PLEASE DO NOT COMMENT FURTHER ON THIS DOCUMENT - The updated version is posted here: https://docs.google.com/document/d/103kazmQlFxRmecNosslsZhg6u0MwxoZ5DiZj86j0JB8/edit?usp=sharing.

Instructions:

Please review this latest version of the legal/natural guidance write up and identify in the Input Table right underneath the write up (page 7) if there are any 'cannot live publishing this in the Initial Report' items that remain that the group should consider.

To review which updates were applied in response to the comments provided, please see the table at the end of this document which includes red line changes as well a staff support team explanation of which changes were applied and why. Note that there are still three outstanding questions that the EPDP Team will review during Thursday's meeting – please review the agenda and come prepared to discuss these. Thank you!

Deadline for identifying cannot live with items = Friday 7 May.

==========

Proposed Language for inclusion in the Initial Report addressing question ii Legal / Natural

The EPDP Team was tasked by the GNSO Council to address the following two questions:

i. Whether any updates are required to the EPDP Phase 1 recommendation on this topic ("Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so");
ii. What guidance, if any, can be provided to Registrars and/or Registries who differentiate between registrations of legal and natural persons.

In addressing these questions, the EPDP Team started with a review of all relevant information, including (1) the study undertaken by ICANN org,[1] (2) the legal guidance provided by Bird & Bird, and (3) the substantive input provided on this topic during the public comment forum on the addendum. Following the review of this information, the EPDP Team identified a number of clarifying questions, that, following review by the EPDP Team's legal committee, were submitted to the Bird & Bird (see https://community.icann.org/x/xQhACQ). The EPDP Team reviewed the responses from Bird & Bird and applied the advice received in its recommendations below.

[1] As part of its Phase 1 Policy Recommendation #17, the EPDP Team recommended, "as soon as possible ICANN Org undertakes a study, for which the terms of reference are developed in consultation with the community, that considers:

- The feasibility and costs including both implementation and potential liability costs of differentiating between legal and natural persons;
- Examples of industries or other organizations that have successfully differentiated between legal and natural persons;
- Privacy risks to registered name holders of differentiating between legal and natural persons; and
- Other potential risks (if any) to registrars and registries of not differentiating.

ICANN or delivered the study to the EPDP Team in July 2020.

Input received on the latest version of the guidance write up by deadline (see https://docs.google.com/document/d/1a7MEle3_e-iXbaiZQV5wCD4Pv0414YjLtC2yxJEqbJc/edit#)

The Working Group approached its task by first considering what guidance would be useful to Registrars and Registry Operators who choose to differentiate between registrations of legal and natural persons.

Definitions (note, these are derived from previous EPDP-related work, as indicated below):

- EPDP-p1-IRT: “Publication”, “Publish”, and “Published” means to provide Registration Data in the publicly accessible Registration Data Directory Services.
- EPDP-p1-IRT: "Registration Data" means the data element values collected from a natural or legal person or generated by Registrar or Registry Operator, in either case in connection with a Registered Name in accordance with Section 7 of this Policy.
- EPDP-P1 Final Report: Disclosure: The processing action whereby the Controller accepts responsibility for release of personal information to third parties upon request.

Background Information and EPDP Team Observations
In developing the guidance below, the EPDP Team would like to remind the Council and broader community of the following:

Scope of GDPR and other data protection legislation

A. GDPR and other data protection legislation set out requirements for protecting personal data of natural persons. It does not protect personal data of legal persons and non-personal data.
B. GDPR does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person. However, when a natural person's information is used in relation to a legal person, e.g. as a representative of a business, that natural person's data does remain protected as personal data under the GDPR.
C. Distinguishing between legal and natural person registrants alone may not be dispositive of how the information should be treated (made public or masked), as the data provided by legal persons may include personal data that is protected under data protection law, such as GDPR.

Relevant EPDP Phase 1 Recommendations

D. Per EPDP Phase 1[2] Recommendation #6, “as soon as commercially reasonable, Registrar must provide the opportunity for the Registered Name Holder to provide its Consent to publish redacted contact information, as well as the email address, in the RDS for the sponsoring registrar”.

[2] For further information about the status of implementation of the EPDP Phase 1 recommendations, please see https://www.icann.org/resources/pages/registration-data-policy-gtlds-epdp-1-2019-07-30-en.

E. Per the EPDP Phase 1 recommendation #17 "Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so".

Relevant EPDP Phase 2 Recommendations

F. Per Phase 2[3] Final Report Recommendation #9.4.4, which addresses automation of SSAD processing: "the EPDP Team recommends that the following types of disclosure requests, for which legal permissibility has been indicated under GDPR for full automation (in-take as well as processing of disclosure decision) MUST be automated from the time of the launch of the SSAD (…) No personal data on registration record that has been previously disclosed by the Contracted Party." This Recommendation 9.4.4 focuses generally on automating disclosure for registration records that do not include personal data.[4]
G. Per Phase 2 Final Report Recommendation #8.7.1, if the Contracted Party receives a request from the SSAD Central Gateway Manager and the Contracted Party has determined this to be a valid request, "if, following the evaluation of the underlying data, the Contracted Party reasonably determines that disclosing the requested data elements would not result in the disclosure of personal data, the Contracted Party MUST disclose the data, unless the disclosure is prohibited under applicable law".

Registrar Business Models

H. Registrars operate different business models (Retail, Wholesale, Brand Protection, Others), and one-size-fits-all or overly prescriptive guidance may not properly consider the range of registrar business models and the various process flows the different business models may require. Instead, any guidance must provide Registrars the flexibility to implement differentiation in a manner that best suits their business model and reduces the risks associated with differentiation to an acceptable level for that particular Registrar. For example, differentiation at the time of registration may not be possible or practical in all circumstances, including for certain registrar business models.

