Please provide your affiliation.	Are you providing input on behalf of another group (e.g., organization, company, government)?	If yes, please explain:

IPC	Yes	IPC

Question for Community Input: Is there new information or inputs that the Phase 2A team has not considered in assessing whether to make changes to the recommendation that Registrars and Registry Operators may, but are not obligated to, differentiate between legal and natural persons?

The IPC takes the position that because WHOIS/RDS data serves the public interest, redaction of legal entity data is not justified by data protection legislation, and because ICANN's stated purpose in the Temporary Specification was "maintaining the former WHOIS system to the greatest extent possible," (https://www.icann.org/en/system/files/files/gtld-registration-data-temp-spec-17may18-en.pdf) there is no legitimate basis for the burden to have shifted so that intellectual property owners, law enforcement, and other members of the public must now justify why redacting this data should not be allowed.

The EPDP Phase 1 Final Report (https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf) contemplates that contracted parties will provide WHOIS data in response to individual requests. Unfortunately, empirical evidence indicates this is not the case. Leading organizations requesting this data from contracted parties for consumer protection purposes report success rates in the range of 10 (https://www.appdetex.com/appdetex-whois-requestor-system-awrs-3/) to 14 (https://clarivate.com/markmonitor/blog/gdpr-whois-and-impacts-to-brand-protection-nine-months-later/) percent, indicating that legitimate requests are often not being considered in good faith. Moreover, in June 2021, the Messaging Malware Mobile Anti-Abuse Working Group ("M3AAWG") and the Anti-Phishing Working Group ("APWG") issued a report entitled "ICANN, GDPR, and the WHOIS: A Users Survery – Three Years Later." The report states that the lack of access to WHOIS data following ICANN's policy changes in an attempt to comply with the GDPR "continue to significantly impede cyber applications and forensic investigations and thus cause harm or loss to victims of phishing, malware or other cyber attacks." (https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf) We note that some contracted parties have contended that criminals do not list legal entity data in WHOIS records, but this assertion is irrelevant to the consideration of whether information otherwise available through other public records should be redacted, and unfounded, as there are many instances of businesses infringing on intellectual property rights and other third-party rights online. While consumer protection and IP rights enforcement may be the primary uses of WHOIS data for IPC members, we note that all other legitimate uses (https://whois.icann.org/en/what-whois-data-used) of this data are also impeded when the data is unavailable.

The IPC also notes that making the distinction between legal and natural person data in the RDS is already required by the EPDP Phase 2 Recommendation 9.4.4. This present recommendation would merely make that requirement public. This would also help the public know whether an SSAD request would even be necessary, since the public RDS record would indicate whether the data was redacted because it contained natural person data or merely out of convenience to the registrar.

Question for Community Input: Is this recommendation necessary for the GNSO council in conside

Yes, this recommendation for the GNSO Council in considering future policy work is necessary because it goes to the essence of the exercise... The Phase 1 and Pha
(GDPR) which formed the basis for analysis in the Temporary Specification and the Phase 1 and Phase 2 deliberations of the EPDP... While the EU has been the focu
and all of those laws could have effects on how data collection, access and processing are implemented through ICANN policy... The GDPR has been the main focus
some notable exceptions including for law enforcement and the performance of certain contracts) is viewed as a “gold standard” for privacy... With all of that said, the
the law… The confusion surrounding the issues of data collection from legal persons and the responsibility of accuracy has reached the such a heightened level that
specifically address the open issues within the EPDP, and most particularly Phase 2 A... Monitoring the progress of the legislation, due for a vote on October 14th 202

The NIS2 proposals affirm the applicability of GDPR and state unequivocally in proposed Article 23.4: “Member States shall ensure that the TLD registries and the ent
not personal data.” It is further clarified in the preceding Article 23.3 that such data must be accurate ... The passing of this regulation will undoubtedly influence the w
legal persons will not be optional, and must be accurate, which means accountability for ensuring accuracy will fall to those providing a domain name service as noted

The policy discussions taking place within the ICANN community are not taking place in a bubble; they are a response to consequential, external regulation that contir
are already in place at ICANN, most notably, through its relationships with the GAC, ICANN Org’s government engagement team, and the Cross Community Engagem
councilors come from organizations that have mechanisms in place for such monitoring as well. These are all substantial resources, which, when fully utilized, ease the

Question for Community Input: Should a standardized data element be available for a Contracted Party to use? If yes, why? If no, why not? Why is harmonization of practices beneficial or problematic?	**Question for Community Input: If yes, what field or fields should be used and what possible values should be included, if different from the ones identified above? Aspects of the recommendation that the EPDP Team is looking for specific input on have been marked with an asterisk (*) on pp. 5-6 of the Initial Report, and indicate the options that are under consideration.**

