3 EPDP Team Responses to Council Questions & Preliminary Recommendations

The EPDP Team will not finalize its responses to the Council questions and recommendations to the GNSO Council until it has conducted a thorough review of the comments received during the public comment period on this Initial Report. At the time of publication of this Report, no formal consensus call has been taken on these responses and preliminary recommendations; however, the EPDP Team Chair made the following preliminary assessment: [placeholder]. This Initial Report did receive the support of the EPDP Team for publication for public comment.[1] Where applicable, differing positions have been reflected in the Report.

3. 1 Legal vs 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,[2] (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] Following a review of public comments, the EPDP Team will take a formal consensus call before producing its Final Report.

[2] 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.

EPDP Team response to Question i.

The EPDP Team discussed this question extensively. As a starting point, the EPDP Team notes that the GDPR[3] and many other data protection legislations set out requirements for protecting personal data of natural persons. It does not protect the non-personal data of legal persons. At the same time, the EPDP Team recognizes that the European Data Protection Board ("EDPB") has advised ICANN in a July 2018 letter that "the mere fact that a registrant is a legal person does not necessarily justify unlimited publication of personal data relating to natural persons who work for or represent that organization," and that "personal data identifying individual employees (or third parties) acting on behalf of the registrant should not be made publicly available by default in the context of WHOIS"[4].

The EPDP Team recognizes that there are different perspectives within the EPDP Team on this question:

- Some EPDP Team members are of the view that differentiation should be required for many reasons that benefit the public. First, a significant percentage of domain names are registered by legal entities and the GDPR generally does not protect their domain name registration data. Further, to the extent that personal information is included in such registration data, the legal guidance received indicates that it is likely to be "low sensitivity" because it relates to an employee's work details rather than their private life. Given the surge in internet-based crimes (including ransomware demands that cripples public infrastructure), publishing the registration data of legal entities would aid law enforcement, consumer protection, and cybersecurity professionals' ability to quickly and more effectively investigate illicit activities facilitated by the DNS. Second, requiring registrars to publish the domain name registration data of legal entities would also significantly reduce the challenges associated with obtaining responses to disclosure. Third, publishing legal persons' data based on differentiation instead of consent significantly reduces the CPs liability. Hence, publishing legal persons' data based on differentiation rather than consent could be considered a best practice. Finally, the legal guidance received stated that if the proper safeguards are followed, the legal risks associated with such publication, even in the event of inadvertent mistakes, seem low. Hence, on balance, the public interest favors differentiating between registrations of legal and natural persons.
- In contrast, others EPDP Team members are of the view that the existing Phase 1 recommendation, which already permits those who wish to differentiate to do so, strikes the appropriate balance by (i) allowing parties to control and mitigate their own legal risk, and (ii) ensuring that parties have the flexibility to quickly respond to

[3] "This Regulation 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."

[4] Andrea Jelinek, European Data Protection Board, Letter to Goran Marby dated 5 July 2018, available at https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf

Deleted: q

Deleted: and recognizes that there are different perspectives within the EPDP Team on this question

Deleted: Nevertheless, some EPDP Team members are of the view that differentiation should be required 1) to ensure that there is no redaction of data that is not protected by GDPR or may not be protected by other data privacy legislation, 2) because it is in the public interest, 3) to address problems and complaints reported due to redaction of data, 4) publishing legal persons' data based on differentiation instead of consent significantly reduces the CPs liability. Hence, publishing legal persons' data based on differentiation rather than consent could be considered good practice. ¶