Proposed Guidance

The EPDP Team would like to put forward the following guidance to assist Registrars who want to differentiate between registrations of natural and legal persons, or those of legal persons containing personal and non-personal data.

1. By allowing registrants to self-identify as legal persons if they wish to do so, differentiation between the data sets of natural and legal persons should typically occur at the time of registration, or at the first opportunity after registration that the Registrar interacts with the Registrant.
2. Any differentiation process must ensure that the data of natural persons is redacted from the public RDDS unless the data subject has provided their consent to publish,

[3] Note that the EPDP Phase 2 recommendations are with the ICANN Board for its consideration / approval.

[4] Please note that the exact details of how this recommendation will be implemented are to be determined by ICANN org in collaboration with the Implementation Review Team, once the ICANN Board has approved the recommendations.

consistent with a "data protection by design and by default" approach (see EDPB guideline on this topic for further information).

3. As part of the implementation, Registrars should consider using a type of flag in the RDDS or their own data sets that would indicate the type of data it concerns (personal or non-personal data) as this could facilitate review of disclosure requests via SSAD and the return of non-personal data of legal persons by systems other than SSAD (such as Whois or RDAP). A flagging mechanism could also assist in indicating changes to the type of data in the registration data field(s).
4. In all of the below scenarios, clear communication and guidance should be provided to the registrant (data subject)[5] by the Registrar concerning the possible consequences of: 1) identifying a data set as being of a legal person, 2) confirming the presence of personal data or non-personal data, and 3) providing consent[6]. This is also consistent with section 3.7.7.4 of the Registrar Accreditation Agreement (RAA).
5. Registrants (data subjects) must have an easy means to correct possible mistakes.
6. Distinguishing between legal and natural person registrants alone may not be dispositive of how the information should be treated (made public or masked), as the data provided by legal persons may include personal data that is protected under data protection law, such as GDPR.

Example scenarios (note, these scenarios are intended to be illustrations for how a Registrar could apply the guidance above. These scenarios are NOT to be considered guidance in and of itself).

The EPDP Team has identified three different high-level scenarios for how differentiation could occur based on who is responsible and the timing of such differentiation. It should be noted that other approaches and/or a combination of these may be possible.

1. Data subject self-identification at time of data collection / registration

a. The Registrar informs the Registrant (per guidance #3 above) and requests the Registrant (data subject) at the moment of Registration data collection to designate legal or natural person type. The Registrar must also request the Registrant to confirm whether only non-personal data is provided for legal person type.[7]

b. If the Registrant (data subject) has selected legal person and has provided a confirmation that the registration data does not include any personal data, the Registrar should (i) contact the provided contact details to verify the Registrant claim[8] (ii) set the registration data set to automated disclosure in response to SSAD queries and (iii)

[5] Note, the Registrant may not be always be the data subject, but in all circumstances appropriate notice / consent needs to be provided to and by all parties as per applicable data protection law.

[6] See also https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[7] Note that the confirmation that only non-personal data is provided could also happen at a later point in time. However, until the Registrant confirms that no personal data is present in the registration data, the Registrar does not set the registration data to automated disclosure.

[8] Per the guidance provided by Bird & Bird, "this verification method is advisable, and will help reduce risk. That risk reduction will be greatest if there is a reasonable grace period within which the objection can be lodged, before the data in question is published in the Registration Data" and "requiring an affirmative response to verification mailings seems over-cautious, unless and until studies show that the measures adopted are failing to keep very substantial amounts of personal data out of published Registration Data. However, if a verification email "bounces" (i.e. a Contracting Party knows it was not delivered), then it would be better if publication does not proceed".

publish the data (to provide Registration Data in the publicly accessible Registration Data Directory Services).

c. If the Registrant (data subject) has selected natural person or has confirmed that personal data is present, the Registrar does not set that registration data to automated Disclosure and Publication, unless the data subject consents to Publication.[9]

2. Data subject self-identification at time when registration is updated

a. The Registrar collects Registration Data and provisionally redacts the data.

b. The Registrar informs the Registrant (per guidance #3 above) and requests the Registrant (data subject) to designate legal or natural person type. The Registrar must also request the Registrant to confirm whether only non-personal data is provided for legal person type.[10]

c. Registrant (data subject) indicates legal or natural person type and whether or not the registration contains personal information after registration is completed. For example, the Registrant may confirm person type at the time of initial data verification, in response to its receipt of the Whois data reminder email for existing registrations, or through a separate notice requesting self-identification.[11]

d. If the data subject identifies as a legal person and confirms that the registration data does not include personal data, the Registrar should (i) contact the provided contact details to verify the Registrant claim[12] (ii) set the registration data set to automated disclosure in response to SSAD queries and (iii) publish the data.

3. Registrar determines type based on data provided

a. The Registrar collects Registration Data and provisionally redacts the data.

b. The Registrar uses collected data to infer legal or natural person type.[13]

c. If legal person is inferred by the Registrar and subsequently the Registrant (data subject) is informed (per guidance #3 above) and confirms that no personal data is present, the Registrar should (i) contact the provided contact details to verify the Registrant claim[14] (ii) set the registration data set to automated disclosure in response to SSAD queries and (iii) publish the data.

---

[9] Note that the data subject may not be the party executing the process but may have requested a third party to do so. In such circumstance consent may not be possible.

