

Final Report of the Temporary Specification for gTLD Registration Data Phase 2A Expedited Policy Development Process

3 September 2021

Status of This Document

This is the Final Recommendations Report of the GNSO Expedited Policy Development Process (EPDP) Team on the Temporary Specification for gTLD Registration Data Phase 2A for submission to the GNSO Council.

Preamble

The objective of this Final Report is to document the EPDP Team's: (i) deliberations on charter questions, (ii) input received on the EPDP's Phase 2A Initial Report and the EPDP Team's subsequent analysis, (iii) policy recommendations and associated consensus levels, and (iv) implementation guidance, for GNSO Council consideration.

Table of Contents

1 EXECUTIVE SUMMARY	3
1.1 BACKGROUND	3
1.2 INITIAL REPORT	4
1.3 RESPONSES AND RECOMMENDATIONS	4
1.4 CONCLUSIONS AND NEXT STEPS	9
1.5 OTHER RELEVANT SECTIONS OF THIS REPORT	10
2 EPDP TEAM APPROACH	11
2.1 WORKING METHODOLOGY	11
2.2 BACKGROUND BRIEFING AND APPROACH	11
2.3 LEGAL COMMITTEE	11
2.4 COUNCIL QUESTIONS	12
3 EPDP TEAM RESPONSES TO COUNCIL QUESTIONS & RECOMMENDATIONS	13
• 3.1 LEGAL VS NATURAL	13
• EPDP TEAM RESPONSE TO QUESTION I.	14
• EPDP TEAM RESPONSE TO QUESTION II.	16
• 3.2 FEASIBILITY OF UNIQUE CONTACTS	23
• EPDP TEAM RESPONSE TO QUESTION I.	27
• EPDP TEAM RESPONSE TO QUESTION II.	27
4 NEXT STEPS	29
GLOSSARY	30
ANNEX A – BACKGROUND INFO	36
ANNEX B – GENERAL BACKGROUND	37
ANNEX C – EPDP TEAM MEMBERSHIP AND ATTENDANCE	39
ANNEX D – MINORITY STATEMENTS	43
ANNEX E - COMMUNITY INPUT	81
ANNEX F – BIRD & BIRD LEGAL MEMOS	82

1 Executive Summary

1.1 Background

On 17 May 2018, the ICANN Board approved the Temporary Specification for generic top-level domain (gTLD) Registration Data to allow contracted parties to comply with existing ICANN contractual requirements while also complying with the European Union's General Data Protection Regulation (GDPR). This Board action triggered the GNSO Council initiation of the PDP on 19 July 2018. The PDP was conducted in two phases: Phase 1 was chartered to confirm, or not, the Temporary Specification by 25 May 2019; Phase 2 was chartered to discuss, among other elements, a standardized access model to nonpublic registration data (SSAD).

The GNSO Council adopted the Final Report for Phase 2 during its meeting on 24 September 2020; however, in response to a request from some EPDP Team members, the GNSO Council [asked](#) the EPDP Team to continue work on two topics: 1) the differentiation of legal vs. natural persons' registration data and 2) the feasibility of unique contacts to have a uniform anonymized email address. These two topics constitute the focus of Phase 2A.

More specifically, the EPDP Team was provided with the following instructions:

- a) Legal vs. natural persons - the EPDP Team is expected to review [the study](#) undertaken by ICANN org (as requested by the EPDP Team and approved by the GNSO Council during Phase 1) together with the [legal guidance](#) provided by Bird & Bird as well as the substantive input provided on this topic during the [public comment forum on the addendum](#) and answer:
 - 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.
- b) In relation to feasibility of unique contacts to have a uniform anonymized email address, the EPDP Team is expected to review the [legal guidance](#) and consider specific proposals that provide sufficient safeguards to address issues flagged in the legal memo. 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. This consideration is expected to address:
 - 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.

1.2 Initial Report

On 3 June 2021, the EPDP Team published its [Initial Report for public comment](#). The Initial Report outlined the Team's thinking up until that point and was intended to serve as a tool to solicit community input, especially on areas where significant divergence remained. Although preliminary recommendations were included in the Initial Report, the EPDP Team requested these recommendations be considered in combination with a set of questions raised to help inform the finalization of its report.

Following the publication of the Initial Report, the EPDP Team: (i) carefully reviewed public comments received in response to the publication of the Initial Report, (ii) continued to review the work-in-progress with the community groups the Team members represent, and (iii) continued its deliberations for the production of a Final Report that will be reviewed by the GNSO Council and, if approved, forwarded to the ICANN Board of Directors for approval as an ICANN Consensus Policy. Consensus calls on the recommendations contained in this Final Report, as required by the GNSO Working Group Guidelines, were carried out by the EPDP Team Chair. In short:

1.3 Responses and Recommendations

Chair's Statement

While this Final Report and its recommendations have the consensus support of the EPDP 2A Team, it's important to note that some groups felt that the work did not go as far as needed, or did not include sufficient detail, while other groups felt that certain recommendations were not appropriate or necessary. Additionally, during the final stage of our work, some groups would have preferred an opportunity to assign more granular consensus-level designations to component parts of the recommendations. In this context, all readers of the EPDP 2A Final Report should also read the minority statements submitted by each group, which have been appended and are part of the Final Report and historical record of our work.

Beyond the consensus reached on the Final Report recommendations, there are several areas where the EPDP 2A groups did not fully agree, including whether differentiation between legal and natural person registration data should be mandatory or optional, and whether the benefit of publication of legal person registration data was appropriately balanced against the risk of inadvertent disclosure of personal data. These differences of opinion and perspective are largely unchanged by the recommendations in the Final Report.

This Final Report constitutes a compromise that is the maximum that could be achieved by the group at this time under our currently allocated time and scope, and it should not be read as delivering results that were fully satisfactory to everyone. This underscores the importance of the minority statements in understanding the full context of the Final Report recommendations.

For further details about these designations, please see section 3.6 of the [GNSO Working Group Guidelines](#).

See section 3 for full text of recommendations and response.

Response to Council instruction (a)(i).

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.

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

Recommendation #1

The EPDP Team recommends that a field or fields **MUST** be created to facilitate differentiation between legal and natural person registration data and/or if that registration data contains personal or non-personal data. ICANN org **MUST** coordinate with the technical community, for example the RDAP WG, to develop any necessary standards associated with using this field or fields within EPP and the RDDS.

This field or fields **MAY** 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, Contracted Parties **MAY** include the field(s) in an RDDS response.

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:

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

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

Response to Council instruction (a)(ii).**Recommendation #2**

The EPDP Team recommends that Contracted Parties who choose to differentiate based on person type SHOULD follow the guidance¹ 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).

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.

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,² 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).

¹ 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>.

² 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 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)³ 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.⁴ 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, that the above developed guidance concerning legal/natural differentiation should be considered by any possible future work within ICANN by the relevant controllers and processors in relation to the development of a GDPR Code of Conduct. For the avoidance of doubt, this Code of Conduct is separate and distinct from the Code of Conduct referenced in the RAA and/or Registry Agreements. Consistent with GDPR recital 99, “When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations”.

Response to Council instruction (b)(i).

The EPDP Team recognizes that it may be technically feasible to have a registrant-based email contact or a registration-based email contact.⁵ Certain stakeholders see risks and other concerns⁶ that prevent the EPDP Team from making a recommendation to require

³ 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.

⁴ See also https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

⁵ 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.

⁶ 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-

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.⁷

Response to Council instruction (b)(ii).

Recommendation #4

The EPDP Team recommends that Contracted Parties who choose to publish an intended to be pseudonymized 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 F), as well as any other relevant guidance provided by applicable data protection authorities.

In assessing the risks, benefits, and safeguards associated with publishing an intended to be pseudonymized 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.

1.4 Conclusions and Next Steps

based or registration-based email addresses.

⁷ 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.

This Final Report will be submitted to the GNSO Council for its consideration and approval.

1.5 Other Relevant Sections of this Report

For a complete review of the issues and relevant interactions of this EPDP Team, the following sections are included within this Final Report:

- Background of the issues under consideration;
- Documentation of who participated in the EPDP Team’s deliberations, including attendance records, and links to Statements of Interest as applicable;
- An annex that includes the EPDP Team’s mandate as defined in the instructions adopted by the GNSO Council; and
- Documentation on the solicitation of community input through formal SO/AC and SG/C channels, including responses.

2 EPDP Team Approach

This Section provides an overview of the working methodology and approach of the EPDP Team. The points outlined below are meant to provide the reader with relevant background information on the EPDP Team’s deliberations and processes and should not be read as representing the entirety of the efforts and deliberations of the EPDP Team.

2.1 Working Methodology

The EPDP Team began its deliberations for Phase 2A on 17 December 2020. The Team has conducted its work through conference calls scheduled one or more times per week, in addition to email exchanges on its mailing list. All of the EPDP Team’s meetings are documented on its wiki [workspace](#), including its [mailing list](#), draft documents, background materials, and input received from ICANN’s Supporting Organizations and Advisory Committees, including the GNSO’s Stakeholder Groups and Constituencies.

The EPDP Team also prepared a work plan as part of the [EPDP Phase 2A project package](#), which was reviewed and updated on a regular basis, and shared with the GNSO Council.

2.2 Background briefing and approach

In order to ensure a common understanding of the topics to be addressed as part of its Phase 2A deliberations, the Staff Support Team developed [background briefings](#) for each of the topics. The background briefings included: 1) Council instructions to the EPDP Team, 2) relevant EPDP Phase 1 & Phase 2 recommendations, 3) relevant studies or legal guidance previously obtained, 4) procedural requirements, 5) timing instructions, and 6) the proposed approach. These background briefings were circulated to the EPDP Team in advance of the first meeting and, together with the assigned reading, formed the basis of the EPDP Team’s first assignment. Specifically, the EPDP Team was asked to thoroughly review the assigned studies and previous legal guidance and identify any clarifying questions.

2.3 Legal Committee

Similar to Phase 1 and Phase 2, the EPDP Team relied on its Legal Committee to review and refine the questions identified by the EPDP Team. The Legal Committee is comprised of one member from each SG/C/AC represented on the EPDP Team.

The Phase 2A Legal Committee worked together to review questions proposed by the members EPDP Team to ensure:

1. the questions were truly legal in nature, as opposed to a policy or policy implementation questions;
2. the questions were phrased in a neutral manner, avoiding both presumed outcomes as well as constituency positioning;
3. the questions were both apposite and timely to the EPDP Team’s work; and
4. the limited budget for external legal counsel was used responsibly.

The Legal Committee distributed all agreed-upon questions to the EPDP Team before sending questions to Bird & Bird.

To date, the EPDP Team agreed to send four Phase 2A questions to Bird & Bird. The full text of the questions and the legal advice received in response to the questions can be found in Annex F.

2.4 Council Questions

In addressing the questions assigned by the GNSO Council, the EPDP Team considered both (1) the input provided by each group as part of the deliberations; (2) relevant input from Phase 1 and 2; (3) the input provided on these topics by each group in response to the request for early input during the previous phases as well as relevant comments provided during the public comment forum on the EPDP Phase 2 addendum;⁸ (4) the required reading identified for each topic in the background briefings, including the ICANN org study on “[Differentiation between Legal and Natural Persons in Domain Name Registration Data Directory Services \(RDDS\)](#)”, and (5) [input](#) provided by Bird & Bird.

⁸ See <https://community.icann.org/x/Ag9pBQ>, <https://community.icann.org/x/Ag9pBQ>, <https://www.icann.org/public-comments/epdp-phase-2-addendum-2020-03-26-en> as well as the [Addendum Public Comment Review Tool](#).

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:

Chair's Statement

While this Final Report and its recommendations have the consensus support of the EPDP 2A Team, it's important to note that some groups felt that the work did not go as far as needed, or did not include sufficient detail, while other groups felt that certain recommendations were not appropriate or necessary. Additionally, during the final stage of our work, some groups would have preferred an opportunity to assign more granular consensus-level designations to component parts of the recommendations. In this context, all readers of the EPDP 2A Final Report should also read the minority statements submitted by each group, which have been appended and are part of the Final Report and historical record of our work.

Beyond the consensus reached on the Final Report recommendations, there are several areas where the EPDP 2A groups did not fully agree, including whether differentiation between legal and natural person registration data should be mandatory or optional, and whether the benefit of publication of legal person registration data was appropriately balanced against the risk of inadvertent disclosure of personal data. These differences of opinion and perspective are largely unchanged by the recommendations in the Final Report.

This Final Report constitutes a compromise that is the maximum that could be achieved by the group at this time under our currently allocated time and scope, and it should not be read as delivering results that were fully satisfactory to everyone. This underscores the importance of the minority statements in understanding the full context of the Final Report recommendations.

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,⁹ (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 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.

- **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.¹⁰ 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”.¹¹ 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.

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

⁹ 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.

¹⁰ “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.”

¹¹ 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>

(“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.

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

Recommendation #1

The EPDP Team recommends that a field or fields **MUST** be created to facilitate differentiation between legal and natural person registration data and/or if that registration data contains personal or non-personal data. ICANN org **MUST** coordinate with the technical community, for example the RDAP WG, to develop any necessary standards associated with using this field or fields within EPP and the RDDS.

This field or fields **MAY** 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, Contracted Parties **MAY** include the field(s) in an RDDS response.

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:

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

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

- **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:¹² “Publication”, “Publish”, and “Published” means to provide Registration Data in the publicly accessible Registration Data Directory Services.
- EPDP-p1-IRT:¹³ “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:¹⁴ “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

¹² See https://docs.google.com/document/d/1SVFkoI6RmrVVz--RrVLSOj1bmz1qLb7_JTuv7At4Uo/edit.

¹³ Ibid.

¹⁴ See <https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-2-20feb19-en.pdf>.

controller and the purposes of the processing[.]¹⁵ [. . .]

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.”¹⁶

- 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.”¹⁷
- c. Data Minimization: “Limit the amount of personal data collected to what is necessary for the purpose.”¹⁸
- 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.”¹⁹

Relevant EPDP Phase 1 Recommendations²⁰

- E. Per EPDP Phase 1²¹ 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 2²² Final Report Recommendation #9.4.4, which addresses automation of SSAD processing: “the EPDP Team recommends that the following types of

¹⁵ 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-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>).

¹⁶ See EDPB Guidelines, 05/2020, Guidelines 05/2020 on consent under regulation 2016/679, Section 3.3.

¹⁷ 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/>).

¹⁸ 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).

¹⁹ 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).

²⁰ 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.

²¹ 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>.

²² Note that the EPDP Phase 2 recommendations are with the ICANN Board for its consideration / approval.

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.²³

- 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

Recommendation #2

The EPDP Team recommends that Contracted Parties who choose to differentiate based on person type SHOULD follow the guidance²⁴ 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).

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

²³ 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.

²⁴ 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>.

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.

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,²⁵ 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).
4. Registrars should ensure that they clearly communicate the nature and consequences of a registrant identifying as a legal person. These communications should include:
 - c. An explanation of what a legal person is in plain language that is easy to understand.
 - d. Guidance to the registrant (data subject)²⁶ 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.²⁷ 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.

²⁵ 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.

²⁶ 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.

²⁷ See also https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

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, that the above developed guidance concerning legal/natural differentiation should be considered by any possible future work within ICANN by the relevant controllers and processors in relation to the development of a GDPR Code of Conduct. For the avoidance of doubt, this Code of Conduct is separate and distinct from the Code of Conduct referenced in the RAA and/or Registry Agreements. Consistent with GDPR recital 99, “When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations”.

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 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

²⁸Note 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.

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

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 a 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 updated³¹

- 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

- 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

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”.

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).

- present, the Registrar should (i) contact the provided contact details to verify the Registrant claim³⁶ (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 F, especially sections 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.

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.

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://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-2-priority-2-items-10sep20-en.pdf>

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],³⁸ which is intended to be pseudonymous³⁹ data when processed by non-contracted parties."⁴⁰⁴¹

"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

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 within 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.

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 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.

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

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.

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.

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.”

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 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 concerns⁴⁶ 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.⁴⁷

- **EPDP Team response to Question ii.**

Recommendation #4

The EPDP Team recommends that Contracted Parties who choose to publish an intended to be pseudonymized 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 F), as well as any other relevant guidance provided by applicable data protection authorities.

In assessing the risks, benefits, and safeguards associated with publishing an intended to be pseudonymized 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.

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.

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.

- 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.

4 Next Steps

4.1 Next Steps

This Final Report will be submitted to the GNSO Council for its consideration and approval. If adopted by the GNSO Council, the Final Report would then be forwarded to the ICANN Board of Directors for its consideration and, potentially, approval.

Glossary

1. Advisory Committee

An Advisory Committee is a formal advisory body made up of representatives from the Internet community to advise ICANN on a particular issue or policy area. Several are mandated by the ICANN Bylaws and others may be created as needed. Advisory committees have no legal authority to act for ICANN, but report their findings and make recommendations to the ICANN Board.

2. ALAC - At-Large Advisory Committee

ICANN's At-Large Advisory Committee (ALAC) is responsible for considering and providing advice on the activities of the ICANN, as they relate to the interests of individual Internet users (the "At-Large" community). ICANN, as a private sector, non-profit corporation with technical management responsibilities for the Internet's domain name and address system, will rely on the ALAC and its supporting infrastructure to involve and represent in ICANN a broad set of individual user interests.

3. Business Constituency

The Business Constituency represents commercial users of the Internet. The Business Constituency is one of the Constituencies within the Commercial Stakeholder Group (CSG) referred to in Article 11.5 of the ICANN bylaws. The BC is one of the stakeholder groups and constituencies of the Generic Names Supporting Organization (GNSO) charged with the responsibility of advising the ICANN Board on policy issues relating to the management of the domain name system.

4. ccNSO - The Country-Code Names Supporting Organization

The ccNSO the Supporting Organization responsible for developing and recommending to ICANN's Board global policies relating to country code top-level domains. It provides a forum for country code top-level domain managers to meet and discuss issues of concern from a global perspective. The ccNSO selects one person to serve on the board.

5. ccTLD - Country Code Top Level Domain

ccTLDs are two-letter domains, such as .UK (United Kingdom), .DE (Germany) and .JP (Japan) (for example), are called country code top level domains (ccTLDs) and correspond to a country, territory, or other geographic location. The rules and policies for registering domain names in the ccTLDs vary significantly and ccTLD registries limit use of the ccTLD to citizens of the corresponding country.

For more information regarding ccTLDs, including a complete database of designated ccTLDs and managers, please refer to <http://www.iana.org/cctld/cctld.htm>.

6. Domain Name Registration Data

Domain name registration data, also referred to as registration data, refers to the information that registrants provide when registering a domain name and that registrars or registries collect. Some of this information is made available to the public. For interactions between ICANN Accredited Generic Top-Level Domain (gTLD) registrars and registrants, the data elements are specified in the current RAA. For country code Top Level Domains (ccTLDs), the operators of these TLDs set their own or follow their government's policy regarding the request and display of registration information.

7. Domain Name

As part of the Domain Name System, domain names identify Internet Protocol resources, such as an Internet website.

8. DNS - Domain Name System

DNS refers to the Internet domain-name system. The Domain Name System (DNS) helps users to find their way around the Internet. Every computer on the Internet has a unique address - just like a telephone number - which is a rather complicated string of numbers. It is called its "IP address" (IP stands for "Internet Protocol"). IP Addresses are hard to remember. The DNS makes using the Internet easier by allowing a familiar string of letters (the "domain name") to be used instead of the arcane IP address. So instead of typing 207.151.159.3, you can type www.internic.net. It is a "mnemonic" device that makes addresses easier to remember.

9. EPDP – Expedited Policy Development Process

A set of formal steps, as defined in the ICANN bylaws, to guide the initiation, internal and external review, timing and approval of policies needed to coordinate the global Internet's system of unique identifiers. An EPDP may be initiated by the GNSO Council only in the following specific circumstances: (1) to address a narrowly defined policy issue that was identified and scoped after either the adoption of a GNSO policy recommendation by the ICANN Board or the implementation of such an adopted recommendation; or (2) to provide new or additional policy recommendations on a specific policy issue that had been substantially scoped previously, such that extensive, pertinent background information already exists, e.g. (a) in an Issue Report for a possible PDP that was not initiated; (b) as part of a previous PDP that was not completed; or (c) through other projects such as a GNSO Guidance Process.

10. GAC - Governmental Advisory Committee

The GAC is an advisory committee comprising appointed representatives of national governments, multi-national governmental organizations and treaty organizations, and distinct economies. Its function is to advise the ICANN Board on matters of concern to governments. The GAC will operate as a forum for the discussion of government interests and concerns, including consumer interests. As an advisory committee, the GAC has no legal authority to act for ICANN, but will report its findings and recommendations to the ICANN Board.

11. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.

12. GNSO - Generic Names Supporting Organization

The supporting organization responsible for developing and recommending to the ICANN Board substantive policies relating to generic top-level domains. Its members include representatives from gTLD registries, gTLD registrars, intellectual property interests, Internet service providers, businesses and non-commercial interests.

13. Generic Top Level Domain (gTLD)

"gTLD" or "gTLDs" refers to the top-level domain(s) of the DNS delegated by ICANN pursuant to a registry agreement that is in full force and effect, other than any country code TLD (ccTLD) or internationalized domain name (IDN) country code TLD.