Deleted: <#>¶

Formatted: Font: (Default) Calibri

changes in future laws impacting the publication of legal person data without requiring additional policy making. Moreover, these EPDP Team members assert that there have not been sufficient reasons demonstrated justifying a change in the Phase 1 recommendation making differentiation between legal and natural person registrants mandatory for Contracted Parties. In their view, no evidence has been presented identifying the problems that mandatory differentiation would solve, or indeed if mandatory differentiation would solve them at all. Such a change would likely result in operational and financial burdens, which would need to be borne by Contracted Parties that do not have a uniform capacity to bear them. Additionally, these EPDP Team members are of the view that such a change would result in increasing their legal risk as controllers of the data, particularly with regard to the issues specifically identified by the EDPB regarding natural person data that may exist in a legal person registrant's registration data. In the absence of a sufficient purpose to change the phase 1 recommendation, these EPDP Team members believe that Contracted Parties need to maintain the flexibility to choose whether they will bear the costs and potential legal risk associated with differentiation. Some members of the EPDP Team agree that there are a number of factors that may affect these viewpoints over time such as possible legislative changes which relate to the processing of personal data used in domain names (including, for example, the Revised Directive on Security of Network and Information Systems (NIS2)). Additionally, some EPDP Team members note the possible adoption of the System for Standardized Access/Disclosure to non-public registration data (SSAD) or alternative differentiated access models may also affect viewpoints over time.

Deleted: <#>

As a result, the EPDP Team recommends that:

Preliminary Rec #1.
No changes are recommended 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"). Nevertheless, the EPDP Team recommends that the GNSO Council monitors developments in relation to the adoption and implementation of relevant legislative changes (for example, NIS2), relevant decisions by pertinent tribunals and data protection authorities, as well as the possible adoption of the SSAD to determine if/when a reconsideration of this question (whether changes are required to the EPDP Phase 1 recommendation "Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so") is warranted. The GNSO Council is expected to consider not only input on this question and any new information from GNSO SG/Cs but also ICANN SO/ACs to help inform a decision on if/when this question is expected to be reconsidered.

Deleted: T

The EPDP Team does recognize that there may be a need to facilitate and harmonize practices for those Contracted Parties who do decide to differentiate between legal and natural persons. The EPDP Team would welcome further input on why harmonization of practices may or may not be beneficial.

To facilitate differentiation, the EPDP Team has developed the guidance that can be found in the section below.[5] In this guidance, the EPDP Team suggests that Registrars may consider the use of a standardized data element that would indicate the type of registrant concerned (legal/natural) and the type of data of legal registrants it concerns (personal/non-personal). This concept of identifying the type of domain name registration data involved is also referenced in EPDP Phase 2 recommendation #9.9.4 (automated response to disclosure requests), which indicates that a Contracted Party needs to have a mechanism to identify that a registration record does not contain any personal data.

In the following recommendation, the EPDP Team outlines how a CP that wants to differentiate can do so by using a standardized data element. Some EPDP Team members are of the view that the use of such a standardized data element should be obligatory for those Contracted Parties that decide to differentiate, while other EPDP Team members are of the view that because there is no requirement to differentiate, there should not be a requirement to use a standardized data element, and a Contracted Party should be able to determine itself how to implement such a differentiation[6]. The EPDP Team hopes to obtain further input on this question during the public comment period of whether 1) a standardized data element MUST be available for a Contracted Party to use, and 2) such a standardized data element MUST be used by those that want to differentiate. Aspects of the recommendation that the EPDP Team is looking for specific input on having been marked with *, indicating the options that are under consideration.

Deleted: must

Deleted: must

The EPDP Team recommends that:

Preliminary Rec #2.
The following additions are made to the EPDP Phase 1 recommendations:

Recommendation #5

The following optional data element (optional for the Registrar to offer to the Registrant and collect) is added to the data elements table:

[5] Note, the NCSG members believe that the EPDP Team should not be providing guidance as such. These members are of the view that it is best for the Contracted Parties to develop guidance on their own and provide the same to their peers.
[6] The Registry Stakeholder Group team members have expressed a specific objection to the inclusion of this preliminary recommendation. In their view, the more acceptable option is to include such a suggestion relating to consistent labelling and handling of potential flags within the body of the voluntary guidance (e.g. Preliminary Recommendation #3.3).

Data Elements (Collected & Generated*)	Collection Logic
Registrant Legal Person (Yes/No/Unspecified[7])	MAY / MUST, IF Contracted Party chooses to differentiate*

For the purpose of the Legal person and non-personal data field, which is optional for the Registrar to provide to the Registrant to self-designate, Registrars should advise the Registered Name Holder at the time of registration what the consequences are of self-designating as a legal or a natural person and to provide non-personal data only (or provide appropriate consent if personal data is involved), consistent with preliminary recommendation #3, point 4.

