option or is required to provide this option, Registrars are to advise the Registered Name Holder at the time of registration that the Registered Name Holder is free to (1) designate the same person (such as the registrant themselves or its representative) as the technical contact; or (2) provide contact information which does not directly identify the technical contact person concerned.	DR. JAIDEEP KUMAR MISHRA ; DIRECTOR MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA	Concerns **EPDP Response:** **Action Taken:** [**COMPLETED / NOT COMPLETED**] – [Instruction of what was done.]

NOT REDACTED
Domain Name Registrar Whois Server Registrar URL Updated Date
Creation Date Registry Expiry Date
Registrar Registration Expiration Date Registrar
Registrar IANA ID
Registrar Abuse Contact Email Registrar Abuse Contact Phone Reseller
Domain Status

Registrant Fields
- State/province
- Country
- Anonymized email / link to web form

Tech Fields
- Anonymized email / link to web form

NameServer(s) DNSSEC No
Name Server IP Address
Last Update of Whois Database

REDACTED
Registrant Fields
- Name

- Street
- City
- Postal code
- Phone
- Email

Tech Fields
- Name
- Phone
- Email

UNDECIDED (REDACTED/ NOT REDACTED)
- Organization (opt.)

Please reference page 14-15 of the Initial Report for details of the data elements.