3 EPDP Team Responses to Council Questions & Recommendations

After reviewing public comments on the Initial Report, the EPDP Team presents its responses and recommendations for GNSO Council consideration. This Final Report states the level of consensus within the EPDP Team achieved for the different recommendations. In short:

[Summary of consensus designations]

For further details about these designations, please see section 3.6 of the GNSO Working Group Guidelines.

○ 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,[1] (2) the legal guidance provided by Bird & Bird, and (3) the substantive input provided on this topic during the public comment forum. 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.

Deleted: the public comment forum on the addendum

[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 org 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 and many other data protection legislations set out requirements for protecting personal data of natural persons. They do not protect the non-personal data of legal persons.[3] 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] For further insights into the different perspectives on this question, readers are encouraged to review the EPDP Team's Initial Report as well as the minority statements that have been appended to this report.

Deleted: 2

Deleted: It

Deleted: es

Deleted: .

The EPDP Team is putting forward the following response to the Council's instruction 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"):

> The EPDP Team did not reach consensus on recommending changes to the EPDP Phase 1 recommendation #17.1 ("Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so").

Proposal to the GNSO Council

> The EPDP Team recognizes that current and future legislative developments may require further policy work on this topic, such as to address potential conflicts with existing policy requirements and/or to consider whether there is a risk of marketplace fragmentation that needs to be addressed. At the same time, the EPDP Team recognizes that until legislation is adopted, it may not be possible to accurately assess the impact. The EPDP Team recommends the GNSO Council to follow these developments through the legislative / regulatory reports that ICANN org produces.

Deleted: either to

Deleted: and implementation plans are clear,

Deleted: expects

> Noting the current discussions and expected adoption of the Revised Directive on Security of Network and Information Systems ("NIS2"), the EPDP Team

[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

strongly encourages the GNSO Council to follow existing procedures to identify and scope possible future policy work following the adoption of NIS2 to assess whether or not further policy development is deemed desirable and/or necessary~~.~~

Differentiation Guidance

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.

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 field 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 #9.4.4 (automated response to disclosure requests).

In the following recommendation, the EPDP Team outlines how a Contracted Party that wants to differentiate can do so by using a new field or fields to capture the results of that differentiation.

Do note that some EPDP Team members are of the view that the use of such a field 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 this field, and a Contracted Party should be able to determine itself how to implement such a differentiation[6].

Recommendation #1

The EPDP Team recommends that a field or fields MUST be created to allow for differentiation between legal and natural person registration data and/or if that registration data contains personal or non-personal data. The EPDP expects that the technical community, for example the RDAP WG, will develop any necessary standards associated with such fields.

Deleted: and confirmation of EU Member State implementation plans …

Deleted: , which indicates that a Contracted Party needs to have a mechanism to identify that a registration record does not contain any personal data

Commented [MOU1]: Ask #1: EPDP Team to consider if this section as well as footnote 5, 20 and 21 can be removed if the Chair statement on consensus designations makes clear that there was significant disagreement within the group on a number of these issues and that readers are encouraged to review the minority statements to better understand the different views and perspectives.

Commented [MOU2]: Ask #2: Do these updates and this reorganization of recommendation #1 address the cannot live with items flagged? If not, how can these be addressed, factoring in the discussions to date.

Deleted: ,

Deleted: for the RDDS

Moved (insertion) [1]

[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).

This field or fields MAY[7] be used by those Contracted Parties that differentiate between legal and natural person registration data and/or if that registration data contains personal or non-personal information. For clarity, Contracted Parties MAY make use of the field(s), which means that if a Contracted Party decides not to make use of the field(s), it may be left blank or may not be present. Additionally, the field(s) is not required to be included in a RDDS response.

Deleted: that

Deleted: [8]

The SSAD, consistent with the EPDP Phase 2 recommendations MUST support the field or fields in order to facilitate integration between SSAD and the Contracted Parties' systems. These field(s) must be able to accommodate the following values:

Deleted:

Legal Status

- The legal status distinction was not made (default value)
- Unspecified – Indicating the Registered Name Holder and/or registrar didn't specify
- Registered Name Holder is a Natural person
- Registered Name Holder is a Legal person

Deleted: .

Deleted: .

Personal Data

- The presence of personal data wasn't determined (default value)
- Unspecified – Indicating the Registered Name Holder and/or registrar didn't specify
- Registration data contains personal information
- Registration data does NOT contain personal information

Moved up [1]: The EPDP expects that the technical community, for example the RDAP WG, will develop any necessary standards associated with such fields.¶

○ EPDP Team response to Question ii.

The EPDP Team 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:[9] "Publication", "Publish", and "Published" means to provide Registration Data in the publicly accessible Registration Data Directory Services.

[7] If a Contracted Party chooses to publish this field or fields in RDDS, the existing Registry Registration Data Directory Services Consistent Labelling and Display Policy is expected to apply.