14. gTLD Registries Stakeholder Group (RySG)

The gTLD Registries Stakeholder Group (RySG) is a recognized entity within the Generic Names Supporting Organization (GNSO) formed according to Article X, Section 5 (September 2009) of the Internet Corporation for Assigned Names and Numbers (ICANN) Bylaws.

The primary role of the RySG is to represent the interests of gTLD registry operators (or sponsors in the case of sponsored gTLDs) ("Registries") (i) that are currently under contract with ICANN to provide gTLD registry services in support of one or more gTLDs; (ii) who agree to be bound by consensus policies in that contract; and (iii) who voluntarily choose to be members of the RySG. The RySG may include Interest Groups as defined by Article IV. The RySG represents the views of the RySG to the GNSO Council and the ICANN Board of Directors with particular emphasis on ICANN consensus policies that relate to interoperability, technical reliability and stable operation of the Internet or domain name system.

15. ICANN - The Internet Corporation for Assigned Names and Numbers

The Internet Corporation for Assigned Names and Numbers (ICANN) is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. Originally, the Internet Assigned Numbers Authority (IANA) and other entities performed these services under U.S. Government contract. ICANN now performs the IANA function. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes.

16. Intellectual Property Constituency (IPC)

The Intellectual Property Constituency (IPC) represents the views and interests of the intellectual property community worldwide at ICANN, with a particular emphasis on trademark, copyright, and related intellectual property rights and their effect and interaction with Domain Name Systems (DNS). The IPC is one of the constituency groups of the Generic Names Supporting Organization (GNSO) charged with the responsibility of advising the ICANN Board on policy issues relating to the management of the domain name system.

17. Internet Service Provider and Connectivity Provider Constituency (ISPCP)

The ISPs and Connectivity Providers Constituency is a constituency within the GNSO. The Constituency's goal is to fulfill roles and responsibilities that are created by relevant ICANN and GNSO bylaws, rules or policies as ICANN proceeds to conclude its organization activities. The ISPCP ensures that the views of Internet Service Providers and Connectivity Providers contribute toward fulfilling the aims and goals of ICANN.

18. Name Server

A Name Server is a DNS component that stores information about one zone (or more) of the DNS name space.

19. Non Commercial Stakeholder Group (NCSG)

The Non Commercial Stakeholder Group (NCSG) is a Stakeholder Group within the GNSO. The purpose of the Non Commercial Stakeholder Group (NCSG) is to represent, through its elected representatives and its Constituencies, the interests and concerns of noncommercial registrants and noncommercial Internet users of generic Top-level Domains (gTLDs). It provides a voice and representation in ICANN processes to: non-profit organizations that serve noncommercial interests; nonprofit services such as education, philanthropies, consumer protection, community organizing, promotion of the arts, public interest policy advocacy, children's welfare, religion, scientific research, and human rights; public interest software concerns; families or individuals who register domain names for noncommercial personal use; and Internet users who are primarily concerned with the noncommercial, public interest aspects of domain name policy.

20. Post Delegation Dispute Resolution Procedures (PDDRPs)

Post-Delegation Dispute Resolution Procedures have been developed to provide those harmed by a new gTLD Registry Operator's conduct an alternative avenue to complain about that conduct. All such dispute resolution procedures are handled by providers external to ICANN and require that complainants take specific steps to address their issues before filing a formal complaint. An Expert Panel will determine whether a Registry Operator is at fault and recommend remedies to ICANN.

21. Registered Name

"Registered Name" refers to a domain name within the domain of a gTLD, whether consisting of two (2) or more (e.g., john.smith.name) levels, about which a gTLD Registry Operator (or an Affiliate or subcontractor thereof engaged in providing Registry

Services) maintains data in a Registry Database, arranges for such maintenance, or derives revenue from such maintenance. A name in a Registry Database may be a Registered Name even though it does not appear in a zone file (e.g., a registered but inactive name).

22. Registrar

The word "registrar," when appearing without an initial capital letter, refers to a person or entity that contracts with Registered Name Holders and with a Registry Operator and collects registration data about the Registered Name Holders and submits registration information for entry in the Registry Database.

23. Registrars Stakeholder Group (RrSG)

The Registrars Stakeholder Group is one of several Stakeholder Groups within the ICANN community and is the representative body of registrars. It is a diverse and active group that works to ensure the interests of registrars and their customers are effectively advanced. We invite you to learn more about accredited domain name registrars and the important roles they fill in the domain name system.

24. Registry Operator

A "Registry Operator" is the person or entity then responsible, in accordance with an agreement between ICANN (or its assignee) and that person or entity (those persons or entities) or, if that agreement is terminated or expires, in accordance with an agreement between the US Government and that person or entity (those persons or entities), for providing Registry Services for a specific gTLD.

25. Registration Data Directory Service (RDDS)

Domain Name Registration Data Directory Service or RDDS refers to the service(s) offered by registries and registrars to provide access to Domain Name Registration Data.

26. Registration Restrictions Dispute Resolution Procedure (RRDRP)

The Registration Restrictions Dispute Resolution Procedure (RRDRP) is intended to address circumstances in which a community-based New gTLD Registry Operator deviates from the registration restrictions outlined in its Registry Agreement.

27. SO - Supporting Organizations

The SOs are the three specialized advisory bodies that advise the ICANN Board of Directors on issues relating to domain names (GNSO and CCNSO) and, IP addresses (ASO).

28. SSAC - Security and Stability Advisory Committee

An advisory committee to the ICANN Board comprised of technical experts from industry and academia as well as operators of Internet root servers, registrars and TLD registries.

29. TLD - Top-level Domain

TLDs are the names at the top of the DNS naming hierarchy. They appear in domain names as the string of letters following the last (rightmost) ".", such as "net" in <http://www.example.net>. The administrator for a TLD controls what second-level names are recognized in that TLD. The administrators of the "root domain" or "root zone" control what TLDs are recognized by the DNS. Commonly used TLDs include .COM, .NET, .EDU, .JP, .DE, etc.

30. Uniform Dispute Resolution Policy (UDRP)

The Uniform Dispute Resolution Policy (UDRP) is a rights protection mechanism that specifies the procedures and rules that are applied by registrars in connection with disputes that arise over the registration and use of gTLD domain names. The UDRP provides a mandatory administrative procedure primarily to resolve claims of abusive, bad faith domain name registration. It applies only to disputes between registrants and third parties, not disputes between a registrar and its customer.

31. Uniform Rapid Suspension (URS)

The Uniform Rapid Suspension System is a rights protection mechanism that complements the existing Uniform Domain-Name Dispute Resolution Policy (UDRP) by offering a lower-cost, faster path to relief for rights holders experiencing the most clear-cut cases of infringement.

32. WHOIS

WHOIS protocol is an Internet protocol that is used to query databases to obtain information about the registration of a domain name (or IP address). The WHOIS protocol was originally specified in RFC 954, published in 1985. The current specification is documented in RFC 3912. ICANN's gTLD agreements require registries and registrars to offer an interactive web page and a port 43 WHOIS service providing free public access to data on registered names. Such data is commonly referred to as "WHOIS data," and includes elements such as the domain registration creation and expiration dates, nameservers, and contact information for the registrant and designated administrative and technical contacts.

WHOIS services are typically used to identify domain holders for business purposes and to identify parties who are able to correct technical problems associated with the registered domain.

Annex A – Background Info

Following the request from some EPDP Team members, the GNSO Council asked the EPDP Team to continue work on two topics, after its completion of phase 1 and phase 2 of its work, namely: 1) the differentiation of legal vs. natural persons' registration data and 2) the feasibility of unique contacts to have a uniform anonymized email address.

Legal vs. Natural persons data - Council Instructions to EPDP Team

Legal vs. natural persons - the EPDP Team is expected to review [the study](#) undertaken by ICANN org (as requested by the EPDP Team and approved by the GNSO Council during Phase 1) together with the [legal guidance](#) provided by Bird & Bird as well as the substantive input provided on this topic during [the public comment forum on the addendum](#) and answer:

- 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.

Feasibility of unique contacts to have a uniform anonymized email address - Council Instructions to EPDP Team

The EPDP Team is expected to review the [legal guidance](#) and consider specific proposals that provide sufficient safeguards to address issues flagged in the legal memo. 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. This consideration is expected to address:

- 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.

Annex B – General Background

Process & Issue Background

On 19 July 2018, the GNSO Council [initiated](#) an Expedited Policy Development Process (EPDP) and [chartered](#) the EPDP on the Temporary Specification for gTLD Registration Data Team. Unlike other GNSO PDP efforts, which are open for anyone to join, the GNSO Council chose to limit the membership composition of this EPDP, primarily in recognition of the need to complete the work in a relatively short timeframe and to resource the effort responsibly. GNSO Stakeholder Groups, the Governmental Advisory Committee (GAC), the Country Code Supporting Organization (ccNSO), the At-Large Advisory Committee (ALAC), the Root Server System Advisory Committee (RSSAC) and the Security and Stability Advisory Committee (SSAC) were each been invited to appoint up to a set number of members and alternates, as outlined in the [charter](#). In addition, the ICANN Board and ICANN Org have been invited to assign a limited number of liaisons to this effort. A call for volunteers to the aforementioned groups was issued in July, and the EPDP Team held its first phase 1 meeting on [1 August 2018](#).

Issue Background

On 17 May 2018, the ICANN Board approved the Temporary Specification for gTLD Registration Data. The Board took this action to establish temporary requirements for how ICANN and its contracted parties would continue to comply with existing ICANN contractual requirements and community-developed policies relate to WHOIS, while also complying with the European Union (EU)'s General Data Protection Regulation (GDPR). The Temporary Specification has been adopted under the procedure for Temporary Policies outlined in the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA). Following adoption of the Temporary Specification, the Board “shall immediately implement the Consensus Policy development process set forth in ICANN’s Bylaws”.⁴⁸ This Consensus Policy development process on the Temporary Specification would need to be carried out within a one-year period. Additionally, the scope includes discussion of a standardized access system to nonpublic registration data.

At its meeting on 19 July 2018, the Generic Names Supporting Organization (GNSO) Council initiated an EPDP on the Temporary Specification for gTLD Registration Data and adopted the EPDP Team charter. Unlike other GNSO PDP efforts, which are open for anyone to join, the GNSO Council chose to limit the membership composition of this EPDP, primarily in recognition of the need to complete the work in a relatively short timeframe and to resource the effort responsibly. GNSO Stakeholder Groups, the Governmental Advisory Committee (GAC), the Country Code Supporting Organization

⁴⁸ See section 3.1(a) of the Registry Agreement: <https://www.icann.org/resources/unthemed-pages/org-agmt-html-2013-09-12-en>

(ccNSO), the At-Large Advisory Committee (ALAC), the Root Server System Advisory Committee (RSSAC) and the Security and Stability Advisory Committee (SSAC) were each been invited to appoint up to a set number of members and alternates, as outlined in the [charter](#). In addition, the ICANN Board and ICANN Org have been invited to assign a limited number of liaisons to this effort.

The GNSO Council voted to adopt all 29 recommendations within the EPDP's Phase 1 [Final Report](#) at its meeting on 4 March 2019. On 15 May 2019, the ICANN Board [adopted](#) the EPDP Team's Phase 1 Final Report, with the exception of parts of two recommendations: 1) Purpose 2 in Recommendation 1 and 2) the option to delete data in the Organization field in Recommendation 12. As per the ICANN Bylaws, a consultation has taken place between the GNSO Council and the ICANN Board to discuss the parts of the EPDP Phase 1 recommendations that were not adopted by the ICANN Board. At the same time, an Implementation Review Team (IRT), consisting of the ICANN organization (ICANN org) and members of the ICANN community, is working on the implementation of the approved recommendations of the EPDP Team's Phase 1 Final Report. For further details on the status of implementation, please see [here](#).

The GNSO Council approved the [Phase 2 Final Report](#) during its meeting on 24 September 2020 by a supermajority. The Final Report sets out the EPDP Team's recommendations for a System for Standardized Access/Disclosure (SSAD) to nonpublic gTLD registration data, as well as recommendations and conclusions for the so-called "Priority 2" topics, which include, et al., data retention and city field redaction.

As part of its approval, the GNSO Council agreed to request a consultation with the ICANN Board to discuss the financial sustainability of the SSAD and some of the concerns expressed within the different minority statements, including whether a further cost-benefit analysis should be conducted before the ICANN Board considers all SSAD-related recommendations for adoption. During ICANN70, the Board directed ICANN org to initiate an Operational Design Phase (ODP) for the SSAD-related recommendations, and the ODP is currently ongoing. For more information on the SSAD ODP, please visit the following [page](#).

As the requested consultation related only to SSAD-related recommendations, the Board opted to consider the Priority 2 recommendations separately, and conducted a [public comment](#) period on those recommendations from December 2020 to January 2021. The Board conducted a separate [public comment](#) period on the SSAD-related recommendations from February to March 2021.

Following the request from some EPDP Team members, the GNSO Council asked the EPDP Team to continue work on two topics as part of a Phase 2A, namely: 1) the differentiation of legal vs. natural persons' registration data and 2) the feasibility of unique contacts to have a uniform anonymized email address.

Annex C – EPDP Team Membership and Attendance

EPDP Team Membership and Attendance

Meeting Activity Summary:

Plenary Meetings:

- 42 Plenary Calls (5 cancelled) for 53.5 call hours for a total of 1924.5 person hours
- 85.3% total participation rate

Legal Committee Meetings:

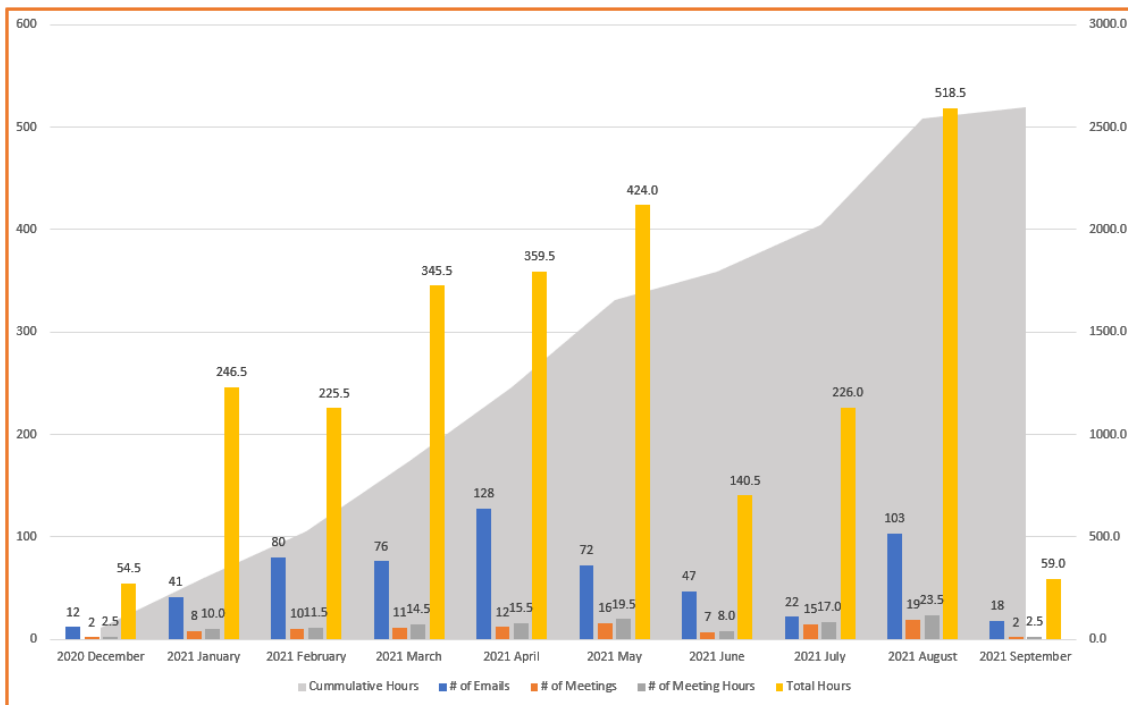
- 11 Subgroup Calls for 17.5 call hours for a total of 232.5 person hours
- 89.2% total participation rate

Small Team Meetings:

- 16 Subgroup Calls for 17.5 call hours for a total of 180.0 person hours
- 99.0% total participation rate

Leadership Meetings:

- 51 Leadership Calls for 39.0 call hours for a total of 268.5 person hours



The EPDP Team email archives can be found at <https://mm.icann.org/pipermail/gnso-epdp-team/>.

The Members of the EPDP Team are:

Represented Group / Member	SOI	Start Date	Depart Date	Attended %	Role
At-Large Advisory Committee (ALAC)				98.6%	
Alan Greenberg	SOI	15-Nov-2020		97.2%	
Hadia Elminiawi	SOI	15-Nov-2020		100.0%	LC
Commercial Business Users Constituency (BC)				88.9%	
Margie Milam	SOI	15-Nov-2020		86.1%	LC
Mark Svancarek	SOI	15-Nov-2020		91.7%	
GNSO Council				88.7%	
Brian Beckham	SOI	18-Feb-2021		86.2%	Vice-Chair, LC
Keith Drazek	SOI	12-Mar-2020		97.2%	Chair, LC
Philippe Fouquart	SOI	26-Jan-2021		81.3%	Liaison, LC
Governmental Advisory Committee (GAC)				74.1%	
Christopher Lewis-Evans	SOI	19-Nov-2020		88.9%	
Laureen Kapin	SOI	19-Nov-2020		83.3%	LC
Melina Stroungi	SOI	20-Nov-2020		50.0%	LC
ICANN Board				73.6%	
Becky Burr	SOI	12-Nov-2020		75.0%	Liaison, LC
Matthew Shears	SOI	12-Nov-2020		72.2%	Liaison
Intellectual Property Constituency (IPC)				84.7%	
Brian King	SOI	20-Nov-2020		97.2%	LC
Jan Janssen	SOI	20-Nov-2020		72.2%	LC
Internet Corporation for Assigned Names & Numbers (ICANN)				93.1%	
Amy Bivins	SOI	12-Jul-2020		88.9%	Liaison, LC
Brian Gutterman	SOI	12-Oct-2020		97.2%	Liaison
Internet Service Providers and Connectivity Providers Constituency (ISPCP)				93.1%	
Christian Dawson	SOI	15-Nov-2020		94.4%	
Thomas Rickert	SOI	15-Nov-2020		91.7%	LC
Non-Commercial Stakeholder Group (NCSG)				65.0%	
David Cake	SOI	12-Mar-2020		72.2%	
Manju Chen	SOI	12-Mar-2020		97.2%	
Milton Mueller	SOI	12-Mar-2020		58.3%	
Stefan Filipovic	SOI	12-Mar-2020		13.9%	LC
Stephanie Perrin	SOI	12-Mar-2020		83.3%	LC
<Vacant>					
Registrar Stakeholder Group (RrSG)				70.4%	
James Bladel	SOI	15-Nov-2020		27.8%	
Sarah Wyld	SOI	15-Nov-2020		94.4%	
Volker Greimann	SOI	15-Nov-2020		88.9%	LC
Registry Stakeholder Group (RySG)				94.4%	
Alan Woods	SOI	15-Nov-2020		91.7%	LC

Marc Anderson	SOI	15-Nov-2020		97.2%	
Matthew Crossman	SOI	15-Nov-2020		94.4%	LC
Security and Stability Advisory Committee (SSAC)				98.5%	
Ben Butler	SOI	15-Nov-2020	14-Jan-2021	50.0%	
Steve Crocker	SOI	2-Oct-2021		100.0%	
Tara Whalen	SOI	15-Nov-2020		100.0%	LC

LC = Participated on Legal Committee

The Alternates of the EPDP Team are:

Represented Group / Alternate	SOI	Start Date	Depart Date	Attended %	Role
At-Large Advisory Committee (ALAC)					
Holly Raiche	SOI	15-Nov-2020		100.0%	
<Vacant>					
Commercial Business Users Constituency (BC)					
Steve DelBianco	SOI	15-Nov-2020		93.3%	
Governmental Advisory Committee (GAC)					
Ryan Carroll	SOI	26-Jan-2021		100.0%	
Velimira Nemiguentcheva-Grau	SOI	26-Jan-2021		100.0%	
<Vacant>					
ICANN Board					
León Felipe Sánchez Ambia	SOI	12-Nov-2020		86.7%	
Intellectual Property Constituency (IPC)					
<Vacant>					
Internet Service Providers and Connectivity Providers Constituency (ISPCP)					
Suman Lal Pradhan	SOI	15-Nov-2020		100.0%	
Non-Commercial Stakeholder Group (NCSG)					
Bruna Santos	SOI	12-Mar-2020		100.0%	
<Vacant>					
<Vacant>					
Registrar Stakeholder Group (RrSG)					
Matt Serlin	SOI	15-Nov-2020		100.0%	
Owen Smigelski	SOI	15-Nov-2020		97.0%	
Theo Geurts	SOI	15-Nov-2020		100.0%	
Registry Stakeholder Group (RySG)					
Amr Elsadr	SOI	15-Nov-2020		100.0%	
Beth Bacon	SOI	15-Nov-2020		100.0%	
Sean Baseri	SOI	15-Nov-2020		100.0%	
Security and Stability Advisory Committee (SSAC)					
Greg Aaron	SOI	15-Nov-2020		100.0%	
<Vacant>					

Staff Support of the EPDP Team are:

Represented Group / Staff Assigned	SOI	Start Date	Depart Date	Attended %	Role
Andrea Glandon		15-Nov-2020			
Berry Cobb		15-Nov-2020			
Caitlin Tubergen		15-Nov-2020			LC
Julie Bisland		15-Nov-2020			
Marika Konings		15-Nov-2020			
Terri Agnew		15-Nov-2020			

Annex D – Minority Statements

[At-Large Advisory Committee](#)

[Business Constituency](#)

[Intellectual Property Constituency](#)

[Governmental Advisory Committee](#)

[Non-Commercial Stakeholder Group](#)

[Registrar Stakeholder Group](#)

[Registries Stakeholder Group](#)

[Security and Stability Advisory Committee](#)

AT-LARGE ADVISORY COMMITTEE
Final Report of the Temporary Specification for gTLD Registration Data Phase 2A
Expedited Policy Development Process

ALAC Minority Statement

The ALAC recognizes and appreciates the work of the EPDP Phase 2A team, the efforts of the chair, vice chair and the liaison to the GNSO council as well as the dedication and efforts of the ICANN org support staff. Nonetheless, the ALAC believes that the Phase 2A did not properly address its mandate. The net result is that the importance of the registration data to various community members such as consumer protection agencies, law enforcement authorities and cybersecurity investigators and the crucial role they play in protecting everyday Internet users, registrants, customers, businesses and the entire online population will not be properly addressed.