[10] Note that the confirmation that only non-personal data is provided could also happen at a later point in time. However, until the Registrant confirms that no personal data is present in the registration data, the Registrar does not set the registration data to automated disclosure.

[11] Note, the implementation of EPDP Phase 1, recommendation #12 (Organization Field) may facilitate the process of self-identification.

[12] Per the guidance provided by Bird & Bird, "this verification method is advisable, and will help reduce risk. That risk reduction will be greatest if there is a reasonable grace period within which the objection can be lodged, before the data in question is published in the Registration Data" and "requiring an affirmative response to verification mailings seems over-cautious, unless and until studies show that the measures adopted are failing to keep very substantial amounts of personal data out of published Registration Data. However, if a verification email "bounces" (i.e. a Contracting Party knows it was not delivered), then it would be better if publication does not proceed".

[13] Some EPDP Team members have noted that there may be risks for the Registrar to infer a differentiation without involvement of the Registrant (data subject).

[14] Per the guidance provided by Bird & Bird, "this verification method is advisable, and will help reduce risk. That risk reduction will be greatest if there is a reasonable grace period within which the objection can be lodged, before the data in question is published in the Registration Data" and "requiring an affirmative response to verification mailings seems over-cautious, unless and until studies show that the measures adopted are failing to keep very substantial amounts of personal data out of published Registration Data. However, if a verification email "bounces" (i.e. a Contracting Party knows it was not delivered), then it would be better if publication does not proceed".

d. If the Registrar has inferred natural person or has detected personal data, the Registrar must not disclose registration data unless the Registrant provides consent for publication or the Registrar Discloses the data in response to a legitimate disclosure request.

Registrars shall not be prohibited from voluntarily utilizing a third party to verify that a registrant has correctly identified its data[15], provided that such verification is compliant with applicable data protection regulations.

The EPDP Team recognizes that in all of the above scenarios, there is the possibility of misidentification, which may result in the inadvertent disclosure of personal data. In this regard, Bird & Bird has noted the following:

> *11.11.1 If the (person representing the) Registrant incorrectly characterises personal data as non-personal, then the verification process this triggers should confer reasonable protection against GDPR Accuracy Principle liability for Contracted Parties, as explained at paragraph 11.7 above, as might the legal argument set out at paragraph 11.8 above.*
> *11.11.2 Alternatively, if the (person representing the) Registrant incorrectly characterises non-personal data as personal data, then whether or not they subsequently consent to its publication, the data would still not actually be personal data, so GDPR liability cannot arise.*

(…)

> *13. However, in our view the risk to Contracted Parties seems low, if they take the measures described in the question presented, to avoid personal data being (or if reported, staying) published in Registration Data.*

(…)

> *14.3 The data in question is likely to be low sensitivity. The scenario being envisaged here (mistaken inclusion of personal data in published Registration Data) seems to be most likely to occur when a legal entity (e.g. a company or non-profit organisation) is registering / maintaining its own domains. In those scenarios, we assume the personal data that could be disclosed would ordinarily relate to an employee's work details (e.g. a company email address), not an individual's private life. Although the GDPR confers protection even in the workplace, the data in question here may arguably be less capable of causing harm to an individual than data relating to the data subject's private life.[16]*

[15] Per the guidance provided by Bird & Bird, "a company registration number may be another means of verifying legal personhood".

[16] As explained above, we have understood this question to be asking about scenarios where Registrants are legal persons, as per the EDPB quote at paragraph 1. In respect of individual (natural person) Registrants, the issues will be largely similar: if a natural person incorrectly states that their data is not personal data, then (i) the verification measures should prevent the data from being published, since they will give the data subject an opportunity to correct their mistake; (ii) the mitigating factors and legal arguments described at paragraphs 11.7 and 11.8 and paragraphs 14.1 - 14.6 here, should confer reasonable legal protection for Contracted Parties.

(…)

> *18. We cannot exclude the possibility of some courts or regulators seeing things differently. Even then, an order to correct the issue (likely accompanied by a reasonable period in which to implement changes), rather than a fine, seems most likely, having regard to the GDPR Article 83(2) factors discussed at paragraph 8 above. Having checked in a selection of Member States, we can find no examples of enforcement in relation to this. Accordingly, there is little guidance available besides what is set out in the GDPR itself.*

As a result, the EPDP Team recommends that Contracted Parties who choose to differentiate based on person type SHOULD follow the guidance above and clearly document all data processing steps. However, it is not the role or responsibility of the EPDP Team to make a final determination with regard to the legal risks, as that responsibility ultimately belongs to the data controller.

Annex – Bird & Bird Legal Advice [to be added to the Initial Report]

==========

EPDP Team Input Table

	This text my group cannot live with for the purpose of inclusion in the Initial Report	**Rationale & proposed alternative that would make it acceptable**
ALAC:		
BC:		
GAC:		
IPC:		
ISPCP:		
NCSG:		
RrSG:		
RySG:		
SSAC:		

THIS TABLE IS PROVIDED FOR BACKGROUND PURPOSES – PLEASE DO NOT PROVIDE ANY FURTHER COMMENTS OR EDITS HERE BUT USE THE TABLE ABOVE INSTEAD TO IDENTIFY CANNOT LIVE WITH ITEMS.