Deleted: are to

Recommendation #7

Transfer of Data Elements from Registrar to Registry:

Data Elements (Collected & Generated*)	Transfer Logic
Registrant Legal Person (Yes/No/Unspecified)	MAY

Recommendation #8

Transfer of Data Elements by Registries and Registrars to data escrow providers

For Registrars:

Data Elements (Collected & Generated*)	Transfer Logic
Registrant Legal Person (Yes/No/Unspecified)	MAY

Deleted: Collection

[7] "Unspecified" means that no self-designation has been indicated by the Registered Name Holder or determined by the Contracted Party, that the status of self-designation is unknown, or that the status may be in the process of being confirmed. It does not imply that the information provided is inaccurate. The value of unspecified is the default until either the RNH or Contracted Party perform a procedure at the discretion of the Contracted Party, that would change the value to a YES or a NO.

For Registries:

Data Elements (Collected & Generated*)	Transfer Logic
Registrant Legal Person (Yes/No/Unspecified)	MAY

Deleted: Collection

Recommendation #10

The EPDP Team recommends that redaction must be applied as follows to the data element IF collected:

Data Elements (Collected & Generated*)	Redacted	Disclosure Logic
Registrant Legal Person (Yes/No/Unspecified)	NO / YES**	MUST / MAY**

**There are different views within the EPDP Team on whether this data element would need to be redacted in the public RDDS. Some members, for example, believe this data element should be redacted in public RDDS but provided to the SSAD. Other members believe this data element should be published in the public RDDS. As a result, the EPDP Team invites those providing input during the public comment period to provide their view on this question and, in particular, the rationale for why this data element should be redacted or not and whether the choice to redact or not should be left to the Contracted Party.

The EPDP Team recommends that the applicable updates are made to the Registry Registration Data Directory Services Consistent Labeling and Display Policy and the RDAP profile consistent with this recommendation. The EPDP Team expects ICANN org to consult with the EPDP Phase 2a IRT, or the IRT that has been assigned the responsibility for implementing this recommendation, and if applicable the GNSO Council, about these changes.

For clarity, the existence of this standardized data element does not require a Contracted Party to differentiate between legal / natural person type or personal / non-personal data.[8] As part of the implementation, it should be considered whether for those Contracted Parties that choose not to differentiate, the data field is not visible in RDDS or automatically set to 'unspecified'.

Deleted: is additional data element does NOT require a Contracted Party to make use of this ability to differentiate between legal / natural person type or personal / non-personal data

[8] The personal/non-personal distinction only applies/is relevant for registrants who have self-identified as legal persons.

EPDP Team response to Question ii.

Deleted: q

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 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.
D. Although the GDPR does not cover the processing of personal data which concerns legal persons, the following GDPR principles may still apply if personal data is processed as part of the differentiation process and should be factored in as appropriate by Contracted Parties:
    a. 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.
    b. Purpose Limitation: Controller must ensure that data is not processed

beyond the purposes disclosed to the data subject

c. Data Minimization: Controller must ensure that no data is collected / processed beyond what is required to achieve the identified purpose(s)
d. Accountability: Controller must be able to demonstrate that they comply with GDPR Principles.

Relevant EPDP Phase 1 Recommendations[9]

E. Per EPDP Phase 1[10] 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".
F. 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

G. Per Phase 2[11] 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.[12]
H. 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

I. 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 should provide Registrars the flexibility to implement differentiation in a manner that best suits

Deleted: must

[9] Note, EPDP Phase 1 recommendation #12 concerning the Organization field may, once implemented, also assist Contracted Parties in differentiating between legal and natural persons, should they choose to.
[10] 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.
[11] Note that the EPDP Phase 2 recommendations are with the ICANN Board for its consideration / approval.
[12] 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.

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 practical in all circumstances, including for certain registrar business models.