It is important to strike a balance between the protection of registrants' personal information and users' experience, safety and security. Redacting data that is not protected by data protection laws does not allow the right balance to occur.

In this Minority statement, the ALAC is concerned about the following aspects of the recommendations of the Phase 2A final report and their impact on the security and safety of everyday Internet users:

- Not mandating differentiation between legal and natural person data,
- Not mandating the usage of the common data element by all contracted parties,
- Lack of means to contact registrants
- "Process"

Not mandating differentiation between legal and natural person data

GDPR does not protect the non-personal data of legal persons. Moreover, the EU GDPR recital number 14 which says "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."

The EPDP received legal guidance that it was reasonable to allow registrants to self-designate and with proper cautions, disclaimers and correction capabilities, there was low risk to contracted parties to do so. This position was supported by the July 2018 EDPB letter to Göran Marby. This advice was ignored by the EPDP. Although the installed base of 200M registrations would take time to address (such as at renewal time), the EPDP did not even recommend that differentiation of new registrations be made. More to the point, even the discussion of taking such action (as formally

proposed by GAC EPDP Members) was summarily dismissed early in Phase 2A, instead focusing only on “guidance” which could be ignored. Taking into consideration all of the above and that the Registration Data Directory Service (RDDS) is a public good that protects global online users and the GDPR and similar privacy laws are a public good that protects the registration data of registrants, a right balance needs to occur. This right balance cannot be achieved if more data than what is required by law and legislation is redacted, and the EPDP made virtually no effort to achieve that balance.

Not mandating the usage of the common data element by all contracted parties

The proposed common data element(s) in Recommendation # 1, allows for eight possible different values including “the legal status distinction was not made” and “the presence of personal data wasn’t determined”. Those statuses allow for contracted parties who do not differentiate to make use of the newly defined field. However, the EPDP failed to recommend that the fields must be used, even by those registrars who voluntarily choose to make a legal/natural distinction or identify the presences/absence of personal data. By not requiring the use of the fields, EVEN WHEN valid and useful data is available makes no sense. Moreover, the EPDP did not designate these fields as eligible for public disclosure, even though they contain NO personal information.

According to the EPDP phase 1 and phase 2 final reports recommendations, the contracted parties (CPs) must update their current registration data directory service (RDDS)

Mandating the use of the common data element by all contracted parties would allow similar processes to be followed by all CPs across the globe, whether they differentiate or not and whether they are subject to EU regulations or not.

As a result, we are creating a common element that no one is required to use, defeating the purpose behind the creation of common ways of doing things and opening the door to fragmentation.

Lack of means to contact registrants

The ALAC regrets that the EPDP failed to reach closure on methodologies to better address anonymization or pseudonymization of contact e-mail addresses. That being the case, we are left with the Phase 1 recommendations allowing anonymization but in the absence of that, allowing web forms for contact. Since the completion of Phase 1, it has become apparent that some (major) registrars use a type of web form that effectively does not allow any useful communications with a registrant. Addressing this apparent gap in the regulations was ruled to be out of scope, despite the GNSO instructions to revisit this Phase 1 recommendation. The net effect is that for a significant part of the gTLD registration base, there is no effective way to achieve registrant communications.

“Process”

The ALAC is concerned that throughout this EPDP, the focus has been exclusively on the projected processes and stated time-schedules with severe impact on the ability to determine and recommend good policy.

Examples include:

- Timelines which do not allow sufficient deliberation of consultation with the groups supporting this EPDP
- Scope determinations that rule some things out of scope because they are not explicitly mentioned in GNSO instructions, but allowing other diversions to proceed (such as the recommendation on Code of Conduct)
- Suspension of discussion on differentiation in favor of “guidance”, with the promise of return, but never doing so.
- Inconsistent standards of “proof” which allow some arguments to be dismissed while others stand.

It appears that there is an increasing reluctance of contracted parties to accept ANY new obligations, regardless of the benefits to other parties or the public good. This is troubling for direction.

Summary

The EPDP Phase 1 determined that Phase 2 would “determine and resolve the Legal vs. Natural issue in Phase 2”. This was deferred to Phase 2a. Clearly, we have not achieved this. Moreover, while we have recommended the creation of critical RDDS elements, we are allowing them to be completely ignored. The ALAC has great difficulty in labeling this effort as a success.

**Minority Statement of the ICANN Business Constituency
on the EPDP Phase 2A Final Report⁴⁹**
10-Sep-2021

Introduction

This minority statement is submitted on behalf of the ICANN Business Constituency (BC).⁵⁰

The BC is an ardent supporter of privacy rights and the protective intent of the GDPR. However, in the context of the EPDP team’s work on this expedited policy development process (EPDP) -- a team that was explicitly directed to “preserve the WHOIS database to the greatest extent possible” while complying with privacy law -- the resulting policy exceeds what is necessary to protect the data of natural persons.

The EPDP Team Phase 2A was tasked by the GNSO Council to focus on two specific topics: 1) the differentiation of legal vs. natural persons' registration data and 2) the feasibility of unique contacts to have a uniform anonymized email address. Our comment focuses on the legal vs. natural distinction, the lack of enforceable outcomes and, importantly, and on the critical need to respond to European legislative progress that will impact developed policy, or the lack thereof.

As previously stated, the BC strongly believes that optional differentiation of legal vs. natural persons is inadequate and that ICANN policy must require such differentiation to ensure the security and stability of the global DNS.

In sum, the Phase 2A recommendations, by not making the distinction between legal vs. natural persons, results in a significant number of records being redacted or otherwise unavailable. This is distressing, and even frustrating, given the well-known prevalence of online harms. Such frustration was well-documented in the recent survey by the Messaging, Mobile and Malware Anti-Abuse Working Group (M3AAWG)⁵¹, which detailed the substantial limitations of current access to non-public domain name registration records and affirmed that the solutions currently discussed by ICANN would not meet the needs of law enforcement and cybersecurity actors.

While the EPDP team has designated its recommendations as supported by “consensus”, the BC restates that it does not support Phase 2A outcomes, does not support a “consensus” designation, and here provides justification for its dissent.

⁴⁹ 3-Sep-2021, EPDP Phase 2A Final Report, at <https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20210903/4c231c0a/EPDPPhase2A-FINALREPORT-3September2021003-0001.pdf>

⁵⁰ Prior BC comments and minority report on EPDP Phase 2 include:

- BC and IPC submitted a [joint minority statement for EPDP Phase 2](#).
- [BC Phase 2A Initial Report comments](#)

⁵¹ https://www.m3aawg.org/sites/default/files/m3aawg_apwg_whois_user_survey_report_2021.pdf

BC's View on EPDP Phase 2A Final Report

A core tenet of ICANN's mission is to establish consensus policy that contributes to the security and stability of the DNS and to rigorously enforce any obligations resulting from such policy. However, the BC observes a recent trend -- particularly pronounced in Phase 2A Working Group (WG) deliberations and outcomes -- toward reliance on "optional" obligations (e.g., the use of "should" and "may" in recommendation language) that skirts obligations and does not firmly commit to maintain security and stability. Further, there is growing reliance on the issuance of guidance instead of binding policy, leaving significant latitude for contracted party compliance and weak, watered down, and probably unenforceable policy. This is an unfortunate outcome. The BC believes that the ICANN community should spend time on policy that will uniformly apply to all registrars and registries -- not merely to an undefined subset, acting on their own whims.

In fact, the BC notes that other than the first part of Recommendation #1 (which obligates ICANN to coordinate with the technical community to develop technical standards to facilitate differentiation between legal and natural person registration data), the EPDP Phase 2A Final Report contains no real policy and places no enforceable obligations on contracted parties. This represents an unfortunate failure of the multistakeholder process.

The EPDP team's "consensus" designation for the final report does not reflect the deep divisions in working group outcomes. It is clear that a significant segment of WG membership, as well as a sizable part of the ICANN community, find Phase 2A outcomes to be inadequate. This division should not be overlooked, even as the WG insists on positioning this report as one supported by consensus.

Requiring a Distinction between legal and natural persons

We reiterate that the inability of Internet users to identify with whom they are doing business online, and the increasing inability of law enforcement, cybersecurity, and legal professionals to identify criminal actors online through their domain name registration data, continues to severely undermine ICANN's security and stability mandate. Thus, the interests of these users are not adequately reflected in the policy.

The EPDP Phase 2A team's inability to reach consensus on recommending changes to Phase 1 Recommendation #17.1, and its failure to "determine and resolve the Legal vs. Natural issue" in its deliberations as required by the Phase 1 policy, does not mean the policy defined in Phase 1 Recommendation #17.1 should stand or should become the "default" ICANN policy. In fact, the opposite has occurred. Because the Phase 2A team was unable to reach consensus on this recommendation, we believe the record should

state that consensus opinion did not and still does not exist that would permit optional legal vs. natural differentiation by registrars and registries.

NIS2 Directive

The maturation of the NIS2 Directive signals that the European Parliament not only will address and impact the issue of legal vs natural differentiation, but other WHOIS-related policy, including accuracy, critical data elements, timely publication of non-personal data, and timely reply to legitimate access seekers. ICANN should be keenly aware that key stakeholders, including regulatory authorities in Europe and the United States, are closely monitoring the European Parliament's engagement on these issues via NIS2. Forthcoming opinions and decisions by tribunal and privacy regulatory authorities are likely, and could accelerate as a result of the NIS2-related proceedings. It is distinctly possible that the progression of NIS2 could rapidly overtake ICANN policy development, and ICANN will need to revisit the impact of NIS2 once it is adopted.

ICANN should thus be obligated to properly respond to the NIS2 Directive when it is adopted by the European Union. That gives time for ICANN to update its contracts and policies before NIS2 is first transposed into EU member states' laws. Failure to do so will likely result in a fragmented and inconsistent industry approach to the obligations of the Directive.

Recommendation #1

The BC does not support this recommendation. While we support an obligation for ICANN to define a standard technical mechanism to facilitate differentiation between legal and natural persons' registration data, the BC regrets the lack of obligations of contracted parties to make use of this field, or even to indicate whether they have differentiated. The failure to require use of this technical mechanism will not result in a consistent and reliable RDDS, and is a missed opportunity to reduce the number of requests for non-personal data which has been unnecessarily redacted, such as the contact data for unaffiliated privacy/proxy services. This outcome falls well short of the needs of those involved in the investigation of DNS abuse, cybercrime activity, intellectual property violations, and other activity that threatens consumer welfare.

As stated above, the BC believes strongly that ICANN must take action to update the EPDP policy when the NIS2 Directive has been adopted by the European Union.

Recommendation #2

The BC opposes Recommendation 2 on procedural grounds and with regard to its specific recommendation.

Procedurally, in violation of ICANN Bylaws and the EPDP Phase 2 Charter, the EPDP Phase 2A team inexplicably devoted significant time to developing guidance rather than binding consensus policies. A subset of WG membership effectively “ran out the clock,” dedicating most of its efforts to creating guidance, thereby delaying until the final weeks of Phase 2A any meaningful and robust discussion of how to create binding consensus policies.

The ICANN Bylaws Annex 2-A specifies the process for producing guidance, which requires the formal initiation of a Guidance Process by the GNSO Council. This process was not followed and, as a result, cannot justifiably produce guidance.

Because of this, the policy defined in Recommendation #2 should be adopted as consensus policy and not merely “guidance”, and appropriately enforced.

With regard to the specifics of the recommendation, the BC finds that it also is weak and unenforceable, further hobbling the usability of domain name registration data for legitimate purposes. The recommendation should require contracted parties to follow the tenets of Recommendation 2.

Finally, we note that there is an error on page 20 of the Final Report, which should be corrected as follows:

“This generally allows for publication 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 published disclosed within data marked as a legal person, as this is an example of information that is within the scope of GDPR.”

These clarifications are needed to ensure consistency with the recommendations from the EPDP Phase 1 report -- namely, that information of a natural person **can be disclosed upon request**, for legitimate purposes, provided that an appropriate legal basis exists under GDPR.

Recommendation #3

The BC observes that this recommendation does not define any enforceable obligations on the part of any specific party, nor does it encourage development of such. Recommending that work on a Code of Conduct be “considered” by “any possible future work within ICANN” is vague and unenforceable, and it leaves unattended community priorities that deserve due attention.

Accordingly, the recommendation should encourage ICANN to commence a process for

establishing a Code of Conduct. Should ICANN do so, the BC would object strongly to any process that would not involve all ICANN stakeholders. The definition and development of a Code of Conduct must be carried out in an open, transparent and inclusive manner and must not be developed outside of the ICANN multi-stakeholder process (e.g. via closed-door negotiations between ICANN Org and contracted parties).

Recommendation #4

It was unfortunate that the EPDP team didn't devote adequate time to address this important topic. The BC continues to believe that a registrant-based pseudonymous email address should be **required** to facilitate the investigation of DNS abuse by enabling contactability and cross-referencing of registrations by registrants.

Once again the BC regrets that this recommendation does not define any enforceable obligations on contracted parties, leaving significant gaps between the recommendation and practical implementation. Recommending that contracted parties evaluate legal advice and assess risks, benefits and safeguards is likely to result in an over-cautious, weak, and ultimately ineffectual policy.

This comment was authored by Alex Deacon, Margie Milam, Steve DelBianco, Mark Svancarek, Drew Bennett, and Mason Cole. It was approved in accord with our charter.

IPC EPDP Phase 2A Minority Statement

Data protection law, including the GDPR, does not apply to non-personal data. In fact, while the GDPR is admittedly somewhat ambiguous, it may not even apply to personal data pertaining to legal entities.⁵² Accordingly, databases like WHOIS/RDDS, which serve a multitude of public interest purposes, should only redact data which are demonstrably personal data requiring disparate treatment due to data protection law. However, the EPDP Phase 2A inexplicably and inappropriately shifted the “burden of proof” or at least “burden of persuasion” to those advocating for the common-sense outcome: non-personal data should not be concealed. The IPC notes that the EPDP Phase 2A began its work on the wrong foot entirely by taking on this inappropriate burden and by attempting to provide guidance rather than create binding consensus policy. This is not the role of the PDP - which is designed to develop consensus policy binding equally on all contracted parties. The IPC further notes a troubling trend in multistakeholder policy development throughout the EPDP’s numerous phases: little success is possible when some stakeholders are only willing to act exclusively in their own interests with little regard for compromise in the interest of the greater good. Now more than ever we need to bring our stakeholders together in the interest of the security, stability, and resiliency of the DNS and “promoting the global public interest” as set forth in ICANN’s Articles of Incorporation. Finally, we note that the “consensus” designation ascribed to EPDP Phase 2A recommendations inadequately reflects the division within the working group on these outcomes, and does not reflect that the EPDP Phase 1 Recommendation 17.3 “The EPDP Team will determine and resolve the Legal vs. Natural issue in Phase 2” remains unresolved without a requirement to differentiate.

Specific comments on the EPDP Phase 2A follow.

I. Rely on registrant self-designation

One of the most common-sense disappointments in the EPDP Phase 2A recommendations is the concept that contracted parties should not be required to rely on what a registrant tells them about the nature of the RDS data, and either publish or redact the data accordingly. Legal advice confirmed this common sense assessment, calling the data “low sensitivity”, the risk “low”, and even in the event of erroneous publication based on a registrant’s incorrect self-designation, that “an order to correct the issue (likely accompanied by a reasonable period in which to implement changes), rather than a fine, seems most likely, finding “no examples of enforcement in relation to this.”⁵³

⁵² “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.” GDPR Recital 14

⁵³ <https://community.icann.org/display/EOTSFGRD/EPDP+-P2A+Legal+subteam>

Operating on the basis of such legal advice, a group truly working in the public interest should have easily agreed to publish data that was identified by the data subject as non-personal data. And yet no such agreement emerged.

II. Common data element

The IPC clearly supports the development of a common data element - or elements - to reflect whether RDS data pertains to a legal entity or a natural person registrant and/or whether the data itself contains personal data. While underwhelming as the most impactful outcome of Phase 2A, the IPC is supportive and appreciative of the multistakeholder model coming to consensus on this standardized data element.

That being said, the IPC and colleagues from other Constituencies and Advisory Committees strongly believe that such a standardized data element should be mandatory, especially in the absence of the common-sense publication of data according to registrant representation. While we are encouraged by the agreement to develop this data element, we doubt the likely positive impact of this compromise if such a data element never achieves widespread use by contracted parties. In fact, the IPC is frankly disappointed and discouraged that the Phase 2A team could not agree on any greater use of this data element. Possibilities ranged from optional collection for new domains only to mandatory collection and publication of the field for all domains under management. Yet the bare minimum - optional collection - was the only outcome with the possibility of gaining consensus. This is especially disappointing given that the field itself is not personal data, and therefore no risk exists to publish it. Furthermore, contracted parties never provided any reason for opposing mandatory collection or publication of this data element. They merely repeated “we don’t see the value” (presumably to them as registries and registrars) when presented with the rationale provided by non-contracted parties, which includes: utility for the SSAD, indication of whether to submit an SSAD request or one-off registry/registrar request, information about whether the data was redacted for cause or out of convenience to the contracted party, among others.

III. Future Code of Conduct work

Finally, although it was potentially out of scope for this EPDP Phase 2A, the Final Report contains a provision requiring ICANN to consider the guidance presented in any future engagement with the European Data Protection Board on a Code of Conduct. As an initial matter, the recommendation is weak insofar as it does not actually mandate the creation of a Code of Conduct. Furthermore, the recommendation is phrased ambiguously to include controllers and processors, with a separate sentence alluding to “the community.” More troublingly, when the IPC insisted that the Final Report clarify that groups representing RDS data requestors be included explicitly as controllers and processors (for their own purposes), some contracted parties objected, referring to

requestors as “third party interests.” In the ICANN multistakeholder environment, the community, especially the diverse community represented within and across the GNSO, must not be relegated to “observer” status on something so impactful as the legal status of RDS data which is so fundamental to the security, stability, and resiliency of the DNS.

IV. Registrant-based pseudonymous email address

The IPC continues to believe that a registrant-based pseudonymous email address should be published on a mandatory basis in WHOIS/RDDS. Legal guidance obtained by the EPDP Phase 2A team identified the risk of such publication as “moderate” given that such data could be used to identify a natural person registrant when combined with other personal data. However, the public interest benefits of such publication outweigh the data subject’s privacy rights as the ability to use pseudonymized registrant-based email addresses is critical in facilitating cross-domain ownership correlation to address large-scale security threat networks, phishing schemes, and intellectual property-infringing sites. We note that publication of pseudonymized registrant-based email addresses would appear to comply with the GDPR, and note that several European entities in the DNS supply chain actually publish *actual* registrant email addresses without running afoul of GDPR, as noted in the legal guidance provided to the EPDP.⁵⁴ In the event that the European Data Protection Board or an individual Data Protection Authority identifies this approach as being non-compliant with GDPR, the policy could be reverted to the current requirement of publishing an anonymized email address or link to web form, with disclosure of actual email address in response to valid third-party requests.

V. Conclusion

In conclusion, although the IPC is supportive of the consensus achieved to create a standardized data element to reflect the (legal vs. natural) nature of the registrant and/or the registration data, the EPDP Phase 2A Final Report fails to accomplish its ultimate goal. The EPDP Phase 1 Recommendation 17.3 required that, in addition to optional differentiation, “The EPDP Team will determine and resolve the Legal vs. Natural issue in Phase 2.” Unfortunately, this topic remains unresolved. Requiring ICANN to coordinate the technical community in the creation of a data element which contracted parties are free to ignore altogether falls far short of “resolving” the legal vs. natural issue. And failing to require differentiation of personal and non-personal data

⁵⁴ “In its Whois database, EURid publishes the email addresses of domain name registrants in the .eu TLD (both natural persons and legal entities)... Similarly, while RIPE-NCC relies on consent to publish personal information about tech/admin contacts, it publishes personal information about resource holders on the grounds that ‘facilitating coordination between network operators is the one purpose that justifies the publication of personal data in the RIPE-NCC database and that it is clear that the processing of the personal data referring to a resource holder is necessary for the performance of the registry function, which is carried out in the legitimate interest of the RIPE community and the smooth operation of the Internet globally (and is therefore in accordance with article 6.1.f of the GDPR).’” Bird & Bird memo of 27 April 2021, EPDP Phase 2A Initial Report at 56-57.

fails to meet the overarching goal of the EPDP to “preserve the WHOIS database to the greatest extent possible” while complying with privacy law.