Current Language	Staff Support Team – Rationale for changes made	Issues Raised / To Consider by EPDP Team
The EPDP Team was tasked by the GNSO Council to address the following two questions: i. Whether any updates are required to the EPDP Phase 1 recommendation on this topic ("Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so"); ii. What guidance, if any, can be provided to Registrars and/or Registries who differentiate between registrations of legal and natural persons. In addressing these questions, the EPDP Team started with a review of all relevant information, including (1) the study	Added language to emphasize that the advice received from Bird & Bird was considered and factored into the development of the EPDP Team's recommendations as suggested by Laureen	Suggest referencing Bird & Bird legal advice on Natural/Legal issues here. (Laureen)

undertaken by ICANN org,[17] (2) the legal guidance provided by Bird & Bird, and (3) the substantive input provided on this topic during the public comment forum on the addendum. Following the review of this information, the EPDP Team identified a number of clarifying questions, that, following review by the EPDP Team's legal committee, were submitted to the Bird & Bird (see https://community.icann.org/x/xQhACQ). the responses from Bird & Bird		
As part of its approach in dealing with these two questions, the EPDP Team agreed to commence with identifying possible guidance to Registrars and/or Registries who decide to differentiate between registrations of legal and natural persons.	Updated as suggested by Sarah. Staff Support Team suggests that language that explains the different positions in relation to the question of mandatory or not are considered in the context of the write up of the response to question.	1. Proposed rewording: 2. The EPDP Team commenced with identifying possible guidance to Registrars and/or Registries who decide to differentiate between registrations of legal and natural persons. The question of whether differentiation must be mandatory was approached only after creation of the guidance. (RrSG - Sarah)

[17] As part of its Phase 1 Policy Recommendation #17, the EPDP Team recommended, "as soon as possible ICANN Org undertakes a study, for which the terms of reference are developed in consultation with the
community, that considers:

- The feasibility and costs including both implementation and potential liability costs of differentiating between legal and natural persons;
- Examples of industries or other organizations that have successfully differentiated between legal and natural persons;
- Privacy risks to registered name holders of differentiating between legal and natural persons; and
- Other potential risks (if any) to registrars and registries of not differentiating.

ICANN or delivered the study to the EPDP Team in July 2020.

		3. "The Working Group approached its task by first considering what guidance would be useful to Registrars and Registry Operators who choose to differentiate between registrations of legal and natural persons. Several stakeholder groups, however, think that the principles set forth in the proposed guidance should be mandatory, not elective" (GAC - Laureen) Maybe we can keep this to the first sentence from Laureen's suggestion? "The Working Group approached its task by first considering what guidance would be useful to Registrars and Registry Operators who choose to differentiate between registrations of legal and natural persons." The second sentence changes topics (instead of describing the team's approach it describes the outcome) and so I don't think it fits here. (RrSG – Sarah)
Definitions (note, these are derived from previous EPDP-related work, as indicated below): ● EPDP-p1-IRT: “Publication”, “Publish”, and “Published” means to provide Registration Data in the publicly accessible Registration Data Directory Services.		

• EPDP-p1-IRT: "Registration Data" means the data element values collected from a natural or legal person or generated by Registrar or Registry Operator, in either case in connection with a Registered Name in accordance with Section 7 of this Policy. • EPDP-P1 Final Report: Disclosure: The processing action whereby the Controller accepts responsibility for release of personal information to third parties upon request.		
Background Information and EPDP Team Observations In developing the guidance below, the EPDP Team would like to remind the Council and broader community of the following: *Scope of GDPR and other data protection legislation* A. GDPR and other data protection legislation set out requirements for protecting personal data, not non-personal data.	Updates made to A and an additional B based on the input from the small team.	
B. Distinguishing between legal and natural person data alone may not be dispositive, as the data provided by	Note, this section will be moved to guidance section	Proposed suggestions:

legal persons may include personal data that is protected under data protection law, such as GDPR.		4. Replace "data" with registrants or registration data? (IPC – Brian, RrSG – Sarah) 5. Move this observation to guidance section, it could be very useful guidance to Contracted Parties (RrSG – Sarah) 6. Question: dispositive of what? (IPC – Brian) I think this phrasing came from GAC? I understood it meant dispositive as to whether the data can be published or not (RrSG – Sarah)
Relevant EPDP Phase 1 Recommendations C. Per EPDP Phase 1[18] Recommendation #6, "as soon as commercially reasonable, Registrar must provide the opportunity for the Registered Name Holder to provide its Consent to publish redacted contact information, as well as the email address, in the RDS for the sponsoring registrar". D. Per the EPDP Phase 1 recommendation #17 "Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so".		

[18] For further information about the status of implementation of the EPDP Phase 1 recommendations, please see https://www.icann.org/resources/pages/registration-data-policy-gtlds-epdp-1-2019-07-30-en.

Relevant EPDP Phase 2 Recommendations E. Per Phase 2[19] Final Report Recommendation #9.4.4, which addresses automation of SSAD processing: "the EPDP Team recommends that the following types of disclosure requests, for which legal permissibility has been indicated under GDPR for full automation (in-take as well as processing of disclosure decision) MUST be automated from the time of the launch of the SSAD (…) No personal data on registration record that has been previously disclosed by the Contracted Party." In other words, if a Contracted Party manually reviews a disclosure request pursuant to EPDP Phase 2 Recommendation 8, and determines there is no personal data present, the Contracted Party must disclose the requested data to the third party. Following disclosure, the Contracted Party must mark the domain name for automated disclosure for future disclosure	Updated as proposed by Laureen and supported by Sarah	7. Suggest removing last two sentences ("In other words…). It is sufficient to only include the Recommendation text as reference, we do not need inferences about how it may be implemented after approval by the Board. (RrSG – Sarah) Proposal by Laureen: Consider as explanatory text instead of "In other words" text: This Recommendation focuses generally on automating disclosure for registration records that do **not** include personal data.