[9] See https://docs.google.com/document/d/1SVFkoI6RmrVVz--RrVLSOj1bmz1qLb7_JTuvt7At4Uo/edit

- EPDP-p1-IRT:[10] "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:[11] "Disclosure" means 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, GDPR Principles, some of which are described below, may still apply if a natural person's personal data is processed as part of the differentiation process and should be factored in as appropriate by Contracted Parties. Consistent with the Principles set forth in Article 5 of the GDPR:

   a. Lawfulness, Fairness and Transparency: "Any processing of personal data should be lawful, fair, and transparent. It should be clear and transparent to individuals that personal data concerning them are collected, used, consulted or otherwise processed, and to what extent the personal data are, or will be, processed." The transparency principle "concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing[…][12][…]

[10] Ibid

[11] See https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-2-20feb19-en.pdf

[12] See: Irish Data Protection Commission guidelines on the Right to be Informed. (https://www.dataprotection.ie/en/individuals/know-your-rights/right-be-informed-transparency-article-13-1 4-

If the legal basis is consent, then "[p]roviding information to data subjects prior to obtaining their consent is essential in order to enable them to make informed decisions, understand what they are agreeing to, and for example exercise their right to withdraw their consent."[13]

b. Purpose Limitation: "Personal data shall be [. . .] collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[14]

c. Data Minimization: "Limit the amount of personal data collected to what is necessary for the purpose."[15]

d. Accountability: The GDPR's accountability principle "requires organisations to demonstrate (and, in most cases, document) the ways in which they comply with data protection principles when transacting business."[16]

Relevant EPDP Phase 1 Recommendations[17]

E. 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".

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[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

gdpr) and Article 29 Working Party Guidelines on transparency under Regulation 2016/679, Section 6 & 7 (as adopted by the EDPB) (https://ec.europa.eu/newsroom/article29/items/622227)

[13] See EDPB Guidelines, 05/2020, Guidelines 05/2020 on consent under regulation 2016/679, Section 3.3

[14] See GDPR Article 5(1)(b); see also UK Information Commissioner's Office guidelines on Purpose Limitation, (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/)

[15] See EDPB Guidelines, 04/2019, Data Protection by Design and by Default, Section 3.5 (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf) and GDPR Article 5.1 (c).

[16] See: Irish Data Protection Commission guidance on Accountability (https://www.dataprotection.ie/en/organisations/know-your-obligations/accountability-obligation); See also EDPB Guidelines, 04/2019, Data Protection by Design and by Default, Section 3.9 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[17] 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.

[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.

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

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.[20]

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 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[21] [22]

Recommendation #2

The EPDP Team recommends that Contracted Parties who choose to differentiate based on person type SHOULD follow the guidance[23] 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).

Commented [MOU3]: Ask #3: Considering the org input ("because this recommendation is for guidance only (and thus not subject to compliance enforcement), the use of should vs may wouldn't be expected to have a significant impact from the org perspective"), can the group live with leaving this as "SHOULD". If not, please provide alternative suggestions that take into account the EPDP Team's discussion.

[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.

[21] 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.

[22] 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.

[23] 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.

The GDPR protects natural persons in relation to the processing of their personal data. The 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. [Recital 14, GDPR] This generally allows for disclosure of legal persons' data because it is outside the remit of GDPR; however, when processing legal persons' data, Contracted Parties should put safeguards in place to ensure that personally identifying data about a natural person is not disclosed within data marked as a legal person, as this is an example of information that *is* within the scope of GDPR. For more information on this distinction, please refer to the letter from the European Data Protection Board, beginning on p. 4.

Deleted: ¶

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,[24] 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 or it may be published due to another lawful basis under the GDPR, 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 the field(s) described in recommendation #1 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 could 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).

Deleted: a standardized data

Deleted: element

Deleted: w

4. Registrars should ensure that they clearly communicate the nature and consequences of a registrant 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)[25] by the Registrar concerning the possible consequences of:
      i. Identifying their domain name registration data as being of a legal person;

[24] 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.

[25] 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.

ii. Confirming the presence of personal data or non-personal data, and;
iii. Providing consent.[26] 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.

Recommendation #3

The EPDP Team recommends, in line with GDPR Article 40 requirements for Codes of Conduct[27], that the above developed guidance concerning legal/natural differentiation should be considered by any future work by the relevant controllers and processors in relation to the development of a GDPR code of conduct.

This future work is expected to be carried out in an open and transparent manner, allowing for observers to follow the discussions and with the opportunity for the community to provide input before the Code of Conduct is finalized.