Governmental Advisory Committee Minority Report on the Final Report of Phase 2A of the Expedited Policy Development Process (EPDP) on gTLD Registration Data

Note: The At-Large Advisory Committee (ALAC), the Business Constituency (BC), and the Intellectual Property Constituency (IPC) support the views expressed in this comment.

Introduction and Overall Comment

The GAC appreciates the considerable time and commitment demonstrated by the EPDP Phase 2A team, its leadership and ICANN support staff to develop these complex and important policy recommendations regarding the treatment of domain name registration data from legal entities and pseudonymized email contacts. While the GAC acknowledges the usefulness of many components of the Final Recommendations, the GAC remains concerned that almost none of the Final Recommendations create enforceable obligations. They therefore fall short of the GAC's expectations for policies that would require the publication of domain name registration data that is not protected under the EU's General Data Protection Regulation (GDPR) and create an appropriate framework to encourage the publication of pseudonymized email contacts with appropriate safeguards.

For context, as the GAC has highlighted in prior inputs,⁵⁵ law enforcement, consumer protection, and others tasked with protecting the public from malicious actions facilitated by the DNS, need quick and effective access to domain name registration data. Up until May 2018, such access was publicly available via the WHOIS system. In response to the GDPR, ICANN implemented policies that permit the masking of much of this data, even data that is not protected by the GDPR. Because the GDPR does not protect the contact information of legal persons, many stakeholder groups including the GAC questioned why ICANN policies permitted the redaction of unprotected information in RDS/WHOIS outputs. Therefore, the GAC and other stakeholder groups urged the development of more precise policies that would protect personal data while publishing non-personal data, including registration data related to legal entities, thus recognizing that publishing unprotected domain name registration data benefits the public interest.

The scope of the work under EPDP Phase 2A followed up on these concerns and focused on two topics, namely:

1. the differentiation of legal versus natural persons' registration data, and

⁵⁵ See GAC input on EPDP Phase 1 Final Report (20 February 2019), GAC Input Phase 2 Initial Report (24 March 2020), and GAC Comment on the Addendum to the Phase 2 Initial Report (5 May 2020). See also GAC Abu Dhabi Communiqué (1 November 2017), GAC San Juan Communiqués (15 March 2018), and GAC Barcelona Communiqué (25 October 2018).

2. the feasibility of unique contacts to have a uniform anonymized⁵⁶ email address.

Under the first topic, the questions addressed were as follows:

- 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”);⁵⁷
- ii. What guidance, if any, can be provided to Registrars and/or Registries who differentiate between registrations of legal and natural persons.

Under the second topic “feasibility of unique contacts to have a uniform anonymized email address”, the EPDP Team addressed the questions of:

- i. Whether or not unique contacts to have a uniform anonymized email address is feasible, and if feasible, whether it should be a requirement; and,
- 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 GAC believes that the Final Phase 2A Recommendations provide several constructive components including:

1. the creation of data fields to flag/identify legal registrants and personal data;
2. specific guidance on what safeguards should be applied to protect personal information when differentiating between the domain name registrations of legal and natural persons;
3. encouragement for the creation of a Code of Conduct that would include the treatment of domain name registration data from legal entities;
4. encouragement for the GNSO to follow legislative developments that may require revisions to the current policy recommendations, and
5. useful context and guidance for those who wish to publish pseudonymized emails.

Nevertheless, the final recommendations fall short because they primarily propose optional rather than required actions, even as applied to information that is not protected under the GDPR such as the non-personal data of legal entities. Optional actions can lead to a fragmented and uncertain system for requesters and data subjects, with different policies across different registrars for how data is protected or disclosed.⁵⁸

⁵⁶ The EPDP team later concluded that the term “pseudonymized” was the more precise term. See “Definitions” on p.24 of the [EPDP Phase 2A Final Report](#).

⁵⁷ See Recommendation 17 in the Final Report of EPDP Phase 1 at: <https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf>.

⁵⁸ The GAC has expressed its concerns regarding policies that risk fragmentation in prior inputs including the [GAC Barcelona Communiqué](#) (25 October 2018). See also [GAC Minority Statement](#) on the Final Report of Phase 2 of the EPDP on gTLD Registration Data (24 August 2020).

For background, a significant percentage of domain names are registered by legal entities and the GDPR generally does not protect their non-personal domain name registration data. Some analysis shows that a considerably larger set of registration information was redacted as compared to what is required by GDPR, i.e. “perhaps five times as much as is necessary.”⁵⁹ Indeed, available data suggest that only around 11.5% of domains may belong to natural persons who are subject to GDPR, while contact data from 57.3% of all domains was redacted.⁶⁰ This arguably unnecessary masking of vast amounts of registration data impedes many of the benefits associated with transparency regarding the ownership of domain names.

With regard to the treatment of data from legal persons, the GAC believes that such differentiation should be required for the many different reasons (as noted below) which benefit the public.

First, the publication of non-public domain name registration data concerning legal entities would increase the information available to those entities tasked with protecting the public. Given the prevalence of internet-based crimes, 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, including efforts to combat cybercrime. In addition, publication permits law enforcement or National Computer Emergency Response Teams to 1) quickly identify the jurisdiction/ location of businesses that are a victim of cybercrime and 2) provide at scale, legal entities with notification and protective messaging in the event that their domains have been compromised.

Second, requiring registrars to publish the domain name registration data of legal entities would significantly reduce the number of requests for disclosure of domain name registration data and the challenges associated with obtaining responses to disclosure,⁶¹ because that data set would already be publicly available. Third, making non-personal data available to the public generally increases trust in the DNS by permitting transparency as to the ownership of domain names, including those domains that facilitate sensitive online communications and transactions.

Finally, the legal guidance received underscores the low risks associated with registration data from legal entities. To the extent that personal information is included in a legal entities’ registration data, it is likely to be “low sensitivity” because it relates to an employee’s work details rather than their private life.⁶² Moreover, if the proper

⁵⁹ See Executive Summary of the WHOIS Contact Data Availability and Registrant Classification Study (25 January 2021) at <https://www.icann.org/en/system/files/correspondence/chapin-to-botterman-25jan21-en.pdf>.

⁶⁰ Ibid

⁶¹ See Section 5.3.1 of the [Draft Report](#) of the RDS Review Team (31 August 2018) and [joint survey](#) from the Anti-Phishing and Messaging Malware and Mobile Anti-Abuse Working Groups (18 October 2018).

⁶² See 6 April 2021 [Bird & Bird Memorandum](#).

safeguards are followed, the legal risks associated with such publication, even in the event of inadvertent mistakes, seem low.⁶³

In **summary**, we maintain that a process of differentiation, by the Contracted Parties between data of legal persons and data of natural persons needs to be made mandatory. The Final Report does not sufficiently reflect the various interests at stake in the discussion on differentiation and the subsequent publication of non-protected information. The GAC believes that the public interest outweighs commercial concerns, particularly because the publicly available information would promote the stability, security and resilience of the DNS.

The following comments identify specific concerns with regard to the Final Recommendations.

Recommendation #1 Fields to Facilitate Differentiation between Legal and Natural Person Registration Data

The GAC urged for the creation and use of data fields to flag legal registrants and the presence or absence of personal information in their data sets. Such flagging mechanisms would provide a necessary first step for differentiation. Recommendation 1 includes several obligations with regard to the creation of fields to facilitate differentiation between legal and natural person registration data and identify whether that registration data contains personal or non-personal data. In addition to creating these fields, there are further obligations:

- for ICANN to coordinate the technical community, for example the RDAP WG, to develop any necessary standards associated with such field(s);
- for the SSAD, consistent with the EPDP Phase 2 recommendations, to support the fields in order to facilitate integration between SSAD and the Contracted Parties' systems; and
- for the fields to support specific values related to the status of legal persons and the presence or absence of personal data.

The GAC especially values the precision of this Recommendation in specifying precisely what values should be included in these fields. The GAC though believes that Recommendation 1 would be more effective in creating the necessary infrastructure for differentiation if it:

1. required contracted parties to not just create but also to use these fields;
2. provided specific timelines for making these fields operable; and
3. ensured that the fields will operate within the current and contemplated systems for data collection and disclosure.

⁶³ Ibid

For clarity, the GAC thinks that requiring contracted parties to populate these fields for all future registrations, irrespective of whether the contracted parties elect to differentiate in their treatment of data from natural versus legal entities, is efficient and in the public interest because it would provide a basis to flag and identify data that may be the subject of future expedited SSAD requests or future legal obligations.⁶⁴

The GAC also notes that a voluntary use of such a field is inconsistent with previous phases of the EPDP where measures such as redactions of data were applied to the whole system rather than relying on individual contracted party decisions.

Recommendation #2 Guidance for Contracted Parties who Choose to Differentiate

The EPDP team created the guidance for differentiation based upon the applicable principles of the GDPR and extensive legal advice. Notably, the legal advice identified very specific safeguards to mitigate the risk of wrongful disclosure and observed that in any event, the data involved was not as sensitive as other categories of personal information because it related to work, rather than private life. Finally, the legal advice observed that if the safeguards were followed, then even inadvertent disclosure of personal information would be unlikely to result in enforcement action. Because the guidance adopted the advised safeguards, the resulting liability risks are low, and discussed previously, the benefits to the public are high.

For the reasons identified above, the GAC believes that Recommendation should have required the contracted parties to differentiate between legal and natural entities, and accordingly should have also required contracted parties to apply the applicable guidance identified in Recommendation 2 and publish all non-personal data of legal entities in the publicly available data. The GAC also believes that the safeguards reflected in Recommendation 2 are more aptly referred to as “Best Practices.”

Recommendation #3 Codes of Conduct and Example Scenarios

The GAC welcomes the EPDP team’s Recommendation that the team guidance set forth in Recommendation 2 should be considered by any possible future work within ICANN by the relevant controllers and processors in relation to the development of a GDPR Code of Conduct. The GAC notes that stakeholders affected by such a Code should be given the opportunity to participate in developing the Code including potential requesters (and therefore potential processors) of domain name registration data.

The GAC also appreciates the guidance provided by the specific scenarios. The GAC believes that the logic and clarity of these three scenarios would be improved if they

⁶⁴ In this regard, the GAC welcomes the Final Report’s encouragement to the GNSO to assess whether future policy work is necessary in light of legislative developments. For example, the EPDP noted the current discussions and expected adoption of the Revised Directive on Security of Network and Information Systems (“NIS2”). See “Proposal to the GNSO Council” on p.15 of the [EPDP Phase 2A Final Report](#).

required publication or non-disclosure under the applicable scenarios. Each scenario sets forth specific conditions which logically mandate either publication or non-disclosure of domain name registration data and hence the use of the word “should” rather than “must” in these scenarios is misplaced.

Recommendation #4 Pseudonymized Email addresses

Regarding unique contacts and pseudonymized email addresses, the GAC welcomes steps to provide guidance on publishing an email address through the data protection method of using anonymizing techniques and notes the reduced levels of risk this provides to publication as highlighted in the legal memos received by the EPDP team.⁶⁵ Though the GAC acknowledges there are certain risks involved with publishing even pseudonymized information, GDPR Recital 28 highlights the use of pseudonymization as a method to reduce these risks to data subjects and help controllers and processors to meet their data-protection obligations. Moreover, pseudonymized emails are widely used by privacy/proxy services with little to no impact experienced by many data subjects. The GAC also notes the benefits that such publication of pseudonymized emails would provide, particularly with regard to facilitating quick and effective communications with domain name registrants. There have been reports that certain web forms have not been effective mechanisms to communicate with registrants.

⁶⁵ See 9 April 2021 Bird & Bird Memorandum on [Options for contact address masking](#), and 4 February 2020 Bird & Bird Memorandum on [Questions regarding a System for Standardized Access/Disclosure \("SSAD"\), Privacy/Proxy and Pseudonymized Emails](#).

NCSG Minority Statement on the Final Report of the EPDP Phase 2a

The NCSG are glad to see the final tasks of the EPDP phases 1 and 2 completed. We are also glad that ICANN is finally complying with data protection law, something we have been pushing for since the earliest days of WHOIS policy discussions. The process for this EPDP has been unnecessarily long and painful, however, and does not reflect an appreciation for ICANN's responsibility to comply with data protection law but rather the difficulty in getting many stakeholders to embrace the concept of respect for registrants' rights. We also think that the proliferation of minority statements, reiterating positions that have been argued repeatedly over at least the last nine months, if not the past three years, is unnecessary. However, far be it from the NCSG to stand on principle and refuse to restate our own arguments.

We have repeatedly brought up the rights of the registrant. We were usually alone in stressing the rights of the registrant; we should be joined by at least ALAC, SSAC and the GAC, who have clear roles in representing registrants' rights. Fortunately, the contracted parties also support their customers and pointed out their own obligations to them regularly. ICANN should also be stressing the rights of customers in its role as neutral broker of the MS arrangement to manage the gTLDs.

The lack of clarity about ICANN Org's role as a data controller in a co-controller relationship has also muddied the waters and made it more complex to imagine the policy. We have frequently stated that the precise nature of the roles of ICANN and the contracted parties should have been clarified, doubtless with the aid of outside legal counsel, at the outset of this effort. The nature of the co-controller arrangements is important; much time would have been saved, and confusion avoided, had we been more aware of these eventual contractual relationships.

Several parties have brought up the issue of draft regulations in Europe which may potentially impact the application of the GDPR, and this has slowed the procedure. It is our position that we should not attempt to modify the work achieved in the first two phases of this EPDP, based on speculation about potential regulation. Again, the desire to curb the implementation of the GDPR years before such regulations would be enacted and cast into national laws, indicates a failure to appreciate data protection law and the privacy rights of registrants.

With respect to the precise issues addressed in this report, we have stressed throughout this EPDP, and in a previous PDP on privacy proxy services, that the distinction between legal and natural is not a useful distinction to make, when deciding about the need to protect data in the RDS. It was, as we have reiterated many times, the wrong question to ask, because many workers employed by a legal person or company have privacy rights with respect to the disclosure of their personal information and contact data. The legal person does not have privacy rights, but people do.

Even if we follow the ‘legal vs. natural’ question with a clarifying question requiring the registrant to testify that no personal information is included in the information they provide, this by no means eliminates the risks of revealing personal information. Both questions are difficult for many organizations to answer, particularly the organizations which the NCSG represents, which includes non-profits, volunteer organizations, clubs and interest groups, religious groups, human rights organizations, etc.

This is also true of sole contractors, some types of professionals, and gig workers who are treated like contractors but are actually functioning in an employer/employee relationship. While it is easy enough for large corporations with legal teams, even those with extensive globally dispersed operations, to ensure that they could answer that question, it is not easy for smaller entities with smaller budgets, and a non-corporate manner of engagement with its volunteers and members.

Our position therefore is that because the distinction is not clear-cut for many entities, it is not practical or desirable to mandate the distinction, and whilst the contracted parties have developed excellent guidance for their members to help them decide how to deal with this distinction, that guidance must not form part of the policy. If it is part of the policy, it becomes guidance on legal matters; this is not something ICANN should be doing. The contracted parties are perfectly capable of publishing this guidance on their own, and ICANN is perfectly capable of pointing to it as private sector best practice, not guidance under their policy and enforced by ICANN. The contracted parties ought to know best their own legal risk, and since they are the controllers and responsible for any fines which might come as a result of enforcement action, they must be free to decide how to manage the disclosure of customer information.

We note that those parties who pushed the hardest for making this distinction between legal and natural persons also pushed hard for a field or fields to input the data. Given that the recommendation will remain that it is a voluntary field, and it is up to the contracted parties, whose business models vary enormously, how they use the field(s), we do not believe that recommendations concerning the precision of the field are useful. If ICANN undertakes to instruct the IETF, for instance, how to standardize the field, how is the distinction and the collection and disclosure of the relevant data necessary to make that distinction still voluntary? This is a matter to be left to private sector best practice.

We have also spoken for the rights of gig workers, sole contractors, and independent artists, sales and tradespeople, even though we are explicitly chartered to represent the non-commercial stakeholders. Nobody else is representing these folks, whose numbers are growing apace as employment patterns morph with the global Internet economy. This gap speaks tellingly of the emphasis on big business, and the lack of focus on competitive issues which are exacerbated by DNS policy. We hope that the contracted parties will address the rights of these individuals, and be careful to ensure that they are treated fairly and with due respect for privacy norms when this policy is implemented.

Registrar Stakeholder Group

The Registrar Stakeholder Group (RrSG) representatives to the EPDP Phase 2A Working Group (WG) would like to thank ICANN Staff and all other EPDP WG members for their hard work throughout this phase of the EPDP. The following statement is intended to supplement our consensus vote and input throughout the course of the Phase 2A EPDP work.

General Comments

Throughout the EPDP Phase 2A deliberations, the RrSG team has emphasized that each individual registrar must be able to determine the level of risk they assume, within a baseline that permits adherence to relevant legal obligations. Similarly, each individual registrar must be able to determine what they consider to be commercially and technically feasible for their own unique business.

Although the Recommendations put forward by this EPDP 2A WG do allow that self-determination to occur, providing options and guidance for those registrars and registries which choose to differentiate based on the presence of personal data in the registration record, or which choose to publish a registrant-based or registration-based contact email, it is disappointing that achieving this result was the product of significant struggle. Throughout the work on this Phase, the WG revisited issues repeatedly without adding anything substantially new to the discussion, and discussed topics which were out of scope. Perhaps most importantly, the WG was on many occasions uninterested in or unconcerned with the legal and financial risks that some proposed obligations would create for contracted parties in varying jurisdictions or of differing business models, or the risks to registrants themselves.

Finally, we note that any potential benefits of mandatory policy obligations in these areas, which would negate the crucial ability for registrars to choose their own legal, commercial, and technical risks, were not demonstrated clearly or convincingly enough to showcase an absolute need for such obligations as opposed to less problematic options suggested by the registrar team. Suggested policy obligations were not grounded in strict necessity or broadly-accepted improvements to the domain ecosystem, which may have provided justification for requiring them. The RrSG team is therefore confident that the outcome of the Phase 2A work, including the guidance and the optional requirements for differentiation and use of a registrant-based or registration-based email address, is the appropriate result.

Legal Entities vs. Natural Persons

The RrSG team supports maintaining Phase 1 Recommendation #17 (1), and considers this to be resolution of the issue as mentioned in Phase 1 Recommendation #17 (3). Although the various groups represented in the EPDP Phase 2A WG did not come to agreement on the topic, all relevant inputs were reviewed and addressed in detail during the deliberations and no further deliberation is planned or expected; as such, the issue

has been resolved. Further, this is the *right* resolution. Each individual registrar must be in control of conducting its own risk/benefit analysis and considering its own unique jurisdictional landscape in order to determine if and how it will differentiate, and this maintains the ability to do so.

The registrar team emphasizes that the method of differentiating will vary across registrars. Both the use of “flags” or “fields” to indicate person type or the presence of personal data as well as the contents of the guidance itself have been approached within this Phase as optional, rather than mandatory for all registrars. This guidance is high-level and the product of significant compromise; it is useful but is not applicable in all situations or to all registrars worldwide. As such, it *must* remain optional. Any mandatory guidance or Code of Conduct can only be created by the relevant Contracted Parties themselves, with all due consideration of input from the community.

Feasibility of Unique Contacts

The RrSG team agrees that publishing a registration-based or registrant-based email address in the public RDDS is a data processing activity and appreciates the helpful and thorough input provided by Bird & Bird on this topic. While some implementations of this publication option may be lower risk than others, we note again that each individual registrar must be able to determine the degree to which they assume legal risks, rather than have this decision made for them by the EPDP Phase 2A WG. Accordingly, we encourage all readers of this Final Report to review the legal guidance provided on this topic (included as Annex F to the Final Report), and we anticipate that further guidance and support will be made available to Registrar Stakeholder Group members as needed.

For further insight into the RrSG team’s views on these topics, please refer also to our post on Circle ID: [Privacy, Legal vs. Natural Persons, and the Never-Ending ICANN EPDP](#). Thank you.

Registries Stakeholder Group

Minority Statement to the Final Report of Phase 2A of the Expedited Policy Development Process on gTLD Registration Data

After more than three years of diligence, the RySG is pleased to celebrate the resolution of the Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data (“EPDP”). This was an almost unprecedented effort, triggered by the enactment of GDPR, which required the ICANN community to come together to address long-standing incompatibilities with data protection obligations. The RySG is incredibly grateful for the hard work and commitment of our Chairs and Vice-Chairs, the indefatigable ICANN staff support team, and EPDP team members who have engaged in good faith to reach common ground and understanding on these admittedly complex topics.

The RySG is confident that, as in prior phases of this work, we have struck the appropriate balance between protecting data subject’s privacy rights, fulfilling our legal obligations, and not creating unnecessary obstacles or operational challenges for our customers or our businesses.

I. The Legal vs. Natural Issue is Resolved

Phase 2A has resolved the issue of legal versus natural differentiation. A PDP does not have to result in consensus recommendations to resolve an issue. That the working group did not agree on changes to the previous recommendation (Phase 1 Recommendation 17) on legal v. natural is a valuable and acceptable outcome. After three phases of EPDP deliberation, a study produced by ICANN org, and legal advice from outside counsel on the legal vs. natural issue, it is well past time to recognize this issue as closed.