[19] Note that the EPDP Phase 2 recommendations are with the ICANN Board for its consideration / approval.

requests associated with that domain name.[20]		
F. Per Phase 2 Final Report Recommendation #8.7.1, if the Contracted Party receives a request from the SSAD Central Gateway Manager and the Contracted Party has determined this to be a valid request, "if, following the evaluation of the underlying data, the Contracted Party reasonably determines that disclosing the requested data elements would not result in the disclosure of personal data, the Contracted Party MUST disclose the data, unless the disclosure is prohibited under applicable law".	As explained during the meeting on 25/4, this recommendation seems relevant to reference as it specifies that Contracted Parties, after establishing that no personal is present but only non-personal data, the Contracted Party MUST disclose the non-personal data. However, if others support its removal, it will can be removed.	
Registrar Business Models G. Registrars operate different business models (Retail, Reseller, Brand Protection, Others), and one-size-fits-all or overly prescriptive guidance does not properly consider the range of registrar business models	In relation to 10), proposed edit that aims to address Sarah's edit and Brian's concern. The group has discussed that guidance cannot be prescriptive but as noted by Brian, policy recommendations are different as they are intended to ensure uniformity in their application and outcomes.	Suggestions: 8. Change "Reseller" to "Wholesale" (RrSG – Sarah) 9. Change "does not" in second sentence to "may not (IPC – Brian) 10. Replace "Registrars desire" with "policy recommendations must provide

[20] Please note that the exact details of how this recommendation will be implemented are to be determined by ICANN org in collaboration with the Implementation Review Team, once the ICANN Board has approved the recommendations.

and the various process flows the different business models may require. Instead, Registrars desire flexibility to implement differentiation in a manner that best suits their business model and reduces the risks associated with differentiation to an acceptable level for that particular Registrar.		Registrars the" (RrSG – Sarah). Policy recommendations are about outcomes and not necessarily methods. We must hold all registrars to the same outcomes. (IPC – Brian)
Proposed Guidance The EPDP Team would like to put forward the following guidance to assist Registrars who want to differentiate between registrations of natural and legal persons, or those of legal persons containing personal and non-personal data.	Agreement during 27/4 meeting to instead of including this language to include the full advice received from Bird & Bird in an annex to the Initial Report.	11. Prior to this section, we suggest to add an italicized section above to include relevant portions of legal advice: 11.8 There may even be an argument, based on EU Court of Justice ("CJEU") caselaw, that this is a situation where Contracted Parties should generally only be liable should they fail to properly address a complaint about the data – i.e. only once they are put on notice about the alleged illegality and thereby have an opportunity to "verify" the merits of the complaint. This bears some parallels to other EU liability regimes for operators of services online that process – unwittingly – content that violates EU law. As discussed at footnote 6 below, this is arguably recognised in (at least some) decisions of GDPR supervisory authorities." (IPC – Brian)

1. Differentiation between the data sets of natural and legal persons could typically occur at the time of registration, However, some EPDP Team members have indicated that this may not be possible or practical in all circumstances, including for certain registrar business models.	Updated as discussed during 27/4 meeting to reflect that it is desirable to differentiate at the time of registration, but to recognize that for some business models the first opportunity to interact with the Registrant may happen after registration. Moved the second sentence to the Registrar Business Models section as an example of why a one-size-fits all approach may not work.	Suggestions: 12. Suggest moving to "BusinessBusines models" section (RrSG – Sarah) 13. Change "could typically" to "should" (IPC – Brian) Disagree (RrSG – Sarah) 14. Add to the first sentence "by allowing registrants to self-identifyself-idenfiy as legal persons if they wish to do so.". We want to emphasize that the process is allowing registrants to designate themselves as legal, but this does not necessarily ask them to declare whether they are claiming to be natural persons. (NCSG – Milton) 15. In relation to the second sentence: "From a user standpoint, I think it makes the most sense to do it at the time of registration, when else would it happen?" (NCSG – Milton) 16. Change "could" to "should" and agree with MM's point (GAC- Laureen) 17. In relation to the second sentence: This does not seem to belong here (I think SW flagged this too). (GAC – Laureen)
2.	Added new guidance as suggested by Sarah with updates as proposed and reference to EDPB guideline on data protection by design and by default to provide additional context.	Suggestion: 18. Add guidance: "2. Any differentiation process must ensure that the data of natural persons is protected, consistent

		with a “data protection by design and by default” approach (RrSG – Sarah) ● Is this consistent with Milton’s principles? There is a lot to unpack here as data that is published or disclosed may still be "protected" in many ways. Combining this broad concept of "protected" with "must" may be problematic. (IPC – Brian) ● ok, should we say "redacted from the public RDDS unless the data subject has provided their consent to publish" instead? (RrSG – Sarah) ● Don't disagree with the principle, but the term "differentiation process" makes it sound as if differentiation is something that CPs do to the RNH, rather than something RNH does for itself. We wish to avoid those connotations (NCSG – Milton) ● Disagree that the phrase "differentiation process" indicates who is doing the process but open to rewording, if you have suggestions? (RrSG – Sarah) ● The reference to “data protection by design and by default” may not be easi;y understood and it’s not clear what obligations this would impose.