Proposed Guidance[13] [14]

Preliminary Rec #3.
The EPDP Team recommends that Contracted Parties who choose to differentiate based on person type SHOULD follow the guidance[15] below 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(s).

1. Registrants should be allowed to self-identify as natural or legal persons. Registrars should convey this option for Registrants to self-identify as natural or legal persons (i) at the time of registration, or without undue delay after registration,[16] and (ii) at the time the Registrant updates its contact information or without undue delay after the contact information is updated.
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, consistent with the "data protection by design and by default" approach set forth in Article 25 of the GDPR.
3. As part of the implementation, Registrars should consider using a standardized data element in the RDDS, SSAD or their own data sets that would indicate the type of person it concerns (natural or legal) and, if legal, also the type of data it concerns (personal or non-personal data. Such flagging would facilitate review of disclosure requests and automation requirements 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 may also assist in indicating changes to the type of data in the registration data field(s).

[13] Note, the NCSG members believe that the EPDP Team should not be providing guidance as such. These members are of the view that it is best for the Contracted Parties to develop guidance on their own and provide the same to their peers. At the same time, the IPC, ALAC and GAC members have advocated that there should be mandatory requirements i.e. consensus policy, not merely guidance/best practices.
[14] Some EPDP Team members have indicated a preference for using the term "best practices", while other EPDP Team members have indicated that the development of "best practices" is typically reserved for industry bodies. ICANN org in its response (see hereunder) has indicated that from an implementation perspective, there would not be a difference whether this is called "guidance" or "best practice". Commenters on the Initial Report are encouraged to weigh in on what terminology is deemed most appropriate and why.
[15] Please note that the ICANN org liaisons provided the EPDP Team with the following feedback on how this guidance would be implemented once adopted: https://mm.icann.org/pipermail/gnso-epdp-team/2021-May/003904.html.
[16] For clarity, registrars should ensure that if the Registrant is not given the option to self-identify at the time of registration, the option should be provided no later than 15 days from the date of registration.

4. Registrars should ensure that they clearly communicate the nature and consequences of identifying as a legal person. These communications should include:
    a. an explanation of what a legal person is in plain language that is easy to understand;
    b. guidance to the registrant (data subject)[17] by the Registrar concerning the possible consequences of:
        i. identifying their domain name registration data as being of a legal person,
        ii. confirming the presence of personal data or non-personal data, and
        iii. providing consent[18]. This is also consistent with section 3.7.7.4 of the Registrar Accreditation Agreement (RAA).
5. [If the Registrants identify as legal persons and confirm that their registration data does not include personal data, then Registrars should publish the Registration Data in the publicly accessible Registration Data Directory Services.]
6. Registrants (data subjects) must have an easy means to correct possible mistakes.
7. 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.

Deleted: must

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.[19]
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

[17] 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.
[18] See also https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf
[19] 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.

Registrar should (i) contact the provided contact details to verify the Registrant claim[20] (ii) set the registration data set to automated disclosure in response to SSAD queries and (iii) 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.[21]

2. Data subject self-identification at time when registration is updated[22]

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 should also request the Registrant to confirm whether only non-personal data is provided for legal person type.[23]

c. Registrant (data subject) indicates legal or natural person type and whether or not the registration contains personal information after update 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.[24]

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[25] (ii) set the registration data set to automated disclosure in response to SSAD queries and (iii) publish the data.

3. Registrar determines registrant's type based on data provided

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

Deleted: registration

[20] 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".

[21] 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 to document.

[22] It is the expectation that for this scenario a similar timeline is followed as currently applies in the WHOIS Accuracy Specification of the Registrar Accreditation Agreement (see https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#whois-accuracy).

[23] 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.

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

[25] 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".

b. The Registrar uses collected data to infer legal or natural person type.[26]
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[27] (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 should not disclose registration data unless the Registrant provides consent for publication or the Registrar Discloses the data in response to a legitimate disclosure request.

Deleted: must

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*

[26] 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).
[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".

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.[28]

(…)

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.