Indeed, the EPDP Team diligently followed the GNSO Council’s instructions to “answer . . . 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.”)⁶⁶ Responding to that specific question required consideration of the three-part Phase 1 Recommendation 17 in its entirety.⁶⁷ Arguments that the EPDP Team has not satisfied 17.3 (“The EPDP Team

⁶⁶ GNSO Council Instructions for Legal vs. Natural in Phase 2A: “[T]he EPDP Team is expected to review the study undertaken by ICANN org (as requested by the EPDP Team and approved by the GNSO Council during Phase 1) together with the legal guidance provided by Bird & Bird as well as the substantive input provided on this topic during the public comment forum on the addendum and answer:

- 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.”

⁶⁷ [The EPDP Phase I Final Report](#) contains the following recommendation on the legal vs. natural person issue:

Recommendation 17.1: “The EPDP Team recommends that Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so.”

will determine and resolve the Legal vs. Natural issue in Phase 2”) takes a deliberately narrow view of the recommendation text, ignoring the plain language of the GNSO Council instructions. The RySG is concerned that some have suggested this issue is not resolved. This question has been discussed in three separate phases of the EPDP and the result each time has been that Contracted Parties may differentiate but are not required to do so. This clearly demonstrates that this matter has been addressed appropriately and consistently. A perception that this work is somehow unresolved could be detrimental to the ICANN community and seen as undermining the effectiveness of the multistakeholder model. It would also be unfair to the members of the working group and the countless hours they spent deliberating and resolving the issue.

II. Optional Differentiation Remains a Good Outcome

The RySG strongly believes that maintaining the permissive but not mandatory Phase 1 policy recommendations⁶⁸ for legal vs. natural person registration data is an objectively good outcome of our policy development work. This outcome is not about simply maintaining the status quo. We affirmatively believe that the balance struck (after significant consideration) in the Phase 1 Recommendation 17 language is crucially important, especially given the regulatory uncertainty that many on the EPDP Team repeatedly invoke as their justification to change the Phase 1 recommendation. Instead, that uncertainty is in part why Recommendation 17 is an appropriate, flexible, and elegant solution to the question of legal vs. natural differentiation.

a. Contracted Parties must be permitted to control their own legal risks

As the RySG has explained throughout Phase 2A, the flexibility inherent in permitting but not requiring differentiation is important in allowing Contracted Parties to control their own legal risks and mitigate risks to their customers. Registries and Registrars have repeatedly stated this as a fundamental premise throughout the entirety of the EPDP.

The legal memos clearly state, “[i]f the relevant parties had no reason to doubt the reliability of a registrant's self-identification, then they likely would be able to rely on the self-identification alone, without independent confirmation. However, we

Recommendation 17.2: “The EPDP Team recommends that 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.”

Recommendation 17.3: “The EPDP Team will determine and resolve the Legal vs. Natural issue in Phase 2.”

⁶⁸ Recommendation 17.1: “The EPDP Team recommends that Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so.”

understand that the parties are concerned that some registrants will not understand the question and will wrongly self-identify. Therefore, there would be a risk of liability if the relevant parties did not take further steps to ensure the accuracy of the registrant's designation."⁶⁹ Similarly, "[i]f there is a reasonable risk that data subjects will wrongly self-identify, then failing to make the consequences of the self-identification known to data subjects could result in liability for failing to meet the Lawfulness, Fairness and Transparency Principle."⁷⁰

The RySG appreciates that Bird & Bird has provided guidance on how to mitigate those risks. However, the question of how to adopt those procedures and in what manner, not to mention determining what is and is not an acceptable risk, must be the sole responsibility of the Contracted Parties who bear that risk. In any other commercial arrangement this would be an uncontroversial proposition. As we have said since the beginning of this PDP, where Contracted Parties bear liability for processing of data, decisions about that data must reside with Registries and Registrars rather than third parties who do not bear any risk themselves, and do not have shared interests in terms of the protection of our customer's data.

b. Flexibility is desirable

Maintaining flexible rather than prescriptive policies on legal vs. natural differentiation ensures that Registrars and Registries are nimble and able to quickly respond to future regulatory changes that may impact the publication of legal person data without requiring additional policy making. The RySG recognizes that the [Revised Directive on Security of Network and Information Systems](#) ("NIS 2") has the potential, once adopted, to affect how Registrars and Registries process legal person data. The uncertainty around how and when EU Member States will implement NIS 2 is precisely why it is imperative that Registries and Registrars have the flexibility to self-determine their compliance with the shifting legal and regulatory landscape. The changing and evolving privacy landscape reinforces the Phase 1 recommendation affirming the Contracted Parties' option to differentiate between legal and natural persons.

c. Insufficient justification that additional requirements are necessary or even beneficial

Although the RySG feels strongly about Phase 1 Recommendation 17 on its own merits, we also note that no compelling justification was provided as to why mandatory differentiation would be necessary or even desirable. Without more information, we do

⁶⁹ "Advice on liability in connection with a registrant's self-identification as a natural or non-natural person pursuant to the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR)," by Ruth Boardman & Gabe Maldoff, dated January 25, 2019:

<https://community.icann.org/download/attachments/102138857/Natural%20vs.%20Legal%20Memo.docx>

⁷⁰ Id

not understand with any precision what problem mandatory differentiation between legal and natural person registrations is attempting to solve.

III. RySG Trusts the GNSO Process to Determine When Future Policy Work is Required

The RySG supports flagging NIS 2 to the GNSO Council for ongoing monitoring. However, we do not feel that the current draft NIS 2 necessitates new policy work and hesitate to predetermine an outcome that it does. The RySG supports and defers to the GNSO Council's role in determining when policy work is required. GNSO practices and procedures make clear that ICANN policy is not required to direct or duplicate obligations that Contracted Parties are subject to under law. ICANN initiated this EPDP to address the enactment of GDPR, policy work in that instance was necessary because of direct conflicts between the requirements in our agreements with ICANN and the requirements of GDPR. The same cannot be said for potential draft NIS 2 legislation. In the meantime, data protection laws have been passed or come into effect in California, Virginia, Japan, India, and China (to name a few) that some or all Contracted Parties must follow. No one has suggested (rightfully) that ICANN make policy to ensure compliance with those obligations because there are no direct conflicts with our agreements. Ultimately the decision of if and when to initiate new policy work must be left to the GNSO Council, following existing processes.

IV. Recommendation #1 is Out Scope and Raises Significant Implementation Questions

As a reminder, on the issue of legal vs. natural differentiation in Phase 2A, the GNSO Council instructed the EPDP to answer two plainly narrow questions: (1) 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"); and (2) what guidance, if any, can be provided to Registrars and/or Registries who differentiate between registrations of legal and natural persons.⁷¹

Adherence to the agreed upon scope of a PDP is fundamentally important in developing good policy. Unfortunately, the Phase 2A work has suffered from constant attempts to expand the scope of our task, ultimately resulting in a recommendation for creating a data element that we have repeatedly flagged as well beyond our instructions from GNSO Council. The mandatory creation of a new data element has no nexus with the Phase 1 Recommendation #17 language, and therefore is not justified as a response to the first part of our task from the GNSO. Instead of seeking clarification on scope at the outset of the consideration of this issue, the EPDP Chair determined that the creation of a data element relates to guidance within the scope of the EPDP. Moreover, "if the

⁷¹ GNSO Phase 2A Charter, available at <https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-2-priority-2-items-10sep20-en.pdf>

GNSO Council feels like what we are producing is out of scope, that they will communicate that.”⁷²

As a result, the RySG respectfully requests that the GNSO council first examine Recommendation #1 from the perspective of whether the proposal is in fact within the scope of the Phase 2A work prior to considering whether to approve the recommendation. As we explain, we believe that it is not. Should the GNSO determine that Recommendation #1 is in scope, the RySG still has significant concerns about the appropriateness and practical implementation of this recommendation.

a. Recommendation #1 is unrelated to our instructions from Council

We believe that the proposed mandatory creation of a new data element, which requires engagement with the IETF, and likely additional engagement in other areas, does not qualify as the “guidance” referred to in the GNSO instructions. The existence (or not) of a standardized data element does nothing to assist parties in the process of differentiation, it merely captures the outcome of that process. Focusing on the outcome rather than the process is not guidance, at least not practical guidance that is meaningful and therefore does not conform to the EPDP’s instructions from Council.

Similarly, we do not, in considering the possibility of a standard data element, agree that recommending a new data element is related to guidance simply because the data element is referenced in that guidance. We cannot bootstrap items into the scope of the PDP in this manner. The EPDP should not go beyond the scope of its instructions, and our recommendations must be similarly focused.

b. Creating a new data element raises significant implementation issues

If the GNSO determines that Recommendation #1 is in scope of Phase 2A, the RySG still believes that there are significant implementation issues that the GNSO and ICANN must closely consider before adopting this recommendation.

The proposed data element is not something that ICANN can create on its own. The EPP and RDAP Internet Standards (the technical specifications), both of which are the basis for most communication channels used for registration data, are controlled by the IETF. The IETF has a process independent of ICANN within a technical community comprised of more than just ICANN-related parties potentially creating implementation challenges.

Given the significant concerns raised regarding the adoption of this data element, we note that no compelling justification as to why this data element is necessary or beneficial, particularly as part of the public RDDS have been provided. The, rationales put forward, including (i) tracking to what extent Contracted Parties are implementing differentiation; (ii) allowing the public to verify the accuracy of a legal vs. natural

⁷² “On your point about scope, the leadership team and staff have discussed this. It’s my view that what we are discussing here as it relates to guidance is within the scope of the EPDP charter and guidance that was given to us, the questions that were given to us. And I think that if the GNSO Council feels like what we are producing is out of scope, that they will communicate that. And that we have a liaison here with Philippe, who is also the GNSO chair, who will manage any issue along those lines related to scope.” EPDP Chair, Phase 2A Meeting, August 5, 2021.

designation; (iii) determining compliance with applicable laws, (iv) passing references to “consistency”, and (v) ‘what harm’ is there in adopting the data element?; lack specific benefit, and are likely achievable via existing mechanisms. None of the rationales presented make much practical sense, let alone are necessary or compelling enough to justify such significant and out-of-scope changes to existing policy.

As stated above, the existence (or not) of a standardized data element does nothing to assist Contracted Parties who wish to differentiate between legal and natural person registrations, it merely captures the outcome of that process. In considering the possibility of a standard data element, Registries did agree that for purposes of integration with a possible future SSAD system, as recommended in Phase 2, it may make sense for a standardized way of indicating if a registration contains personal data or not. While we acknowledge there may be a use case linked to disclosure decisions in the SSAD, we would prefer to defer those decisions, as is appropriate, to the development of the SSAD rather than taking steps now that may limit the utility of this data element once the SSAD is functional.

The recommendation goes far beyond this, requiring ICANN to create this field in coordination with the technical community for use with EPP and the RDDS. To be clear, the RySG does not support using this field in either EPP or RDDS. As a compromise, we agreed that this is a completely optional field that Contracted Parties who choose to differentiate between legal and natural persons and/or indicate if a registration contains personal data or not could make use of, but are in no way required to use.

In the interests of collaborating in good faith towards a compromise solution, Registries agreed to the creation of a standardized data element and that Contracted Parties could, if they choose to, make use of that standard data element. We have considerable misgivings with the use of such a field in either EPP or RDDS and need to make clear that we don’t support its use with either. We did not hear compelling rationale for why such a field should be used in either case and our support for the creation of such a field does not indicate guidance or a recommendation that it should be used.

V. The Guidance Developed on Legal vs. Natural Differentiation is Insufficient

The RySG supports the concept of guidance that helps Contracted Parties navigate the complex legal and technical challenges that Registries and Registrars routinely face in operating our businesses. In our experience, the best guidance is drafted by those with the appropriate expertise and interests to confront complexity and offer clarity on difficult or ambiguous questions. Despite Contracted Parties’ continued objections and suggestions for improvement, the guidance included in this report on legal vs. natural differentiation meets none of these criteria.

In developing the guidance contained in Recommendation #2, the working group agreed that this is optional guidance that Contracted Parties who choose to differentiate between legal and natural person registrations can leverage at their

discretion. However, the final report language for Recommendation #2 says the Contracted Parties who choose to differentiate SHOULD follow this guidance. The RySG feels that the use of the word SHOULD here does not accurately capture what was agreed to by the working group. Per RFC 2119, “SHOULD . . . means that that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.” Since following this guidance for differentiation is optional, the more appropriate term here is MAY (“an item is truly optional”). While in the interest of collaborating in good faith towards a compromise solution, Registries chose to support the recommendation, we must note that we don’t agree with the use of SHOULD and that Contracted Parties need to consider if the guidance is useful and applicable to them before deciding if they adopt it.

In short, the guidance included in this report on legal vs. natural differentiation is woefully inadequate if its purpose is actually assisting a Contracted Party who wants to differentiate. The guidance falls short for several reasons. First, the guidance is deliberately and unreasonably outcome oriented. Those who have advocated for the necessity of this guidance minimized the process by which differentiation happens, and the associated legal requirements and considerations. This approach almost intentionally obscures rather than grapples with the complexities and risks involved in the process of differentiation, which does nothing to assist the user of the guidance in understanding and addressing those complexities and risks.

Second, the guidance is not practical. Again, by failing to grapple with the complexities and risks inherent in differentiation, the resulting guidance is barely more than a restatement of the law and expected outcomes. For example, the guidance states:

“Registrars should ensure that they clearly communicate the nature and consequences of a registrant identifying as a legal person. These communications should include:

- *An explanation of what a legal person is in plain language that is easy to understand.*
- *Guidance to the registrant (data subject)^{35 641} by the Registrar concerning the possible consequences of:*
 - *Identifying their domain name registration data as being of a legal person;*
 - *Confirming the presence of personal data or non-personal data, and;*
 - *Providing consent. This is also consistent with section 3.7.7.4 of the Registrar Accreditation Agreement (RAA).”*

Unfortunately, for a user of this guidance, this brief section raises more questions than it answers. What is a legal person? What if the registrant is not the data subject? What are the consequences to flag for the data subject? What steps are needed to ensure that the data subject understands this messaging (e.g., A/B testing, user panels)? What are

the risks if these steps are not followed? How is meaningful consent obtained, especially where the registrant may not be the data subject? Is education of, or notice to the registrant sufficient to mitigate risk? Merely restating obligations that are largely already dictated by law does very little here to actually assist a user of the guidance in navigating these issues.

Similarly, the guidance states in the very last paragraph that:

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.

This is in fact the hardest and riskiest issue in differentiating between legal and natural person registrations. As the EDPB directed ICANN, “[t]he 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.”⁷³ This guidance does nothing to contemplate or even minimally explain how a Registrar might begin to approach the issue. Addressing this core challenge almost in passing severely undermines the utility of this guidance and increases our concern about the overall practicality of this advice.

In the interest of collaborating in good faith, the RySG agreed to support the publication of this guidance despite the concerns outlined above, as the recommendation makes clear that the guidance is truly optional and Contracted Parties (even those who choose to differentiate) are in no way required to follow Recommendation #2. We are skeptical that this guidance will be widely adopted, not because guidance on this issue is not wanted, but because these guidelines do nothing to guide practical implementation and do not offer any comfort to the parties that bear the legal risks.

VI. Conclusion

For all the above reasons, given the continued support of the various parties in the EPDP team for the publication of this final report and the recommendations as stated, and notwithstanding our concerns relating to the scope of the recommendations, the RYSG does not object to the passage of this report and the recommendations as stated. It is noted however, that this support is based on the good faith belief that all parties maintain the agreed level of consensus. While, the RYSG does not support a number of aspects of this report, in the spirit, and support, of the multistakeholder model, we have compromised.

⁷³ EDPB Letter to Goran Marby, dated July 2018, available at <https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf>

SSAC Minority Statement On the Temporary Specifications for gTLD Registration Data - Phase 2A Expedited Policy Development Process Final Report⁷⁴

1 Introduction

The ICANN Security and Stability Advisory Committee (SSAC) appreciates the circulation of the Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2A (hereinafter referred to as “the EPDP 2A Initial Report”),⁷⁵ and we thank the working group for the opportunity to comment on it.

In this document the SSAC presents both general comments about the overall Expedited Policy Development Process and specific comments on individual recommendations in the EPDP 2A Initial Report. The SSAC would be happy to discuss these comments with the EPDP team at their convenience to explain any items that may be unclear and require further elaboration.

The SSAC would like to acknowledge the significant time and effort devoted by the members of the EPDP team and thank them for their contribution on this important topic.

2 Background

In this section we review the questions under consideration by the EPDP Phase 2A Working Group (WG), we make some observations about the overall Expedited Policy Development Process, and then we describe our approach. In the following section we present our recommendations, some of which apply to the overall effort and some of which are specific to the Phase 2A effort.

2.1 Questions Under Considerations by the EPDP Phase 2A WG

2.1.1 Distinguishing Natural versus Legal Persons

The General Data Protection Regulation (GDPR) provides specific protection for natural persons (i.e., humans), and no protection for legal persons (i.e., businesses).^{76,77} The EPDP WG, and particularly the EPDP Phase 2A WG, has focused considerable attention on this distinction. Among the questions the EPDP WG has considered are:

⁷⁴ The document was published as SAC118, available at: <https://www.icann.org/en/system/files/files/sac-118-en.pdf>

⁷⁵ See Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2A, <https://www.icann.org/en/system/files/files/epdp-phase-2a-initial-report-02jun21-en.pdf>

⁷⁶ See GDPR Recital 14: “The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. 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.” <https://gdpr-info.eu/recitals/no-14/>

⁷⁷ See GDPR Article 4, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1374-1-1>

1. Should there be a specific data element to record whether the registrant is a natural person versus a legal person?
2. Should every registrar be required to make this determination for every registration?
3. What evidence should be required to make this determination?
4. What are the risks if the registrar's determination is incorrect?
5. Should the registrant be required to declare whether they are a natural person or legal person and should the registrar rely on that attestation?
6. Should the contact data for registrants classified as legal persons always be available publicly?⁷⁸
7. Should the contact data for registrants classified as natural persons never be publicly available?
8. Should the status of the registrant be available publicly?
9. How to proceed when the personally identifiable information (PII) of a natural person is included as part of the registration of a legal person?

2.1.2 Feasibility of Unique Contacts

The EPDP team was asked to consider the questions:

- Whether or not a unique contact in the form of a uniform anonymized email address is feasible, and if feasible, whether it should be a requirement?
- If feasible, but not a requirement, what guidance, if any, can be provided to ICANN Contracted Parties who may want to implement uniform anonymized email addresses?

The EPDP team observed that “unique contacts” is a vague term, and that there are two distinct goals stated by those advocating for unique contacts. These are: (1) the ability to quickly and effectively contact the registrant without disclosing personal data, and (2) A common identifier that helps investigators to correlate domain registrations with a common contact.

The EPDP team tried to disambiguate these purposes by proposing two terms:

- **Registrant-based email contact** - an email for all domains registered by a unique registrant [sponsored by a given registrar] OR [across registrars], which is intended to be pseudonymous data when processed by non-Contracted Parties.
- **Registration-based email contact** - 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.

⁷⁸ The EPDP WG generally treats the request and response process as if the “public” data is published for anyone to see. In all anticipated scenarios, all access to registration data is via a request-response process. That is, the registration data is not published in the sense that publication is generally understood. In this document, we use the phrasing “available publicly” to mean data that is available to anyone who requests it without restrictions on use and without attribution.

After some deliberation, the EPDP team did not provide a conclusive answer on the feasibility of registrant or registration-based email contact. The EPDP team recommended that “Contracted Parties who choose to publish a registrant- or registration-based email address in the publicly accessible registration data directory service (RDDS) should ensure appropriate safeguards for the data subject in line with relevant guidance on anonymization techniques provided by their data protection authorities and the appended legal guidance.”

The SSAC notes that some registrars have already deployed a few different methods to support registrant-based email contact. For example, registrant-based email addresses have been uniquely created for each registrant, hosted with a domain of the registrar. Messages directed to these email addresses are redirected upon receipt by the registrar to the actual recipient. Some registrars provide a web-based form that can be used to direct a message to the registrant of a particular domain name. In most cases, the sender of the original message does not know if the forwarded message was delivered or opened. The Temporary Specification does not provide any service level requirements for the email forwarding.^{79,80}

The SSAC is not currently aware of any deployed solution that satisfies the requirements of registration-based email contact as defined above. Anecdotally, a small number of solutions have been proposed but none have achieved any consensus.

2.2 SSAC Observations

Based on participation in the EPDP, SSAC offers two comments regarding the overall effort to achieve a differentiated access system that meets multiple objectives. By differentiated access system, the SSAC means a system that provides the capability for the response to be conditioned based on the requester and the purpose of the request. The System for Standardized Access/Disclosure (SSAD) is a specific example of such a system.

2.2.1 Competing Interests

From the SSAC’s perspective, there are three competing interests at work in the policy deliberations.

1. **Privacy advocates.** Some parties want to ensure the contact data for natural persons is not available publicly unless the natural person provides explicit and informed consent to allow public availability. They want this protection to apply to legal persons as well if the contact data includes PII or if PII can be inferred from the contact data.