		Suggest further discussion. (GAC-Laureen)
3. As part of the implementation, Registrars should consider using a type of flag in the RDDS or their own data sets that would indicate the type of data it concerns (personal or non-personal data) as this could facilitate review of disclosure requests via SSAD and the return of non-personal data of legal persons by systems other than SSAD (such as Whois or RDAP). A flagging mechanism could also assist in indicating changes to the type of data in the registration data field(s).	No changes made at this point – EPDP Team to consider whether further specificity is necessary or whether that would be too prescriptive. Alternatively, EPDP Team could consider providing further examples of how this could be done in practice?	•
4. In all of the below scenarios, clear communication and guidance should be provided to the registrant (data subject) by the Registrar concerning the possible consequences of: 1) identifying a data set as being of a natural or a legal person, 2) confirming the presence of personal data or non-personal data, and 3) providing consent[21]. This is also consistent with	Updated as suggested by Milton. Added footnote to clarify that the registrant may not always be the data subject (Staff Support Team suggestionproposed clarifying edit).	Suggestions / Comments: Delete "natural or a" - Our understanding of the appropriate way to handle this is to allow registrants to self-designate as legal persons if they want to, but not to require a positive attestation that they are a natural person. In other words, the choice should not be /_/ Legal /_/ Natural but rather /_/ Legal. /_/ Choose not to declare. (NCSG – Milton)

[21] See also https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

section 3.7.7.4 of the Registrar Accreditation Agreement (RAA).		
5. Registrants (data subjects) must have an easy means to correct possible mistakes.	No updates made at this point – ALAC to confirm that proposed language would replace 1-5 and indicate why this update is recommended to replace the current language (what is missing that should be included).	
6. Distinguishing between legal and natural person registrants alone may not be dispositive of how the information should be treated (made public or masked), as the data provided by legal persons may include personal data that is protected under data protection law, such as GDPR.	Moved from background section to guidance section as discussed during 27 April meeting.	

Current Language	**Staff Support Team – Rationale for changes made**	**Issues Raised / To Consider by EPDP Team**
Example scenarios	EPDP Team to consider whether or not these scenarios should remain or whether they should be replaced by the RrSG table (see below) as suggested by ALAC.	Suggestions: Suggest adding a note that these scenarios are examples but are not part of the formal guidance (RrSG – Sarah)
The EPDP Team has identified three different high-level scenarios for how differentiation could occur based on who is responsible and the timing of such differentiation. It should		

be noted that other approaches and/or a combination of these may be possible. 4. Data subject self-identification at time of data collection / registration a. The Registrar informs the Registrant (per guidance #3 above) and requests the Registrant (data subject) at the moment of Registration data collection to designate legal or natural person type. The Registrar must also request the Registrant to confirm whether only non-personal data is provided for legal person type.[22]		
b. If the Registrant (data subject) has selected legal person and has provided a confirmation that the registration data does not include any personal data, the Registrar should (i) contact the provided contact details to verify the Registrant claim[23] (ii) set the registration data set to automated disclosure in response to SSAD queries and (iii) publish the data		

[22] Note that the confirmation that only non-personal data is provided could also happen at a later point in time. However, until the Registrant confirms that no personal data is present in the registration data, the Registrar does not set the registration data to automated disclosure.

[23] Per the guidance provided by Bird & Bird, "this verification method is advisable, and will help reduce risk. That risk reduction will be greatest if there is a reasonable grace period within which the objection can be lodged, before the data in question is published in the Registration Data" and "requiring an affirmative response to verification mailings seems over-cautious, unless and until studies show that the measures adopted are failing to keep very substantial amounts of personal data out of published Registration Data. However, if a verification email "bounces" (i.e. a Contracting Party knows it was not delivered), then it would be better if publication does not proceed".

(to provide Registration Data in the publicly accessible Registration Data Directory Services).		
c. If the Registrant (data subject) has selected natural person or has confirmed that personal data is present, the Registrar does not set that registration data to automated Disclosure and Publication, unless the data subject consents to Publication.[24]		
~~d. If the Registrant (data subject) makes any substantive change to the registration data, the Registrar is expected to confirm that these updates do not result in changes to the registrant type or the previous confirmation of whether only non-personal data is provided for legal person type. If the updates do result in changes, Registrar must repeat Steps a-c above.~~	Deleted as suggested by RrSG. See also update to scenario 2 that incorporates this aspect as a result.	19. This is too prescriptive. Guidance should be that if any changes are made then the data is treated as natural-person data until the Registrant indicates otherwise via repetition of steps a-c. We also caution that a complex and high-touch process such as the one proposed here will drive away data subjects from the registration data update process and encourage them to abandon the domain data update process entirely, resulting in inaccurate data at a higher rate than if the whole process did not exist. (RrSG – Sarah) EPDP Team to discuss. This was updated following input during the previous meeting with the

[24] Note that the data subject may not be the party executing the process but may have requested a third party to do so. In such circumstance consent may not be possible.

		suggestion that it would make sense to ask a registrant when updates are made whether these updates change the data type instead of reverting to a default position. (Staff support team) Upon further consideration, we think this item d should be removed entirely, as it does not align with the scenario (at the time of data collection/registration). Instead this item reflects scenario 2 which is sufficiently outlined and does not need any more info. (RrSG – Sarah)
5. Data subject self-identification after initial collection	EPDP Team to discuss / consider timelines for this scenario.	Suggestions: 20. Some timelines would be helpful for this scenario (GAC – Laureen). Agree that timeline would be helpful. Instead of "after initial collection " it should say "at time when registration data is updated" to be clear that this is the scenario for existing registrations whenever their data are updated. We also emphasize that this is for moving forward only, not backfilling existing registrations which were created prior to this policy being implemented. (RrSG – Sarah)
a. The Registrar collects Registration Data and provisionally redacts the data.		