3.2 Feasibility of Unique Contacts

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

i. Whether or not unique contacts to have a uniform anonymized email address is feasible, and if feasible, whether it should be a requirement.
ii. If feasible, but not a requirement, what guidance, if any, can be provided to Contracted Parties who may want to implement uniform anonymized email addresses.

The Council also indicated that "Groups that requested additional time to consider this topic, which include ALAC, GAC and SSAC, will be responsible to come forward with concrete proposals to address this topic"[29].

In addressing these questions, the EPDP Team started with a review of the legal guidance received during Phase 1 and considered possible proposals that could provide sufficient safeguards to address issues flagged in the legal memo.

The EPDP Team noted how an anonymized email address was utilized had an impact on the safeguards needed and the possible impacts on the data subjects and thus the feasibility.

[28] 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.

[29] https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-2-priority-2-items-10sep20-en.pdf

The team considered the effects and benefits of two uses of such a contact, in line with the two distinct goals stated by those advocating for unique contacts, namely 1) the ability to quickly and effectively contact the Registrant, and 2) correlation between registrations registered by the same registrant.

The EPDP Team also observed that the terminology used in the context of this discussion could benefit from further precision. The EPDP Team tasked the legal committee with proposing both updated terminology and reviewing clarifying questions to send to Bird & Bird. The legal committee proposed a set of working definitions, which it submitted to the EPDP Team on 23 February 2021 (see here). In addition, the legal committee developed a set of follow up questions which it submitted to Bird & Bird, and Bird & Bird provided a response on 9 April 2021. The EPDP Team considered this legal guidance in the development of its response to the Council's questions.

Definitions

Following the initial review of the first charter question, the EPDP Team noted the term anonymous was misapplied in this question. The EPDP Team noted that for data to be truly anonymized under the GDPR, the data subject could not be identifiable "either by the controller or by any another person" either directly or indirectly. (See, GDPR Article 26) With this understanding, the EPDP Team chose to focus its question on the pseudonymization of data and further refined the definitions in its follow-up questions to Bird & Bird.

"Registrant-based email contact", means "an email for all domains registered by a unique registrant [sponsored by a given Registrar] OR [across Registrars], [30] which is intended to be pseudonymous[31] data when processed by non-contracted parties.[32"33]

[30] The Legal Committee was tasked with reviewing the legal guidance received during Phase 2 and determining if additional legal guidance was necessary. As an initial matter, the Legal Committee chose to refine the terminology used in its Phase 2 question; specifically, instead of referring to "anonymization" and "pseudonymization," the Legal Committee agreed to use the terms "registration-based email contact" and "registrant-based email contact" because the EPDP Team noted the previous use of "anonymization" was inconsistent with the GDPR definition of anonymous. In its formation of new definitions, the Legal Committee noted a registrant-based contact might exist within the sponsoring registrar OR across all registrars. The Legal Committee determined, however, that the question of whether the registrant-based contact should exist within the sponsoring registrar or across registrars was a policy question for the EPDP Team, not a legal question for the Legal Committee or Bird & Bird. Accordingly, the Legal Committee chose to leave both options in brackets, and Bird & Bird opined on the legality and associated risks of both options with the Phase 2A memo.

[31] Some EPDP Team members believe that pseudonymous should be changed to anonymous. It should be noted, however, the definition provided above was included in the question to and guidance from Bird & Bird.

[32] Some EPDP Team members believe "by non-contracted parties" should be changed to "by parties other than the controller". It should be noted, however, the definition provided above was included in the question to and guidance from Bird & Bird.

[33] Some EPDP Team members have suggested expanding the definition to include "OR [across TLDs operated by the same Registry Service Provider]". It should be noted, however, the definition provided above was included in the question to and guidance from Bird & Bird.

"Registration-based email contact", means “a separate single use email for each domain name registered by a unique registrant, which is intended to be anonymous data when processed by non-contracted parties.”

Note, however, that even adopting these definitions, Bird & Bird advised that either Registrant-based or Registration-based email contacts create “a high likelihood that the publication or automated disclosure of such email addresses would be considered to be the processing of personal data”.