⁷⁹ Temporary Specification for gTLD Registration Data; Appendix A: Registration Data Directory Services, paragraph 2. <https://www.icann.org/resources/pages/gtld-registration-data-specs-en>

⁸⁰ There have been documented problems with the contactability implementations at registrars. See pp 55-59 of “Domain Name Registration Data at the Crossroads: The State of Data Protection, Compliance, and Contactability at ICANN.” <http://www.interisle.net/domainregistrationdata.html>

2. **Data requesters.** Requesters want the maximum amount of data they can get. Requestors want the privacy protections to be as close as possible to only what's legally required. They want requests to be fulfilled reliably, quickly, and inexpensively.
3. **Data controllers.**⁸¹ Those who collect and make the data publicly available, namely registrars and registry operators, want to minimize cost and risk.

Specific individuals or organizations may embody more than one of these competing interests.

2.2.2 An Unspoken Concern

The SSAD is a new system proposed to centrally handle requests for non-public registration data, envisioned in Recommendations 1-18 of the Final Report of the GNSO Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Phase 2.⁸²

A well-designed access system will allow requesters with legitimate needs to gain access to non-public data, and to do so reliably, quickly, and inexpensively.

At this time, it is uncertain if we can achieve a satisfactory differentiated access control system. Currently, the ICANN Board has requested a six-month Operational Design Phase (ODP) Assessment to inform its deliberations of the policy recommendations. The proposed SSAD does not yet have a scheduled date of delivery. The initial cost estimate has been criticized by the community as too expensive. There is also a lack of definition as to what data will be available to which requesters, and under what circumstances. Finally, Contracted Parties may be performing manual reviews of data requests, because the EPDP was unable to agree on automation cases.

Due to the lack of clarity on SSAD, some of the participants in the EPDP appear to be assuming the only data they are likely to access for the foreseeable future is publicly available data, and they are pressing to keep the privacy protection to the minimum required by law. The result is an inability to resolve many questions in the EPDP.

2.3 SSAC's Approach

The SSAC believes it is very important for security investigators to get access to domain name registration data. At the same time, it is also important for those who deserve protection to have it. These two alternatives can coexist. But they cannot coexist in the context of a head-to-head argument about whether every single contact should be public or not as the only choice to be made.

⁸¹ The term also includes others collecting or processing the data collected during registration (i.e., resellers).

⁸² See Final Report of the Temporary Specification for gTLD Registration Data Phase 2 Expedited Policy Development Process, <https://gns0.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf>

It should be possible for contact information which is considered personal, to be held privately and made available under appropriate circumstances to the people who need it. From the SSAC perspective, a timely, reliable, effective, and efficient differentiated access system would make it possible to achieve a result that would be an improvement for all of the competing interests.

Thus, the SSAC believes the focus of the ICANN Community and ICANN org’s attention should be to build and operate an effective SSAD.

As things stand, discussion of access to non-public data is outside the scope of the Phase 2A EPDP, and discussion of the Phase 1 and Phase 2 reports is considered closed. Therefore, in this report, we make two kinds of recommendations.

1. Overarching recommendations on differentiated access and the SSAD.
2. Within the scope of the EPDP Phase 2A, we offer some detailed recommendations that, if adopted, make the best of an imperfect situation.

3 Recommendations

3.1 Recommendation to GNSO and ICANN org

Recommendation 1: The SSAC recommends the Generic Name Supporting Organization (GNSO) and ICANN org focus their attention on building and operating an effective differentiated access system.

A differentiated access system with the following properties is needed:

Timely	It must come into operation soon.
Reliable	It must operate in a predictable and consistent fashion, both in the operation of the system and the decision-making by the participants of the system.
Useful	It must provide results that are of benefit to the requesters.
Efficient	It must provide responses to legitimate data requests quickly, and at a cost to all the parties that are acceptable for the purpose.
Easily Accessed	Gaining and maintaining credentials has to work well enough to facilitate—rather than impede—use.

This document uses the term “effective” to refer to a differentiated access system fulfilling all the above requirements, and, of course including the functionality required to manage distinct requests and responses to various combinations of requesters and purposes as noted in Section 2.2.

3.2 Recommendations to the Phase 2A EPDP

3.2.1 Legal Versus Natural

From a security practitioner’s perspective, the maximum amount of registration data needs to be available for investigation, either through an effective differentiated access system, or through making it available in the public RDDS.

Recommendation 2: The SSAC recommends the following regarding legal versus natural persons:

- A. A data element should be defined that denotes the legal status of the registrant. Initially we propose three admissible values: Natural, Legal, and Unspecified. “Unspecified” would be the default value until the registrant identifies themselves as a natural or legal person. This field should be able to support status values depending upon future policy decisions.
- B. This data element should be displayed as part of the publicly available data.
- C. Registrants should be classified as either natural or legal persons. This should be required at the time of registration, for all new domain registrations. For existing registrations, the value can remain “Unspecified” until it is filled at a later time. Registrars should be required to ask at relevant times, such as upon domain renewal and/or the annual accuracy inquiry, whether the registrant is natural or legal, with the goal of eventually obtaining that data for all registrants, and reducing “Unspecified” to the lowest practical level.
- D. Registrants currently are able to and should continue to have the option of making their contact data publicly available. Legal person registrants should also have the ability to protect their data via privacy and proxy services.

These recommendations are consistent with SSAC’s previous advice.⁸³

3.2.2 Feasibility of Pseudonymous Email Contact

Recommendation 3: The SSAC recommends the following regarding the feasibility of pseudonymous email contact:

- A. The two policy objectives--namely (1) the ability to quickly and effectively contact the registrant without disclosing personal data, and (2) A common identifier that helps investigators to correlate registrations with common contacts should be considered separately.
- B. To achieve policy objective (A1), registrars should deploy (or continue to deploy) methods to support registrant-based email contact (See section 2.1.2 discussion of the two methods). The SSAC further recommends uniform requirements for safeguards be developed for the registrant-based email contact. The requirements should include maintaining the privacy of the registrant as appropriate and service level commitments to set expectations for the use of the

⁸³ See SAC104, section 3.6. <https://www.icann.org/en/system/files/files/sac-104-en.pdf>

- service. These safeguards are independent of the method chosen (e.g., unique email addresses or web-based forms).
- C. To achieve policy objective (A2), additional research is needed on the methods, their efficacy, and their tradeoffs. We recommend the EPDP Phase 2A *not* specify a method for correlating registrations with a common contact at this time.

Annex E - Community Input

E.1. Request for Input

According to the GNSO's PDP Manual, an EPDP Team should formally solicit statements from each GNSO Stakeholder Group and Constituency at an early stage of its deliberations. The EPDP Team is also encouraged to seek the opinion of other ICANN Supporting Organizations and Advisory Committees who may have expertise, experience or an interest in the issue.

The EPDP Team solicited input on these two topics as part of the early input requested during Phase 1 and Phase 2, and accordingly, the EPDP Team reviewed and considered the input provided at that point (see <https://community.icann.org/x/Ag9pBQ> and <https://community.icann.org/x/Ag9pBQ>) at part of its deliberations.

E.2. Public Comment forum on the Initial Report

On 3 June 2021, the EPDP Team published its [Initial Report for public comment](#). The Initial Report outlined the team's thinking up until that point and was intended to serve as a tool to solicit community input, especially on areas where significant divergence remained. Although preliminary recommendations were included in the Initial Report, the EPDP Team requested these recommendations be considered in combination with a set of questions raised to help inform the finalization of its report.

The EPDP Team used a Google form to facilitate review of public comments. Sixteen contributions were received from GNSO Stakeholder Groups, Constituencies, ICANN Advisory Committees, companies and organizations, in addition to one contribution from an individual. The input provided can be found here: https://docs.google.com/spreadsheets/d/1aRxF19pd5tEyO07_zaj7YvzOPjflBfgi4WRy-nx8yY/edit?resourcekey#gid=1754667842.

To facilitate its review of the public comments, the EPDP Team developed a set of public comment review tools (PCRTs) and discussion tables (see <https://community.icann.org/x/coMZCg>). Through online review and plenary sessions, the EPDP Team completed its review and assessment of the input provided and agreed on changes to be made to the recommendations and/or report.

Annex F – Bird & Bird Legal Memos

Response to Questions 1 and 2 (Legal v. Natural)

MEMORANDUM

To: Internet Corporation for Assigned Names and Numbers, EPDP Team
From: Ruth Boardman & Phil Bradley-Schmieg
Date: 6 April 2021
Subject: March 2021 questions regarding legal personhood, consent *etc.*

Background

1. The EDPB, in [a July 2018 letter to Göran Marby](#), stated 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”.

Consent

2. [Appendix A of the Temporary Specification](#) states that

“In responses to domain name queries, Registrar and Registry Operator MUST treat the following fields as "redacted" unless the contact (e.g., Admin, Tech) has provided Consent to publish the contact's data: (...)”.

3. Recommendation #6 of the [EPDP Phase 1 Final Report](#), adopted by the ICANN Board in May 2019, states:

“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.”

4. The [EPDP Team Phase 2 Final Report](#), dated 31 July 2020, also noted at footnote 83 that:

“Another topic that would encourage less manual processing would be to explore what legally permissible mechanisms contracted parties could implement to permit data subjects to provide either freely given consent or objection to disclosure of their data at the time of domain name registration. This would facilitate maintenance of databases of protected versus non-protected

information, opening non-protected databases to lower-cost automated processing.”

5. Bird & Bird has provided advice on this issue, notably in our Memorandum dated 13 March 2020, “*Advice on consent options for the purpose of making personal data public in RDS and requirements under the [GDPR]*” (the “[Consent Memorandum](#)”).

Legal vs. natural personhood

6. In May 2019, the ICANN Board also adopted Recommendation #17 of the EPDP Phase 1 Final Report, which states:

“1) The EPDP Team recommends that Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so.

2) The EPDP Team recommends that 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.*

3) The EPDP Team will determine and resolve the Legal vs. Natural issue in Phase 2.”

7. Bird & Bird has provided advice relevant to this issue, notably in:
 - 7.1 our Memorandum dated 25 January 2019, “*Advice on liability in connection with a registrant's self-identification as a natural or non-natural person pursuant to the [GDPR]*” (the “[Natural vs. Legal Memorandum](#)”); and
 - 7.2 our Memorandum dated 9 April 2020, “*Advice on Accuracy Principle under the [GDPR]: follow up queries on “Legal vs. Natural” and “Accuracy” memos*” (the “[Accuracy Follow Up Memorandum](#)”).
8. EPDP members may also recall that GDPR Article 83(2) lists the factors to be considered when a supervisory authority decides whether to impose an administrative fine (and if so, how much). These include the number of data subjects affected, the nature of the data, the intentional or negligent character of the infringement, actions taken by the controller to mitigate damage, and the

degree of responsibility of the controller taking into account technical and organisational measures implemented by them pursuant to GDPR Articles 25 and 32.

9. Against this background, you have raised a number of inter-related questions.

Question 1

Question presented: Under the consensus policy adopted, Registrars will give Registrants the opportunity to consent to publication of personal data included in their Registration Data. Please compare the legal risks for contracted parties associated with:

1) publishing personal data based on the Registrant's consent, on the one hand,
and,

2) publishing data based on a Registrant's (i) self-identification of the data as either containing legal person data only or also containing natural person data (organization or individual) prior to publication and (ii) undertaking the verification procedures outlined in Bird & Bird's January 25, 2019 memo (i.e., notify/explain; confirm; verify; opportunity to correct) on the other hand.

Analysis

10. We assume this question, and those below, are asking about the scenario raised as an issue by the EDPB in its letter to Göran Marby at paragraph 1 above; namely where the Registrant is a legal person, and one of its employees (or agents) completing a registration on behalf of the Registrant provides their own and/or other data subjects' personal data (e.g. listing a colleague as Admin contact).
11. In such a scenario, of these two measures, the latter (which for the purposes of this memorandum we shall refer to as Verified Self-Characterization, "VSC") is legally lower risk for Contracted Parties. It may be possible to combine the two.

Consent

- 11.1 A data subject must themselves decide whether to give consent. This means that in the scenario being analysed, the person completing a domain registration on behalf of the (legal person) Registrant could only consent to the publication of their own personal data. They cannot consent on behalf of their colleagues or others ("third party data subjects"), if details of any are provided. In that situation, they could only *relay* the outcome of that third party's consent decision to a Contracted Party.
- 11.2 In such a situation, which we expect is not uncommon, the first option (reliance on Registrant consent) may therefore leave Contracted Parties unable to concretely demonstrate that (i) the third party data subject actually consented; and/or (ii)

- that such consent met all GDPR requirements for consent validity (which are explained in paras 13-18 of the Consent Memorandum).
- 11.3 The Consent Memorandum presented five options for a consent-led approach (Consent Memorandum, para. 24). It is not clear which of these options is envisaged for the purposes of the present question.
- 11.4 The Consent Memorandum explained that:
- 11.4.1 a scheme where controllers seek valid consent directly from all data subjects (contrary to what the present question appears to be proposing) would be lower risk than merely relying on assertions from the Registrant that a valid consent had been obtained from data subjects; and
- 11.4.2 *if*, nevertheless, the system was designed around confirmation from the Registrant that a valid consent was obtained from data subjects, Contracted Parties would be better off either verifying the consent directly with the individuals, or demanding that the Registrant provide *evidence* that a valid consent was obtained.

Verified Self-Characterization

- 11.5 The second option provided in the Question presented, VSC, is presumably suggesting that as a rule personal data will **not** be published in Registration Data (and just in case it will be included by default, a check is made by contacting the provided contact details).
- 11.6 Therefore, *if* any personal data is in fact included in Registration Data, this would be a hopefully rare and unintended event.⁸⁴ In short, the GDPR should for the most part be inapplicable except in accidental edge cases.
- 11.7 In those theoretically rare edge cases, several factors would mitigate Contracted Party liability (particularly in light of GDPR Article 83(2), discussed at paragraph 8 above) – whether for the inaccuracy, or the processing of personal data without a legal basis (e.g. consent). In particular:
- 11.7.1 Significant steps were taken to verify that the data is not personal data; and
- 11.7.2 An easy means of correcting mistakes was provided.
- 11.8 There may even be an argument, based on EU Court of Justice (“CJEU”) caselaw, that this is a situation where Contracted Parties should generally only be liable should they fail to properly address a complaint about the data – i.e. only once they are put on notice about the alleged illegality and thereby have an opportunity to “verify” the merits of the complaint.⁸⁵ This bears some parallels to other EU

⁸⁴ Attributable to the Registrant’s own error and/or a failing in the verification mechanisms deployed by a Contracted Party.

⁸⁵ In its judgement in Case C-136/17 *GC and Others*, the CJEU explained that GDPR obligations relating to an erasure (“Right to Be Forgotten”) request apply “to the operator of a search engine in the context of his responsibilities, powers and capabilities as the controller of the processing carried out in connection with

liability regimes for operators of services online that process – unwittingly – content that violates EU law.⁸⁶ As discussed at footnote 88 below, this is arguably recognised in (at least some) decisions of GDPR supervisory authorities.

Combination

- 11.9 Though VSC offers lower risk for Contracted Parties, it has a downside: it means that personal data is not (normally) published. For some stakeholders, this will seem like a missed opportunity to maximise the availability of publicly available registration data.
- 11.10 Contracted Parties may therefore wish to consider a combination of mechanisms: ask the individual completing the registration, whether the data they are providing is personal data. If they say no, then verify this claim by contacting the provided contact details (VSC). If they instead say yes, then ask them whether the personal data relates to them, and if so, whether they would be happy for those details to be published.
- 11.11 Accuracy is sometimes presented as a GDPR concern with respect to registration data publication. Though our enquiries have turned up no substantial precedent for enforcement in a situation such as that being discussed here, it seems to us that under this combination model (VSC + consent):
- 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.

QUESTION 2

Question presented: Paragraphs 17 through 25 of Bird & Bird’s memo dated January 25, 2019 [the Natural vs. Legal Memorandum] discussed the potential risks to Registrars associated with reliance on a Registrant’s (i) self-designation as a legal person and (ii) confirmation that the registration data does not contain personal

*the activity of the search engine, on the occasion of a verification performed by that operator, under the supervision of the competent national authorities, following a request by the data subject”. As the Advocate General explained in that case, “such an operator can act only within the framework of its responsibilities, powers and capabilities. In other words, such an operator may be incapable of ensuring the full effect of the provisions of [EU data protection law], precisely because of its limited responsibilities, powers and capabilities. . . An ex ante control of internet pages which are referenced as the result of a search does not fall within the responsibilities or the capabilities of a search engine.” It could not know, from the moment it indexed a webpage, that the content of that page was (for example) out of date (as in the original *Google Spain / Costeja* ruling), or (in the *GC and Others* case) “special category” or “criminal offence” data for which it required consent.*

⁸⁶ See, for example, [Article 14](#) of the e-Commerce Directive 2000/31/EC and its transposition into the national laws of EU/EEA Member States and the UK.

data. The memo identified a variety of steps that Registrars could take to mitigate the risk of inadvertent publication of personal data.

For example, the memo suggested Registrars might take certain steps to improve the accuracy of self-designation/attestation such as: providing separate, clear disclosures, including descriptions of the consequences of self-designation as a legal person and asking the registrants to confirm that they are not submitting personal data; testing the clarity/readability of such disclosures; periodic follow up emails to registrants and/or technical contact; and providing a mechanism to change self-designation, or correct or object to publication of personal data.

Q2(1): Assuming that a Registrar takes the mitigation steps identified by Bird & Bird, and based on your experience and applicable precedent, please describe the level of risk, likelihood of enforcement actions, fines, counseling, etc. flowing from subsequent inadvertent publication of personal data contained in the Registration data of a legal person.

Q2(2): Expanding on Question [2(1)], please discuss what level of risks (e.g., enforcement actions, fines, counseling, etc.) a Contracted Party faces with respect to publication of personal data if a confirmation email sent by a Registrar the Registrant and/or the Registrant's tech contacts (i) clearly states that the Registrant has self-designated as a legal person and has affirmatively stated that no personal data has been included in its registration data; (ii) explains that based on those two representations all fields in the registration data will be published on the Internet; and (iii) provides an easy-to-use mechanism through which the self-designation can be rescinded and an individual receiving the email can object to publication of their personal data and/or rectify any inaccurate data? Must the Registrar require the registrant's and/or tech contact's affirmative response to the confirmation email? Does the answer differ depending on the medium of the notification (e.g., snail mail v. email)?

Q2(3): Are there additional or alternative mitigation and/or verification steps that a Contracted Party could take to further reduce/eliminate liability associated with inadvertent publication of personal data in connection with reliance on a registrant's self-designation, e.g. confirming the existence of corporate identifiers (Inc., GmbH, Ltd. Etc.), reviewing account holder data for indicia of legal personhood, etc.? To what degree would each such additional step reduce liability?

12. With respect to Q2(1) (level of risk, generally, if the described VSC measures are adopted): despite our having searched for precedent in several EU/EEA Member States, we are not aware of comparable precedent. Moreover, note that enforcement trends and regulatory action policies are continuously evolving, as is the viability of civil suits by litigants.
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. Our view is based on the following factors (also bearing in mind GDPR Article 83(2), discussed at paragraph 8 above):
- 14.1 Erroneous inclusion of personal data, despite the measures described there (assuming they are well implemented), seems like it would occur only on an exceptional basis. As we advised in the Natural vs. Legal Memorandum, it would be advisable for ICANN and the Contracted Parties to study (e.g. gather statistics) in order to monitor whether the measures are acting as intended.
- 14.2 If personal data is erroneously included in published Registration Data, it would in this scenario occur despite substantial (VSC) steps taken by the Contracted Parties, and would be primarily attributable to the actions/omissions of the Registrant. This is likely to be taken into account by data subjects, data protection supervisory authorities, and courts.
- 14.3 The data in question is likely to be low sensitivity. The scenario being envisaged here (mistaken inclusion of personal data in published Registration Data) seems to be most likely to occur when a legal entity (e.g. a company or non-profit organisation) is registering / maintaining its own domains. In those scenarios, we assume the personal data that could be disclosed would ordinarily relate to an employee's work details (e.g. a company email address), not an individual's private life. Although the GDPR confers protection even in the workplace, the data in question here may arguably be less capable of causing harm to an individual than data relating to the data subject's private life.⁸⁷
- 14.4 In more sensitive cases (e.g. disclosing that a person works for a company in a sensitive or "embarrassing" sector), a Registrant would be putting itself at serious risk of complaints from its own employees. Registrants are therefore already incentivised to avoid errors that could have serious consequences for their own staff.
- 14.5 The measures envisaged include an ability to correct the mistake. Of course, the nature of the global Internet is that it may be difficult to fully remove erroneously-published data from mirrors / caches / archives, if any services are set up to do this. We would therefore encourage the supplementary measures envisaged for Q2(2) below.
- 14.6 Finally, as noted above, it may be possible to base arguments on the *GC and Others* case, that liability should attach to a Contracted Party only if and when they fail to properly address complaints about the inclusion of personal data in published Registration Data – and not from the earlier point of the data's unintended publication. That said, this seems conditional on the controller(s)

⁸⁷ 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.

having taken reasonable measures to prevent such inclusion (e.g., the VSC measures discussed herein).