b. The Registrar informs the Registrant (per guidance #3 above) and requests the Registrant (data subject) to designate legal or natural person type. The Registrar must also request the Registrant to confirm whether only non-personal data is provided for legal person type.[25] c. Registrant (data subject) indicates legal or natural person type and whether or not the registration contains personal information after registration is completed. For example, the Registrant may confirm person type at the time of initial data verification, in response to its receipt of the Whois data reminder email for existing registrations, or through a separate notice requesting self-identification.[26] d. If the data subject identifies as a legal person and confirms that the registration data does not include personal data, the Registrar should (i) contact the provided contact details to verify the Registrant		

[25] Note that the confirmation that only non-personal data is provided could also happen at a later point in time. However, until the Registrant confirms that no personal data is present in the registration data, the Registrar does not set the registration data to automated disclosure.
[26] Note, the implementation of EPDP Phase 1, recommendation #12 (Organization Field) may facilitate the process of self-identification.

claim[27] (ii) set the registration data set to automated disclosure in response to SSAD queries and (iii) publish the data.		
6. Registrar determines type based on data provided	EPDP Team to consider whether this scenario should be deleted and/or whether further updates can be considered to address NCSG concerns.	Question: 21. Should this scenario be deleted? Note, NCSG objects to inclusion of this scenario, unless Registrar is barred from inferring registration type. (Staff Support Team) We still want it to be deleted (NCSG – Milton) The CPH is happy to continue discussing ways to address the NCSG's concerns on this scenario. (CPH – Amr)
a. The Registrar collects Registration Data and provisionally redacts the data. b. The Registrar uses collected data to infer legal or natural person type.[28] c. If legal person is inferred by the Registrar and subsequently the Registrant (data subject) is informed (per guidance #3 above) and confirms that no personal data is present, the Registrar should (i) contact the provided contact details to verify the		

[27] Per the guidance provided by Bird & Bird, "this verification method is advisable, and will help reduce risk. That risk reduction will be greatest if there is a reasonable grace period within which the objection can be lodged, before the data in question is published in the Registration Data" and "requiring an affirmative response to verification mailings seems over-cautious, unless and until studies show that the measures adopted are failing to keep very substantial amounts of personal data out of published Registration Data. However, if a verification email "bounces" (i.e. a Contracting Party knows it was not delivered), then it would be better if publication does not proceed".

[28] Some EPDP Team members have noted that there may be risks for the Registrar to infer a differentiation without involvement of the Registrant (data subject).

Registrant claim[29] (ii) set the registration data set to automated disclosure in response to SSAD queries and (iii) publish the data. d. If the Registrar has inferred natural person or has detected personal data, the Registrar must not disclose registration data unless the Registrant provides consent for publication or the Registrar Discloses the data in response to a legitimate disclosure request.		
Registrars shall not be prohibited from voluntarily utilizing a third party to verify that a registrant has correctly identified its data[30], provided that such verification is compliant with applicable data protection regulations.	EPDP Team to consider the concept of third party verification in the context of scenario 3 and concerns expressed by NCSG.	Comments: 22. Proposed language changes from Volker were applied to not disallow this option but not to indicate this is recommended (Staff Support Team). NCSG objects to this even more. This makes scenario 3 ten times worse. (NCSG – Milton)
The EPDP Team recognizes that in all of the above scenarios, there is the possibility of misidentification, which may result in the inadvertent disclosure of personal data. In		

[29] Per the guidance provided by Bird & Bird, "this verification method is advisable, and will help reduce risk. That risk reduction will be greatest if there is a reasonable grace period within which the objection can be lodged, before the data in question is published in the Registration Data" and "requiring an affirmative response to verification mailings seems over-cautious, unless and until studies show that the measures adopted are failing to keep very substantial amounts of personal data out of published Registration Data. However, if a verification email "bounces" (i.e. a Contracting Party knows it was not delivered), then it would be better if publication does not proceed".

[30] Per the guidance provided by Bird & Bird, "a company registration number may be another means of verifying legal personhood".

this regard, Bird & Bird has noted the following: *11.11.1 If the (person representing the) Registrant incorrectly characterises personal data as non-personal, then the verification process this triggers should confer reasonable protection against GDPR Accuracy Principle liability for Contracted Parties, as explained at paragraph 11.7 above, as might the legal argument set out at paragraph 11.8 above.* *11.11.2 Alternatively, if the (person representing the) Registrant incorrectly characterises non-personal data as personal data, then whether or not they subsequently consent to its publication, the data would still not actually be personal data, so GDPR liability cannot arise.* (…) *13. However, in our view the risk to Contracted Parties seems low, if they take the measures described in the question presented, to avoid personal*		

data being (or if reported, staying) published in Registration Data. (…) *14.3 The data in question is likely to be low sensitivity. The scenario being envisaged here (mistaken inclusion of personal data in published Registration Data) seems to be most likely to occur when a legal entity (e.g. a company or non-profit organisation) is registering / maintaining its own domains. In those scenarios, we assume the personal data that could be disclosed would ordinarily relate to an employee's work details (e.g. a company email address), not an individual's private life. Although the GDPR confers protection even in the workplace, the data in question here may arguably be less capable of causing harm to an individual than data relating to the data subject's private life.*[31]		

[31] As explained above, we have understood this question to be asking about scenarios where Registrants are legal persons, as per the EDPB quote at paragraph 1. In respect of individual (natural person) Registrants, the issues will be largely similar: if a natural person incorrectly states that their data is not personal data, then (i) the verification measures should prevent the data from being published, since they will give the data subject an opportunity to correct their mistake; (ii) the mitigating factors and legal arguments described at paragraphs 11.7 and 11.8 and paragraphs 14.1 - 14.6 here, should confer reasonable legal protection for Contracted Parties.