Yes. A standardized data element should be defined and be required to be published by Contracted Parties. Given future regulation (e.g., NIS2) that will require the distinction of legal and natural persons, a standardized RDS data element will ensure a consistent mechanism for RDS users to reliably ascertain if a Registrant is a legal or natural person.	The IPC believes that the “Registrant Legal Person” data element must be collected and published. We believe that Contracted Parties must be obligated to differentiate between registrations of legal and natural persons; if Contracted Parties are not obligated to do so, the existence of this field must still be required. In the case where a Contracted Party decides not to differentiate, the value of this field should be set to “Unspecified”. This new data field is not personal information and thus must be published in the public RDDS. Redacting this new data field and using a disclosure mechanism (SSAD or otherwise) would be inappropriate.

Question for Community Input: If such a standardized data element is available, MUST a Contracted Party who decides to differentiate use this standardized data element or should it remain optional for how a Contracted Party implements this differentiation?	**Question for Community Input: Does this guidance as written provide sufficient information and resources to Registrars and Registry Operators who wish to differentiate? If not, what is missing and why?**

Yes. A Contracted Party who differentiates must use this standardized data element. Allowing 2000 registrars to determine how this data should be displayed in the RDDS would be conflict with recent RDS policy work to ensure a consistent labeling and display of RDS data to RDS users.	The usefulness of a flagging mechanism was discussed in both the Phase 2 and Phase 2a EPDP discussions. In particular the use of a flag is important to streamline the processing of disclosure requests – be they performed manually or automated via a system such as the SSAD. For example, a flag can be updated once a disclosure request has been processed and the nature of the registration (legal vs. natural) and the absence or presence of personal information has been determined.

Question for Community Input: Are there additional elements that should be included in the guidance?	**Question for Community Input: Are there legal and regulatory considerations not yet considered in this Initial Report, that may inform Registries and Registrars in deciding whether and how to differentiate, and if so, how?**

n/a	Registries and registrars should consider the benefits of embracing a minimum voluntary (binding through ICANN compliance) threshold for differentiation in the interest of eliminating the need for varying legislation across the various jurisdictions where they operate, which are sure to have different standards, requirements, and associated penalties for noncompliance. Registries and registrars should not invite a complex patchwork of regulation on a topic as simple as agreeing not to apply data protection measures where such measures have no legal justification. We invite registries and registrars to consider NIS 2 as the merely the first legislative development among others which may follow if they choose not to self-regulate as suggested by the European Commission via the GAC.

Question for Community Input: If a Registrar or Registry Operator decides to differentiate, should this guidance become a requirement that can be enforced if not followed (“MUST, if Contracted Party decides to differentiate”)?	Question for Community Input: Does this guidance as written provide sufficient information and resources to Registrars and Registry Operators who wish to publish a registrant-based or registration-based email address? If not, what is missing and why?	Are there any other comments or issues you would like to raise pertaining to the EPDP Phase 2A Initial Report? If yes, please enter your comments here. If applicable, please specify the section or page number in the Initial Report to which your comments refer.

This should not be guidance. There should be a requirement to differentiate.	As an initial matter, the IPC is strongly in favor of a mandatory registrant-based email contact in public WHOIS data to facilitate cross-domain correlation, which as noted is essential for law enforcement and cybersecurity efforts, as well as online IP enforcement (which often overlaps with anti-phishing and similar anti-abuse efforts). As noted in the Bird & Bird Memoranda, in its Whois database, EURid publishes the email addresses of domain name registrants in the .eu TLD (both natural persons and legal entities). Similarly, RIPE-NCC publishes contact information, including email addresses, for its IP Address allocation recipients. We believe these approaches demonstrate the limited GDPR risk to Contracted Parties in publishing a registrant-based email contact in public WHOIS, so long as relevant registration agreements outline the legitimate purposes of such publication. We appreciate that publication of registrant-based email contacts is not the lowest possible degree of GDPR compliance risk, as outlined in the Bird & Bird Memo, but is also not flagged as a high risk. The several benefits of this approach for many parties in the ICANN community, as well as in serving ICANN's own security, stability, and resiliency mission, easily counterbalance the potential risks. Another concern raised is the possibility of using registrant-based email contacts for SPAM. We agree this is a reasonable concern, but question whether the desire to minimize SPAM email is on par with the ability to more effectively address networks of abusive domain names engaging in phishing, malware, fraud, or other abuse, which would be hugely improved through the availability of registrant-based email contacts. Systems are already in place to mitigate harvesting of public email addresses for SPAM, such	