With respect to Q2(2) (level of risk if a confirmation email is sent, offering an easy means of rescinding self-designation / rectifying inaccuracies):

15. In our view, 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.
16. Contracted Parties would need to account for postal (“snail mail”) timescales if that medium is used – it may take some time for post to be delivered to the organisation, and then find itself to the right person (who may be out of office, e.g. on annual leave), and then be dealt with by that person. Email would at least not usually suffer from delivery delays; the grace period would then only need to address a possible leave of absence and/or the recipient’s temporary inability to deal with the email for other reasons.
17. In our view, 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 (i.e. the VSC check should be treated as failed in that case).
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.
19. With respect to Q2(3) (additional or alternative steps to reduce liability under VSC): our advice at paragraphs 21-25 of the Accuracy Follow Up Memorandum is especially pertinent here. Much of that discussion, and the table of 16 possible additional measures that could be taken to minimize or compensate for possible inaccuracies in Registration Data, remains relevant here.
20. The question, as you have posed it, already reiterates many of those measures, namely: *“providing separate, clear disclosures, including descriptions of the consequences of self-designation as a legal person and asking the registrants to confirm that they are not submitting personal data; testing the clarity/readability of such disclosures; periodic follow up emails to registrants and/or technical contact; and providing a mechanism to change self-designation, or correct or object to publication of personal data.”*
21. The present question also suggests *“confirming the existence of corporate identifiers (Inc., GmbH, Ltd. Etc.) [and/or] reviewing account holder data for*

- indicia of legal personhood*". In addition, asking for a company registration number may be another means of verifying legal personhood.
22. That said: most employers will be able to provide a company number and/or a company name ending in Ltd., PLC, SA, BV, GmbH, *etc.* – and yet they could also provide personal data about their employees, e.g. as contacts for the domain. Accordingly, such a check – even if viable – only confirms that the Registrant is a legal person. It does *not* confirm that a legal-person Registrant has not (also) provided personal data, e.g. about its staff. This measure thus helps avoid natural-person registrants from mischaracterising their own data – but that may not be a major risk (from a GDPR perspective), since those persons are in any event incentivised to properly declare their status as a natural person, and their declaration can be verified by contacting them. The alternative and possibly greater risk – that an employer includes its employees' personal data – is unaffected by such a measure. Such a measure therefore has limited GDPR benefits.
 23. What may be useful, if feasible, could be a technical tool used to assess whether email addresses include an individual's name or appear to be generic. Alone, this would not be sufficient; email addresses may relate to an identifiable individual (i.e. be personal data) despite not using their name. Such a tool should therefore only be considered as part of a basket of measures. As for telephone numbers: if these will be collected, a technical tool might check for typical prefixes associated with cellphones (which are typically linked to a single individual, perhaps more often than fixed-line numbers).
 24. Such features would need careful testing, since the rate of false positives and false negatives may be significant, especially given the very international nature of the domain name system overseen by ICANN (even in English, we assume email addresses of the form "@johndeere.com" or "@annsummers.com" could present challenges).
 25. Rather than act automatically on the findings of such tools, perhaps some Contracted Parties would be prepared to "manually" assess suspect data – though this would likely involve substantial effort on behalf of Contracted Parties. It seems more likely that such a tool would instead present a prompt to the Registrant ("*it looks like you may have provided an individual's contact details, (...)*"), asking them whether they want to dismiss or act upon that prompt.
 26. In essence, therefore, such tools may be better if deployed act as an additional (smart, content-aware) "nudge" for Registrants, not as an automated determinant of whether data publication can proceed.
 27. Given the unclear viability and merits of such an approach, it could for instance be something kept as a more medium/long-term item for exploration and testing; its full development and deployment could be made conditional on showing not only that it is technically viable, but also that experience is showing that additional measures are in fact necessary.

28. Ultimately, therefore, we cannot presently foresee other measures being required or expected of Contracted Parties, besides those already being discussed in the question posed.
29. Differences of opinion on this point are possible. Also, much could turn on *how* the suggested measures, including those proposed in the question posed, are implemented. For instance, there is some precedent in Hungary that when the accuracy of data is disputed, the data's processing (e.g. publication) may need to be temporarily halted, except to the extent necessary to verify and act on the reported inaccuracy⁸⁸ – seemingly whether or not the data subject has explicitly invoked GDPR Article 18(1) (right to request the restriction of data while inaccuracies are verified). While the design suggested here does not seem to require or lend itself to such a temporary suspension (since data subjects would be able to instantaneously self-rectify a self-characterization that they consider inaccurate – i.e. reporting and rectification should normally be simultaneous), we recommend keeping this in mind if plans evolve and ultimately lead to a possibility of a lag between reporting and rectification of inaccurate data.
30. We explained in the Accuracy Follow-Up Memorandum, at paragraph 21, that *“ICANN and/or the contracted parties will be best placed to evaluate whether the procedures currently in place are sufficient or if it would be reasonable to take additional measures to comply with the Accuracy Principle – and if so, to assess which measures would be more appropriate.”* That same memorandum advised at paragraph 24 that *“[t]he use of statistics and the monitoring of the number of correction requests from data subjects are also measures that could contribute to ensuring an adequate level of accuracy. For example, monitoring trends in rectification requests could allow to identify an accuracy gap or where a measure may not be entirely effective and take steps to cover the gap or replace the measure with a more appropriate one”*.

* * *

⁸⁸ Decision of the NAIH in Case Number NAIH/2019/363/2; available online at https://www.naih.hu/files/NAIH-2019_363_hatarozat.pdf ; a machine translation of the relevant passage is as follows: *“The Authority agrees with the [defendant] that there is no obligation for the controller to erase data in a case where the accuracy of data previously provided by the customer is called into question by a third party and it is not demonstrated that the data is no longer at the disposal of the customer but at the disposal of the notifier. However, the measures taken by the controller on the basis of the notification should promote the principle of accuracy and prevent the use of inaccurate data. In such a case, the Authority considers that the controller should temporarily limit the processing of inaccurate data by taking reasonable steps.”*

Response to Question 3 (Legal v. Natural)**MEMORANDUM**

To: Internet Corporation for Assigned Names and Numbers, EPDP Team
From: Ruth Boardman & Phil Bradley-Schmieg
Date: 27 April 2021
Subject: March 2021 question re. EU and third-party recognition of registration data publication interests

Background

31. The EDPB, in a July 2018 letter to Göran Marby (the “EDPB July 2018 Letter”),⁸⁹ stated 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”.
32. This has prompted several GDPR-related questions, most recently in our memorandum dated 6 April 2021 (the “**VSC and Consent Options Memorandum**”), which discussed two questions (“**Question 1 and Question 2**”) discussing different approaches (and resulting risks) in respect of (i) consent-conditional publication of registration data; and (ii) publication of registration data if it relates (only) to a legal person (e.g. a company), rather than being personal data (and how this can be verified) – i.e. Verified Self-Characterisation, “VSC”.
33. You have also asked, in the question presented below, whether certain provisions in EU legislation, and/or the practices of two third parties (EURid, and the RIPE-NCC), create helpful precedent in this area. This memorandum addresses that third question.

Question presented: Commission Regulation (EC) No 874/2004 of 28 April 2004 laying down public policy rules concerning the implementation and functions of the .eu Top Level Domain and the principles governing registration (‘.eu Regulation’) sets out the public policy rules concerning the implementation and functions of the .eu Top Level Domain (TLD) and public policy principles on registration of domain names in the .eu TLD.

Article 16 of the .eu Regulation is entitled ‘Whois database’ and provides:

⁸⁹ EDPB Letter to Göran Marby dated 5 July 2018; available online at https://edpb.europa.eu/sites/default/files/files/news/icann_letter_en.pdf

‘The purpose of the WHOIS database shall be to provide reasonably accurate and up to date information about the technical and administrative points of contact administering the domain names under the .eu TLD.

The WHOIS database shall contain information about the holder of a domain name that is relevant and not excessive in relation to the purpose of the database. In as far as the information is not strictly necessary in relation to the purpose of the database, and if the domain name holder is a natural person, the information that is to be made publicly available shall be subject to the unambiguous consent of the domain name holder. The deliberate submission of inaccurate information, shall constitute grounds for considering the domain name registration to have been in breach of the terms of registration.’

As from 13 October 2022, the .eu Regulation will be repealed by Regulation 2019/517, which provides under Article 12, entitled WHOIS database:

‘1. The Registry shall set up and manage, with due diligence, a WHOIS database facility for the purpose of ensuring the security, stability and resilience of the .eu TLD by providing accurate and up-to-date registration information about the domain names under the .eu TLD.

2. The WHOIS database shall contain relevant information about the points of contact administering the domain names under the .eu TLD and the holders of the domain names. The information on the WHOIS database shall not be excessive in relation to the purpose of the database. The Registry shall comply with Regulation (EU) 2016/679 of the European Parliament and of the Council.’

The Whois database is currently administered by EURid, a non-profit designated by the European Commission to manage the .eu registry. In its Whois database, EURid publishes the email addresses of domain name registrants in the .eu TLD (both natural persons and legal entities). EURid distinguishes between natural persons and legal entities by publishing the postal address information of legal entities, whereas this information is not published for natural persons.

Through Article 16 of the .eu Regulation, EURid is able to rely on GDPR Article 6(1)(e), which provides a legal basis for processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. While we understand that this Article 16 public interest basis is not available outside the .eu domain, the existence of this lawful basis for EURid’s processing could be interpreted to suggest that the EU legislature recognized that disclosure of the Registrant data serves a legitimate interest in stability, security, and resilience. Further, in carrying out its mandate under Article 16, EURid has determined that publication of the Registrant’s email “is not excessive in relation to the purpose of the database.”

Similarly, while RIPE-NCC relies on consent to publish personal information about tech/admin contacts, it publishes personal information about resource holders on the grounds that “facilitating coordination between network operators is the one purpose that justifies the publication of personal data in the RIPE-NCC database and that it is clear that the processing of the personal data referring to a resource holder is necessary for the performance of the registry function, which is carried out in the legitimate interest of the RIPE community and the smooth operation of the Internet globally (and is therefore in accordance with article 6.1.f of the GDPR).”

We understand that the public interest basis supplied by Article 16 is not available to Contracted Parties outside of the .eu top level domain. Based on your experience and applicable precedent to what extent if any do:(i) the existence of Article 16 of the EU Regulation; (ii) EURid’s decision to publish Registrant email addresses consistent with Article 16, (iii) RIPE-NCC’s decision to publish the email addresses of resource holders; and (iv) draft language regarding access to registration data in the recently proposed NIS2 Directive create precedent that would reduce Contracted Party risk in connection with publication of a legal person Registrant’s email address, even if it contained personal information? Do these facts affect your answers to Questions [1-2]? If it does not affect your answers, please explain why.

34. We believe that overall, the cited documents do not affect our answers to Questions 1 and 2 in the VSC and Consent Options Memorandum. More specifically, we believe the cited documents have limited impact on Contracted Party risk in connection with publication of a legal person Registrant’s email address, even if it contained personal data. Our view is based on the reasons set out below.

Regulation (EU) 2019/517, replacing Commission Regulation (EC) No 874/2004 (the “New .EU Regulation”)

35. When Regulation (EU) 2019/517 (the “New .EU Regulation”) replaces Commission Regulation (EC) No 874/2004 (the “Old .EU Regulation”), it will delete a provision of the Old .EU Regulation that allowed for the “not strictly necessary” publication of personal data in Registration Data (if the data subject expressly consented to this). The relevant provisions are quoted in the question presented.
36. The New .EU Regulation does not expressly say that a consent-driven approach has proven to be impractical or non-compliant; it simply offers no comment on such an approach. In fact, the New .EU Regulation now does not make any comment specifically about the publication of personal data, whether “strictly necessary” or otherwise. It limits itself to requiring that the data processing complies with the GDPR (if applicable), without saying how. In particular, Recital 22 of Regulation (EU) 2019/517 specifically requires the .eu Registry to choose an implementation of the WHOIS database and related systems that complies with “personal data protection by design and data protection by default”, “necessity” and “proportionality”.
37. The most direct reference to distribution of the registration data, if it is personal data, can be found in Recital 21. This speaks only about data sharing with/access

by law enforcement agencies, acting pursuant to “[EU] or national law” – not the public at large, nor interested parties such as IP rightsholders.⁹⁰

“21. The Registry should support law enforcement agencies in the fight against crime, by implementing technical and organisational measures aimed at enabling competent authorities to have access to the data in the Registry for purposes of the prevention, detection, investigation and prosecution of crimes, as provided for by Union or national law.”

38. In essence, the New .EU Regulation strikes a mostly neutral and inconclusive position here. It generally defers to GDPR requirements, and *specifically* calls out a need to respect proportionality and privacy by default. The fact that it discusses legitimate access by *specific* stakeholder groups, does not necessarily exclude a system in which some personal data is made public, e.g. with a data subject’s consent. Nevertheless, the New .EU Regulation has dropped wording (found in its predecessor) that explicitly accepted an approach founded (in part) on consent; it is possible that a supervisory authority or court might seek to draw an adverse inference from this.

EURid’s reliance on the GDPR “public task” legal basis

39. The question posed suggests that EURid relies on Article 16 of the Old .EU Regulation to assert that its (partial) publication of registrants’ personal data is permitted by GDPR Article 6(1)(e).
40. GDPR Article 6(1)(e) permits processing that is necessary for the performance of a task carried out either in the public interest or in the exercise of official authority vested in the controller. These must be laid down in EU or EU Member State law.
41. If the question’s suggestion is correct,⁹¹ then EURid is implicitly asserting that such publication is “strictly necessary in relation to the purpose of the database”. If that were not the case, then EURid would be operating in breach of Article 16 of the Old .EU Regulation, since this states that “In as far as the information is not strictly necessary in relation to the purpose of the database, and if the domain name holder is a natural person, the information that is to be made publicly available shall be subject to the unambiguous consent of the domain name holder.” Based on the question posed, we understand that EURid does not obtain such consent.

⁹⁰ Other references to wider interests do not discuss sharing Registrant data with them. For example, Recital 20 says “[t]he Registry should adopt clear policies aiming to ensure the timely identification of abusive registrations of domain names and, where necessary, should cooperate with competent authorities and other public bodies relevant to cybersecurity and information security which are specifically involved in the fight against such registrations, such as national computer emergency response teams (CERTs).” “Cooperation” could entail sharing of personal data, but (perhaps deliberately), the new .EU Regulation is silent on this point.

⁹¹ We have not been able to confirm this; the current [EURid privacy notice](#) does not specifically state what GDPR legal basis justifies the publication of registration data, though it does state that “We are required to maintain a complete and accurate database of all registered Domain Names. The purpose of the WHOIS look-up facility (<https://whois.eurid.eu/en/>) is to provide accurate and up-to-date information about the technical and administrative contact persons administering the Domain Names. This helps us in creating and maintaining a trusted and safe Internet environment.” The reference to publications being “required” seems consistent with either GDPR Article 6(1)(e) (public task) or Article 6(1)(c) (legal obligation).

42. On the one hand, this presumed position indicates that at least one Registry (EURid) upholds the importance (“strict necessity”) of publishing (some) data in WHOIS, even if it is personal data, and without consent or measures such as VSC (provided, at least, that some of the personal data is redacted, as per EURid’s policy on the matter).⁹²
43. However, the view held by EURid is not necessarily reflective of the views of the courts or supervisory authorities that enforce the GDPR – and is not binding on them. It is the view of one Registry, among others. The fact that this particular Registry’s policies are also subject to European Commission supervision⁹³ is of similarly limited precedential value; even if – hypothetically – this is a question that has been discussed between EURid and the European Commission, the latter does not enforce the GDPR, nor speak for those who do.
44. The question presented further states that “EURid distinguishes between natural persons and legal entities by publishing the postal address information of legal entities, whereas this information is not published for natural persons”. EURid’s current [Registration Policy \(v.11\)](#) explains that “Where no undertaking or organisation name is specified, the individual requesting registration of the Domain Name will be considered the Registrant; if the name of the undertaking or organisation is specified, then the undertaking or organisation is considered the Registrant”.
45. This may mean that an assumption is made that postal details provided by an organisation (a legal person registrant) *do not* contain personal data; or simply that if it does so, this is strictly necessary and/or lower risk for individuals. EURid – as the controller of much of the data in question – will be better placed than we are to determine whether that assumption holds true in practice.
46. Even if that assumption hypothetically holds true for EURid and the postal addresses it publishes as part of legal persons’ .eu registration data, we note that in light of the EDPB’s comments to ICANN,⁹⁴ it may be inadvisable to extrapolate from this to other contact information (e.g. email addresses, which might refer specifically to one readily-identifiable individual within the organisation).

⁹² We note with interest that the question posed asserts that EURid invokes GDPR Article 6(1)(e) – task in the public interest / public authority – *not* GDPR Article 6(1)(f), legitimate interests. EURid is not a public authority, so it is in principle capable of invoking legitimate interests for its publication of personal data. We are not privy to EURid’s reasoning for avoiding the “legitimate interests” basis, and therefore cannot offer substantial comment on this observation; that said, it might not be helpful/reassuring for other Contracted Parties; unlike EURid, most Contracted Parties cannot rely on GDPR Article 6(1)(e) because, unlike EURid, there is no EU or Member State law underpinning their own WHOIS-related processing.

⁹³ E.g. Recital 11 of the New .EU Regulation states: “The Commission should enter into a contract with the designated Registry, which should include the detailed principles and procedures that apply to the Registry for the organisation, administration and management of the .eu TLD.”

⁹⁴ “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, such as natural persons who manage administrative or technical issues on behalf of the registrant. For example, the publication of the personal email address of a technical contact person consisting of `firstname.lastname@company.com` can reveal information regarding their current employer as well as their role within the organization. Together with the address of the registrant, it may also reveal information about his or her place of work.” EDPB July 2018 Letter, at page 5.

47. Based on those observations, plus an appreciation that EURid operates within a somewhat unique legislative framework giving it the option to rely on something other than consent or legitimate interests – unlike other Contracted Parties – it is therefore difficult to draw any general conclusions from EURid’s approach.

The RIPE-NCC’s decision to publish the email addresses of resource holders

48. The question posed quotes from a blog post from 2018 authored by the RIPE-NCC’s Head of Legal, entitled “[How We’re Implementing the GDPR: Legal Grounds for Lawful Personal Data Processing and the RIPE Database](#)”.
49. In that blog post, as the question posed correctly states, the RIPE-NCC states that it relies on legitimate interests (the GDPR Art. 6(1)(f) legal basis) for publishing personal data – primarily contact details – to assist with the proper functioning of an important Internet system.
50. It should be noted, however, that the blog post also states:
- “However, when the resource holder appoints another individual to perform this role [i.e., as a contact point], they must obtain the consent of the person(s) whose personal data will be inserted in the RIPE Database before their data is inserted (in accordance with Article 6.1.a of the GDPR).”
51. In other words, it appears to us that when the resource-holder itself is a legal person, (i) the RIPE-NCC views legitimate interests as an appropriate legal basis in first party settings (i.e. when the person completing/updating a registration provides their own contact details, and are therefore the relevant data subject), but (ii) the RIPE-NCC had (at least, in 2018) instead preferred to do this only with a data subject’s consent in third party settings (e.g. when the contact details are those of a colleague of the person completing/updating the registration).
52. This distinction might be due to fears that it would be harder to assert that the third party’s own interests are sufficiently aligned with those of the resource-holder and/or the RIPE-NCC (and related stakeholders); and/or fears that there are greater risks for third party data subjects (for instance because it is more difficult to provide a GDPR privacy notice to them, so they may be less aware of their rights). Such concerns may therefore have driven the RIPE-NCC to instead prefer to rely on consent for those “third party” situations.
53. While the RIPE-NCC must seek its own legal advice on the matter, our view so far as the ICANN-EPDP is concerned is that such a distinction may not be legally required. GDPR Article 6(1)(f) (the legitimate interests basis) does not require the data subject’s interests to be aligned with those of the controllers(s) – merely, there must be an appropriate *balance* between the interests at stake (those of the controller and/or of third parties), versus the “fundamental rights and freedoms of the data subject which require protection of personal data”. In this case, the RIPE-NCC and its own legal advisors will have the best insight into the various interests and risks, however it appears to us that:
- 53.1 *The interests of the controller and wider stakeholders* would seem to be broadly the same whether dealing with a first party or third party’s contact

- details: e.g. either set of contact details are presumably important for the proper investigation and resolution of disruptions to a key Internet system;
- 53.2 On the risks side, first party or third party contact details could equally be abused, e.g. for unsolicited marketing; there may be other types of risk, but once again, those seem likely to be similar whether for first party or third party data subjects;
- 53.3 As for the notice issue, the GDPR specifically accepts that there will be situations where data is not collected directly from a data subject, and notice might therefore not be provided to them (see, in particular, GDPR Article 14(5)). This therefore is not an automatic reason to dismiss the potential use of legitimate interests in third party settings; and
- 53.4 It may be for this reason that the EDPB's letter to ICANN, in July 2018, endorsed potential reliance on legitimate interests even for third-party data, provided that registrants are not *compelled* to provide such third party data, but can instead provide their own.⁹⁵ We understand that this is indeed the case for the system overseen by the RIPE-NCC.
54. The RIPE-NCC likely feels that regulators and courts would at first glance welcome the autonomy and control offered by reliance on consent, rather than a non-consensual GDPR legal basis like legitimate interests. However, those authorities might also recognise the practical downsides of such an approach:
- 54.1 The RIPE-NCC's own blog post acknowledges the doubts that sometimes surround consents obtained in employment contexts (i.e., that such consents, if requested by an employer, may not have been freely given by an employee).
- 54.2 The RIPE-NCC also ends up relying on the first party's representations that they have obtained a valid consent from the third party ("[The RIPE NCC considers that it is the responsibility of the one who inserts the data in the RIPE Database \(i.e. the maintainer\) to ensure that they have obtained valid consent for the processing to take place.](#)"). This could make it difficult, in theory, for the RIPE-NCC (as controller) to demonstrate that those consents met all GDPR requirements.
- 54.3 Contracted Parties could face the same GDPR issues in respect of domain name registration data.
55. The views of the RIPE-NCC are, like those of EURid, not necessarily reflective of – and certainly not binding on – authorities tasked with GDPR enforcement.
56. Moreover, the legitimate interests balancing exercise to be conducted by the RIPE-NCC is different to that of ICANN and Contracted Parties; the data in question relates to different resources (IPv4, IPv6 and AS Number resources, often allocated

⁹⁵ EDPB July 2018 Letter, at pages 2-3.

by the RIPE-NCC – in blocks – to very large organisations; versus specific domain names sometimes being registered by specific individuals for private use).