(…) *18. We cannot exclude the possibility of some courts or regulators seeing things differently. Even then, an order to correct the issue (likely accompanied by a reasonable period in which to implement changes), rather than a fine, seems most likely, having regard to the GDPR Article 83(2) factors discussed at paragraph 8 above. Having checked in a selection of Member States, we can find no examples of enforcement in relation to this. Accordingly, there is little guidance available besides what is set out in the GDPR itself.* As a result, the EPDP Team recommends that Contracted Parties who choose to differentiate based on person type SHOULD follow the guidance above and clearly document all data processing steps. However, it is not the role or responsibility of the EPDP Team to make a final determination with regard to the legal risks, as that responsibility ultimately belongs to the data controller.		

[Proposed addition by RrSG]

This chart provides guidance for how a Registrar could comply with GDPR principles in each of the three example scenarios (see section below), along with some notes about risks present for various options.

Principle	Data subject self-identification at time of data collection resulting in publication of non-personal data	Data subject self-identification after initial data collection resulting in publication of non-personal data	Registrar determines type based on data provided resulting in publication of non-personal data
Lawfulness, Fairness and Transparency: Controller must identify their legal basis (or bases) for processing data and ensure the data subject is aware of the processing prior to when it occurs. If the legal basis is consent, then consent must be obtained prior to the processing. See also: Transparency: RAA 3.7.7.4 Consent: RAA 3.7.7.5	Identify and document legal basis for each processing activity (collection, retention, publication, erasure); provide explanation to data subject when data is collected and data subject selects person type. Risk: Data subject identifies person type/provides consent on behalf of a third party (Bird & Bird Memo II on Consent)	Identify and document legal basis for each processing activity (collection, retention, publication, erasure); provide explanation at the time when data subject self-identifies (post collection) and when option to change or correct self-designation is provided. Risk: Data subject identifies person type/provides consent on behalf of a third	Identify and document legal basis for each processing activity (collection, retention, publication, erasure); provide explanation at the time when data is collected and person type is inferred. Risk: Registrar identification post-collection does not allow for pre-processing disclosure to data subject.

		party (Bird & Bird Memo II on Consent)	
Purpose Limitation: Controller must ensure that data is not processed beyond the purposes disclosed to the data subject See also: RAA 3.7.7.4.1, 3.7.7.4.2, EPDP Phase 1 and Phase 2 Addendum Purposes	All relevant processing activities (including post-publication activities) must be included in the explanation to the data subject. Risk: post-publication processing may be unknown to both the controller and the data subject and thus cannot be adequately disclosed	All relevant processing activities (including post-publication activities) must be included in the explanation to the data subject. Risk: post-publication processing may be unknown to both the controller and the data subject and thus cannot be adequately disclosed	All relevant processing activities (including post-publication activities) must be included in the explanation to the data subject. Risk: post-publication processing may be unknown to both the controller and the data subject and thus cannot be adequately disclosed
Data Minimisation: Controller must ensure that no data is collected/processed beyond what is required to achieve the identified purpose(s) See also: RAA 3.7.7.4.3, EPDP Phase 1 exercise justifying all data elements collected	Only the minimum required data must be collected and published.	Only the minimum required data must be collected and published.	Only the minimum required data must be collected and published.

Accuracy: Controller must take all reasonable steps to ensure data subject can keep person type data updated and accurate See also: WHOIS Accuracy Program Specification	Allow the data subject to provide person type information and make updates when needed.	Allow the data subject to provide person type information and make updates when needed.	Allow the data subject to view their inferred person type designation and make updates when needed. Risk: registrar incorrectly infers data subject person type, resulting in improper publication of natural person data
Storage Limitation: Controller must retain data only as long as is necessary for the purposes for which the data are processed See also: RAA 3.4, EPDP Phase 1 data retention requirement	Ensure that personal data is erased as soon as it is no longer required to fulfill the processing purposes Risk: When data is public and erasure is required, controller has obligation to inform other controllers that the data subject has requested erasure.	Ensure that personal data is erased as soon as it is no longer required to fulfill the processing purposes Risk: When data is public and erasure is required, controller has obligation to inform other controllers that the data subject has requested erasure.	Ensure that personal data is erased as soon as it is no longer required to fulfill the processing purposes Risk: registrar incorrectly infers data subject person type, resulting in disclosure of data which cannot be recalled and redacted; when data is public and erasure is required, controller has obligation to inform other controllers that the data subject has requested erasure.

Integrity and Confidentiality: Controller must process personal data in a way that ensures security, protects against unlawful processing See also: RAA 3.4.1 “securely maintain, in its own electronic database…”	Ensure that only non-personal data is published	Ensure that only non-personal data is published	Ensure that only non-personal data is published. Risk: publishing personal data due to mis-identification
Accountability: Controller must be able to demonstrate that they comply with GDPR Principles	Document processing activities with explanation of how the chosen implementation complies with GDPR Principles for processing data	Document processing activities with explanation of how the chosen implementation complies with GDPR Principles for processing data	Document processing activities with explanation of how the chosen implementation complies with GDPR Principles for processing data

For reference: GAC revised Proposal incorporating recent input from Rgr and Principles from MM

1. Distinguish between natural and legal persons in a manner that does not compromise privacy rights
    a.

i. Registrars decide how to engage with customers to explain what Natural/Legal entities are and the consequences of identifying as a legal entity.

2. Distinguish between personal and non-personal data of legal persons.

risks to registrant

1.