Commented [MOU4]: Ask#4 – please consider the updates proposed by the RrSG ("any future work **within ICANN** by the ….") & RySG team ("any future work **by ICANN** ~~by the relevant controllers and processors~~ in relation…". Also, please provide further input on what these changes would mean or imply as work on a Code of Conduct was not part of phase 1 or phase 2 recommendations. Also consider additional language suggested by IPC (late submission): "For the avoidance of doubt, RDS data requestors are relevant controllers and processors and must be included in any such future work."

Three 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.[28]

b. If the Registrant (data subject) has self-identified as a legal person and has provided a confirmation that the registration data does not include any personal data, the

[26] See also https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf
[27] Not to be confused with the Code of Conduct that is referenced in the RAA and/or Registry Agreements.
[28] 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[29] (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 self-identified as 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.[30]

2. Data subject self-identification at time when registration is updated[31]

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 self-identify as a legal or natural person type. The Registrar should also request a Registrant self-identified as a legal person to confirm that no personal data has been provided.[32]

c. Registrant (data subject) self-identifies as legal or natural person type and confirms that no personal data has been provided 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.[33]

d. If the data subject self-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[34] (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

[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] 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.

[31] 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).

[32] 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.

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

[34] 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".

a. The Registrar collects Registration Data and provisionally redacts the data.
b. The Registrar uses collected data to infer legal or natural person type.[35]
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[36] (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 that the Registrant is a 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.

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, the EPDP Team encourages review of the Bird & Bird memo which can also be found in Annex E, especially sections 11.11.1-2, 13, 14.3 and 18.

○ 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".[37]

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.

[35] 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).

[36] 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".

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

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. 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.

Deleted: ¶

"Registrant-based email contact", means "an email for all domains registered by a unique registrant [sponsored by a given Registrar] OR [across Registrars], [38] which is intended to be pseudonymous[39] data when processed by non-contracted parties.[40]"[41]

"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." [42]

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

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

> 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-P1 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-P1 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.

Deleted: *

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.[43]

*Note, during the Phase 2A deliberations, some EPDP Team members raised the issue of web forms and potential issues with the use of such web forms. It was noted that even though the option of a web form is part of EPDP Phase 1 recommendation #13, this requirement is the same as in the Temporary Specification which has been in force since 25 May 2018. Consultations with ICANN org indicated that web forms have not been a significant source of complaints nor has this been raised as an issue in the context of the Implementation Review Team which is tasked to implement the phase 1 recommendation.[44] Some members are of the view that even if there are issues, these are not within scope for the EPDP Team to address, considering its limited remit. The EPDP Team was not able to come to an agreement on how to proceed on this topic.

Deleted: Nevertheless, if further evidence concerning issues with web forms is received during the public comment period as well as specific proposals for why and how the issues identified should be addressed, the EPDP Team will, at a minimum, pass on this information to the GNSO Council and ICANN org (e.g., to be relayed to the Phase I IRT) to see if/how the issues identified can be further considered. This could result in the GNSO Council directing further policy work on this topic, or the Phase I IRT or ICANN org looking into this subject.

[43] 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.

[44] See https://community.icann.org/x/I4GBCQ

EPDP-P1 Recommendation #14

In the case of a domain name registration where an "affiliated" privacy/proxy service used (e.g. where data associated with a natural person is masked), Registrar (and Registry where applicable) MUST include in the public RDDS and return in response to any query full non-personal RDDS data of the privacy/proxy service, which MAY also include the existing privacy/proxy pseudonymized email.

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.[45] Certain stakeholders see risks and other concerns[46] 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

[45] 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.

[46] 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.

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.[47]

○ EPDP Team response to Question ii.

Recommendation #4

Deleted: 3

The EPDP Team recommends that Contracted Parties who choose to publish a registrant-based or registration-based email address in the publicly accessible RDDS should evaluate the legal guidance obtained by the EPDP Team on this topic (see Annex E), as well as any other relevant guidance provided by applicable data protection authorities.

In assessing the risks, benefits, and safeguards associated with publishing a registrant-based or registration-based email address in the publicly accessible RDDS, Contracted Parties should at a minimum consider:

- Both registrant-based and registration-based email addresses of natural persons are likely personal data (i.e., neither approach creates anonymous data as defined under GDPR). This data is likely personal data both from the perspective of the data controller and for third-parties.
- However, even if considered personal data, masking email addresses does provide benefits compared to publishing actual registrant email addresses, including: (i) demonstrating a privacy-enhancing technique/data protection by design measure (Article 25 GDPR); and (ii) some risk reduction relevant when conducting a legitimate interest balancing analysis for disclosure of the masked email address to third parties.
- On balance, publication of a registration-based email address likely carries lower risk than publication of registrant-based email addresses due to the amount of information a party can potentially link to a data subject based on a registrant-based email contact.
- For both registrant-based and registration-based email address publication, Contracted Parties should adopt effective measures to mitigate the availability of contact details to spammers

Deleted: data

[47] 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.