Background Information and EPDP Team Observations

In developing its response to the Council questions, the EPDP Team would like to remind the Council and broader community of the following:

Annex to the Temporary Specification (“Important Issues for Community Consideration”)

- The Temporary Specification for gTLD Registration Data, as adopted by the ICANN Board on 17 May 2018, included the following language in the Annex titled “Important Issues for Community Consideration”:
  > “Addressing the feasibility of requiring unique contacts to have a uniform anonymized email address across domain name registrations at a given Registrar, while ensuring security/stability and meeting the requirements of Section 2.5.1 of Appendix A.”

  For reference, Appendix A, Section 2.5.1 states that: “Registrar MUST provide an email address or a web form to facilitate email communication with the relevant contact, but MUST NOT identify the contact email address or the contact itself”.

Relevant EPDP Phase 1 Recommendations

EPDP Team Recommendation #6
The EPDP Team recommends that, 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.

EPDP Team Recommendation #13
1) The EPDP Team recommends that the Registrar MUST provide an email address or a web form to facilitate email communication with the relevant contact, but MUST NOT identify the contact email address or the contact itself, unless as per Recommendation #6, the Registered Name Holder has provided consent for the publication of its email address.
2) The EPDP Team recommends Registrars MUST maintain Log Files, which shall not contain any Personal Information, and which shall contain confirmation that a relay of the communication between the requestor and the Registered Name Holder has occurred, not including the origin, recipient, or content of the message. Such records will be available to

ICANN for compliance purposes, upon request. Nothing in this recommendation should be construed to prevent the registrar from taking reasonable and appropriate action to prevent the abuse of the registrar contact process.[34]

EPDP Phase 2 consideration of this topic

The EPDP Phase 2 Final Report noted that:

> "Feasibility of unique contacts to have a uniform anonymized email address: The EPDP Team received legal guidance that indicated that the publication of uniform masked email addresses results in the publication of personal data; which indicates that wide publication of masked email addresses may not be currently feasible under the GDPR. Further work on this issue is under consideration by the GNSO Council."

EPDP Team Proposed Responses to Council Questions

i. Whether or not unique contacts to have a uniform anonymized email address is feasible, and if feasible, whether it should be a requirement.
ii. If feasible, but not a requirement, what guidance, if any, can be provided to Contracted Parties who may want to implement uniform anonymized email addresses.

EPDP Team response to Question i.

The EPDP Team recognizes that it may be technically feasible to have a registrant-based email contact or a registration-based email contact.[35] Certain stakeholders see risks and other concerns[36] that prevent the EPDP Team from making a recommendation to require Contracted Parties to make a registrant-based or registration-based email address publicly available at this point in time. The EPDP Team does note that certain stakeholder groups have expressed the benefits of 1) a registration-based email contact for contactability purposes as concerns have been expressed with the usability of web forms and 2) a registrant-based email contact for registration correlation purposes.[37]

EPDP Team response to Question ii.

[34] Examples of abuse could include, but are not limited to, requestors purposely flooding the registrar's system with voluminous and invalid contact requests. This recommendation is not intended to prevent legitimate requests.
[35] Some EPDP Team members note that even though it is technically possible, other factors related to the efforts required to implement such a feature would need to be considered to determine overall feasibility.
[36] Such as 1) It is not clear that the work involved to implement such a concept is justified by the potential benefit. 2) It is furthermore not clear that the goals, as presented, are either effectively or even best met by requiring registrant-based or registration-based email addresses.
[37] The ability to identify what domains a particular registrant has registered is important for law enforcement and cyber-security investigations of bad actors who often register many domains for malicious purposes.

[Registrars are encouraged to publish the following in the publicly accessible Registration Data Directory Services (RDDS):
A Registrant-based email contact where the Registrar can ensure appropriate safeguards for the data subject in line with relevant guidance on anonymisation techniques provided by their data protection authorities and the appended legal guidance in this recommendation.]

For those Contracted Parties who choose to provide a registrant-based or registration-based email address, either publicly or upon request, the EPDP Team recommends that those Contracted Parties review the guidance provided by Bird & Bird on this topic (see Annex E).