57. It is therefore difficult to draw any general conclusions from the RIPE-NCC's approach.

Draft language regarding access to registration data in the recently proposed NIS2 Directive

58. In December 2020, the European Commission published its draft for a [revised Directive on measures for a high common level of cybersecurity across the Union \("NIS2"\)](#).

59. The Recitals of the proposed NIS2 Directive state that:

"15. Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers.

(...)

(59) Maintaining accurate and complete databases of domain names and registration data (so called 'WHOIS data') and providing lawful access to such data is essential to ensure the security, stability and resilience of the DNS, which in turn contributes to a high common level of cybersecurity within the Union. Where processing includes personal data such processing shall comply with Union data protection law.

(60) The availability and timely accessibility of these data to public authorities, including competent authorities under Union or national law for the prevention, investigation or prosecution of criminal offences, CERTs, (CSIRTs, and as regards the data of their clients to providers of electronic communications networks and services and providers of cybersecurity technologies and services acting on behalf of those clients, is essential to prevent and combat Domain Name System abuse, in particular to prevent, detect and respond to cybersecurity incidents. Such access should comply with Union data protection law insofar as it is related to personal data.

(61) In order to ensure the availability of accurate and complete domain name registration data, TLD registries and the entities providing domain name registration services for the TLD (so-called registrars) should collect and guarantee the integrity and availability of domain names registration data. In particular, TLD registries and the entities providing domain name registration services for the TLD should establish policies and procedures to collect and maintain accurate and complete registration data, as well as to prevent and correct inaccurate registration data in accordance with Union data protection rules.

(62) TLD registries and the entities providing domain name registration services for them should make publically (sic) available domain name registration data that fall outside the scope of Union data protection rules, such as data that concern legal persons. TLD registries and the entities providing domain name registration services for the TLD should also enable lawful access to specific domain name registration data concerning natural persons to legitimate access seekers, in accordance with Union data protection law. Member States should ensure that TLD registries and the entities providing domain name registration services for them should respond without undue delay to requests from legitimate access seekers for the disclosure of domain name registration data. TLD registries and the entities providing domain name registration services for them should establish policies and procedures for the publication and disclosure of registration data, including service level agreements to deal with requests for access from legitimate access seekers. The access procedure may also include the use of an interface, portal or other technical tool to provide an efficient system for requesting and accessing registration data. With a view to promoting harmonised practices across the internal market, the Commission may adopt guidelines on such procedures without prejudice to the competences of the European Data Protection Board.

(...)

69. The processing of personal data, to the extent strictly necessary and proportionate for the purposes of ensuring network and information security by entities, public authorities, CERTs, CSIRTs, and providers of security technologies and services should constitute a legitimate interest of the data controller concerned, as referred to in Regulation (EU) 2016/679. That should include measures related to the prevention, detection, analysis and response to incidents, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure, as well as the voluntary exchange of information on those incidents, as well as cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Such measures may require the processing of the following types of personal data: IP addresses, uniform resources locators (URLs), domain names, and email addresses.”

60. Recitals 59-62 inclusive are then broadly mirrored in Article 23 of the draft NIS2 Directive.
61. Recitals 15, 59-61 inclusive, and 69, and Articles 23(1-3) of the draft NIS2 Directive, are broadly supportive of complete, fulsome registration data processing, provided it is GDPR-compliant. The final sentence of Recital 61 also expressly supports measures designed to promote compliance with the GDPR’s accuracy principle, such as those mentioned in our previous memoranda.
62. However, Recital 62, and Articles 23(4-5), are more specifically relevant to the matters under discussion in this memorandum, as they concern the publication/dissemination of registration data, not just its mere collection and retention. Those provisions of the NIS2 Directive draw a clear distinction between personal and non-personal data, and only expressly support the publication of non-personal data. In respect of personal data, the NIS2 Directive limits itself to

discussing what appears to be *restricted* access by “legitimate access seekers, in accordance with Union data protection law” (and equivalent wording in Article 23(5)).

63. In our view, therefore, the current draft NIS2 Directive does not appear to consider a system in which some personal data may (legitimately) be openly published, e.g. with a Registrant’s consent. It is not clear whether this just because that option was not considered by the drafters, *or* because the drafters did not consider such an approach to be worthwhile and/or compliant. However, it means that the current draft NIS2 Directive does not offer significant support/risk-reduction for a system premised on, for example, Registrant consent (though nor does it expressly undermine such an approach).

* * *

Response to Question 4 (regarding options for contact address masking)**MEMORANDUM**

To: Internet Corporation for Assigned Names and Numbers, EPDP Team
From: Ruth Boardman & Phil Bradley-Schmieg
Date: 9 April 2021
Subject: March 2021 question regarding options for contact address masking

Background

64. The European Data Protection Board (“EDPB”), in [a July 2018 letter to Göran Marby](#), stated 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”.

65. Against this background and building on previous advice you have received in this matter, you have raised the following question.

Question presented: B&B’s [Memo dated 4 February 2020 regarding email contact information](#) discussed two options: (a) a “pseudonymous email contact” where the same unique string is used for multiple registrations by the data subject; and (b) an “anonymous email contact” where a separate unique email string is used for each such registration. B&B opined that publication of either (a) or (b) would be treated as publication of personal data on the web because the purpose of making this masked email address available is to allow 3rd parties to directly contact the data subject and because third parties with legitimate and proportionate interests would have access to the underlying data.

Upon review, the EPDP Legal Team has proposed to describe options (a) and (b) going forward as follows:

- The phrase “pseudonymous email contact” (option (a)) should be replaced with the phrase “**Registrant-based email contact**,” defined as: “an email for all domains registered by a unique registrant, *which is intended to be pseudonymous data when processed by third party users* (i.e., non-contracted parties). (The question of whether the email should be common across ICANN-accredited Registrars requires a policy determination TBD.)
- The phrase “anonymous email contact” (option (b)) should be replaced with the phrase “**Registration-based email contact**,” defined as “a separate single use

email for each domain name registered by a unique registrant, *which is intended to be virtually or “essentially” anonymous data when processed by third party users* (i.e., non-contracted parties).”

In answering the questions below, please assume, for discussion purposes, that third-party users of Registration-based email contact information cannot identify the data subject without disproportionate effort so that the risk of identification appears in reality to be insignificant.

1. Based on your experience and applicable precedent, please compare the level of risk, likelihood of enforcement actions, fines, counseling, etc. associated with (a) publication on the web or (b) automated disclosure of (i) a Registrant-based email contact on the one hand and (ii) a Registration-based email contact on the other? In responding to this question please consider:
 - a. Whether the assumed fact that the risk of data subject identification by a third party (i.e., non-contracted party) through a Registration-based email contact appears to be insignificant would render such emails effectively “anonymous” with respect to such third parties under the *Breyer* standard?
 - b. If not, how would the choice of email contact (Registrant-based or Registration-based) affect the outcome of the legitimate interests balancing test under Article 6(1)(f)? To what extent would the use of a Registration-based email contact reduce the impact of publication on the interests or fundamental rights and freedoms of the data subject?

Does the answer to these questions change if the primary purpose for publishing a masked email is to support statistical research and analytics, and not to communicate with the data subject?

Analysis

66. Our answer starts by addressing your sub-question, “*Whether the assumed fact that the risk of data subject identification by a third party (i.e., non-contracted party) through a Registration-based email contact appears to be insignificant would render such emails effectively “anonymous” with respect to such third parties under the Breyer standard?*”, to explain why we consider that the GDPR would remain applicable in a Registration-based email contact scenario. We then turn to the wider GDPR compliance aspects of your question.

Anonymity

67. We maintain our view, expressed in our Memorandum dated 4th February 2020, that with either option (Registrant-based or Registration-based email contact), there remains a high likelihood that the publication or automated disclosure of such email addresses would be considered to be the processing of personal data.

68. For the GDPR to apply to the processing of electronic data (assuming the GDPR's territoriality test is met, and its subject matter carve-outs are not applicable), a two-part test applies:
- 68.1 First, there must be processing of information that relates to a particular individual, having regard to the data (and its processing's) "content, purpose, or effect". This is the "*Nowak*"⁹⁶ / "relates to" test.
- 68.2 Second, that particular individual must be "identified or identifiable", which means that there must exist "means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."⁹⁷ "Identification" does not necessarily mean finding the real name of a person; rather, it has a more general meaning, generally revolving around the ability to specifically "single out" someone for different treatment (singling out),⁹⁸ and/or having the ability to collect/connect more data about them (inference and/or linking).⁹⁹ A technical identifier – even one that was randomly generated – can be sufficient for such purposes, particularly if it is linked with other information about the person that makes it easier to distinguish them from someone else.¹⁰⁰ There are no "reasonably likely means" of reidentification if such activity is "prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and manpower, so that the risk of identification appears in reality to be insignificant"¹⁰¹. This is the "*Breyer*" / "identifiability" test.
69. Our view, expressed above, is that the processing of these email aliases would still likely be seen as meeting both tests, to the extent that the purpose of the processing is to provide a means of contacting data subjects.

Nowak test

70. Regarding the *Nowak* test: when a contact is a natural person, such addresses will be masked aliases for a real email address used by that person. In light of this:
- 70.1 Where the purpose / intended effect of the processing of that data is to enable correspondence with the recipient (i.e., often, with a specific data subject),

⁹⁶ Judgement of the CJEU in Case C-434/16 *Nowak*, ECLI:EU:C:2017:994, at paragraph 35.

⁹⁷ GDPR Recital 26

⁹⁸ As quoted above, GDPR Recital 26 specifically refers to "singling out" when discussing means that are reasonably likely to be used to identify the data subject.

⁹⁹ Singling out, linkability and inference are three parts of the anonymisation test proposed by the Article 29 Working Party, in its Opinion 05/2014 on Anonymisation Techniques ("WP 216"), available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

¹⁰⁰ On this point, see GDPR Recital 30 ("Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.")

¹⁰¹ Judgement of the CJEU in Case C-582/14 *Breyer*, ECLI:EU:C:2016:779, at paragraphs 45 and 46.

then having regard to the EU Court of Justice (“CJEU”)’s test in *Nowak*, that “purpose” and/or “effect” means there is a link to a *particular* individual.¹⁰²

- 70.2 By contrast, purely statistical processing aimed at creating *aggregate* metrics (describing relatively large cohorts) – e.g. counting how many such contact aliases have been created – may arguably *not* be subject to the GDPR. This is because the *content* of a randomly-generated contact alias does not specifically link to a specific individual, at least in a Registration-based email contact scenario; and – again, arguably – neither the *purpose* nor the *effect* of creating aggregate results of statistical research carries a link to a *particular* individual; rather, aggregate statistics describe and differentiate between *cohorts/groups* (e.g. by nation, Registry, Registrar, etc.). The *Nowak* test may arguably not be satisfied in respect of that class of processing (but note that this is to be distinguished from statistics aimed at generating new information about, or classification of, any specific data subject – e.g. counting how many domain names are associated with a given Registrant-based email contact).
- 70.3 However, in practice we do not think it would be reasonably possible to say that the sole purpose of creating and publishing the contact aliases is for the aggregate statistical processing just described. If this were the case, there would be no need to provide an email address at all. The fact that an email address is provided suggests that a significant purpose for the creation and publication of contact aliases will always be to provide a means of contacting specific persons. Accordingly, while *some* processing (for aggregate statistics) may fall outside the GDPR’s scope based on the *Nowak* test, the GDPR seems likely to remain a compliance concern at the very least in respect of the *other* purpose of processing.
- 70.4 We should also caution against over-reliance on *Nowak*-based arguments. Despite the ruling echoing early Article 29 Working Party guidance,¹⁰³ we are not aware of the *Nowak* test being systematically applied in the analyses and guidance of courts and supervisory authorities applying the GDPR. For example, as of early April 2021, a search of the Belgian Data Protection Authority’s website, across all available languages, turns up (i) just two directly references to the *Nowak* case, and only on unrelated points; and (ii) apparently no citations of the key “content, purpose or effect” phrase from *Nowak*. That authority’s explanation (in its Lexicon) of the term “personal data” concentrates exclusively on the *Breyer* test – i.e. identifiability of a data subject.¹⁰⁴ Other authorities may take a different view (e.g. the UK authority does discuss the “content, purpose or effect” test, and summarises its impact as follows: “Information must ‘relate to’ the identifiable individual to be personal data. This means that it does more than simply identifying them – it must concern the individual in some way. (...) Data can reference an

¹⁰² In some cases, a recipient contact address might be a shared mailbox (e.g. enquiries@example.com), in which case the masked contact address is arguably *not* personal data, whether by application of the *Nowak* or *Breyer* tests.

¹⁰³ WP 136, at page 10.

¹⁰⁴ <https://www.autoriteprotectiondonnees.be/citoyen/vie-privee/lexique>

identifiable individual and not be personal data about that individual, as the information does not relate to them.”)¹⁰⁵

- 70.5 Moreover, not only do authorities in this field not always place substantial emphasis on *Nowak*, but *if* they were to do so, they could also take quite differing approaches to its interpretation. Differences of opinion might in particular surround the “content” limb of the “content, purpose or effect” test. Article 29 Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136)¹⁰⁶ explained that “[t]he “content” element is present in those cases where - corresponding to the most obvious and common understanding in a society of the word “relate” - information is given about a particular person, regardless of any purpose on the side of the data controller or of a third party, or the impact of that information on the data subject.” If that explanation is correct, then a court or regulator might conclude that publishing an email address (even a randomly generated one) for a contact associated with a domain registration is *inherently* publishing information “about” that person – because it tells us how to contact that person. This is a problematic view, however, as it “borrows” reasoning from the *purpose* and *effect* tests (it looks at a possible purpose for the information, *not* at the content of the information itself), *and* bases itself on a *hypothetical* purpose/effect, not the *actual* purpose/effect of processing – thus completely short-circuiting two thirds of the “content, purpose or effect” test. From both a logical and rule of law (clarity/certainty) perspective, this is problematic. From a simpler point of view, something randomly generated (as876bnk@example.com) is a pure expression of random “noise” -- an instantaneous snapshot of the electrical state of a computer’s “random number generator” circuitry. It thus does not and cannot of itself “contain” any information about any person. If it *did* in and of itself convey information about a person, it logically would not be random. From that view, a randomly-generated address thus does not pass the “content” test; instead, the focus would need to be on the data processing’s purpose and/or effect.
- 70.6 Clearly, then, there is a significant risk of disagreement with at least some authorities if arguments rest on the *Nowak* case.

Breyer test

71. Regarding the *Breyer* test: in that case, the CJEU constructed a thought experiment: if there was a cyber attack, a controller holding an IP address (and, we presume – though the court is not explicit on this point – a timestamp indicating when that IP address was in use by a device/person of interest), could communicate that information to the police/judicial authorities. The CJEU expected that the authorities would then often be empowered to then demand corresponding information from the internet access provider that assigned that IP address, and thereby bring a prosecution (although the CJEU asked the referring

¹⁰⁵ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-the-meaning-of-relates-to/#pd5>

¹⁰⁶ Article 29 Working Party, *Opinion 4/2007 on the concept of personal data* (WP 136), at p. 10. Available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

national courts to verify that assumption). The CJEU thus held that unless this scenario was prohibited by law or practically impossible, there were “reasonably likely means” of identifying a data subject.

- 72. The key point here is that although a third party may just know a Registrant-based or Registration-based email contact, competent authorities could correlate this to non-public registration data held by Contracted Parties, allowing for reidentification. So far as we are aware, this would not always require “practically impossible” levels of effort, nor would it be universally prohibited by law.
- 73. Thus even from the perspective of *third parties*, the distribution and use of such contact aliases could be treated as personal data processing.
- 74. From the perspective of a *Contracted Party* that knows which contact alias it has assigned to a Registrant / Registrant’s nominated contact, the creation and hosting of such addresses, and their making available for use by others, is almost certainly personal data processing (when the contact persons are natural persons).

Risk of the respective options presented

- 75. Having explained our view that for either option, the GDPR remains relevant, we turn now to your request that we compare risks associated with (a) publication on the web or (b) automated disclosure of (i) a Registrant-based email contact on the one hand and (ii) a Registration-based email contact on the other.
- 76. Our summary (which reflects the important assumptions and caveats provided later in this answer) is as follows:

	Registrant-based email contact	Registration-based email contact
Web publication	Medium	Low
Automated disclosure	Low	Lowest

- 77. Based on an application of the GDPR’s principles, the sharing (whether through web publication or automated disclosure) of Registration-based email aliases carries lower risk compared to Registrant-based email aliases.
- 78. This is because someone holding a Registrant-based email address may be able to learn more information about the data subject – specifically, what other domain names that data subject is associated with. This is because unless a different *real* contact address was provided for that data subject for each domain they register, then each registration would carry the same email alias.
- 79. Web publication of such details could make it relatively easy to build such profiles and potentially even build a reverse lookup tool (“for a given Registration-based email contact, what domain names is this contact associated with?”).

80. Automated disclosure, alone, would presumably make this more difficult, since unless the automated disclosure tools *specifically* provide reverse lookup functionality,¹⁰⁷ requesters would presumably need to query potentially quite large numbers of domain names to gather enough information to be able to make matches and start to build an (incomplete) reverse lookup function. That said, requestors that have a pre-established list of specific domain names (e.g. suspected “mirrors” of a website hosting illegal contents) could determine whether the same email address was provided for some or all of those sites. Thus even in an automated disclosure scenario, the use of a Registrant-based email contact scheme carries added risks to privacy, relative to Registration-based email contact scheme.
81. Accordingly, having regard to the following considerations:
- 81.1 The need to comply with the GDPR’s data minimisation rule;
 - 81.2 The need to comply with a “privacy by design and by default” rule;
 - 81.3 That reliance on GDPR Article 6(1)(f) (the legitimate interests legal basis) is more robust when system design minimises prejudice to “[the interests or fundamental rights and freedoms of the data subject which require protection of personal data](#)”; and
 - 81.4 That in assessing whether and to what extent fines should be levelled against a controller, authorities must have regard *inter alia* to the “[gravity](#)” of an infringement, the “[scope](#)” of processing, the “[the level of damage suffered by](#)” data subjects, “[any action taken by the controller or processor to mitigate the damage suffered by data subjects](#)” and “[the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32](#)” (see GDPR Article 83),

we therefore consider that a Registration-based email contact scheme carries lower risk than a Registrant-based email contact scheme.

82. Having explained the balance of risk along the “Registration vs. Registrant-based scheme” axis, we turn now to contrasting risks for web-based publication versus automated disclosure.
83. A risk common to both a Registration-based and Registrant-based email contact schemes is spam or other unsolicited emails; this “addressability” is, arguably, one aspect of privacy.¹⁰⁸ Spam has been a longstanding concern for WHOIS systems; it was the subject of an ICANN Security and Stability Advisory Committee study in 2007, which concluded that “the appearance of email addresses in response to

¹⁰⁷ Such features, before being rolled out, would require careful consideration. For old guidance on the issue, see Article 29 Working Party Opinion 5/2000 on The Use of Public Directories for Reverse or Multi-criteria Searching Services (Reverse Directories) (“WP 33”), available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp33_en.pdf

¹⁰⁸ Recital 40 of Directive 2002/58/EC (the EU’s “ePrivacy Directive”) states: “Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages.”

- WHOIS queries is indeed a contributor to the receipt of spam, albeit just one of many”.¹⁰⁹
84. Accordingly, whether a Registrant- or Registration-based email contact system is employed, effective measures should be taken to address the availability of addresses to spammers (e.g. use of technical features to prevent “harvesting” of such addresses; and/or filtering out inappropriate communications before they are delivered to the intended recipient).
85. In comparison to web-based publication, we presume that automated disclosure allows further scope to evaluate the motives for a request, the sources of that request, and to monitor / audit and apply protective measure (e.g. rate limits) on such requests – i.e. greater scope to deploy the sorts of mitigations that will reduce liability based on the factors set out in paragraph 81 above. It would therefore appear that automated disclosure poses inherently less risk on this front, compared to web-based publication.
86. Those potential advantages of automated disclosure compared to web-based publication also conceivably present GDPR Article 25 (privacy by design and by default) advantages. Particularly, some thought would need to be given to ensuring that web-based publication is designed in such a way that it complies with GDPR Article 25(2), “such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons”.¹¹⁰
87. That said, if effective measures against spam are employed, and if a Registration—based approach is taken (due to its advantages discussed earlier), then given the resulting low utility of the data, it is difficult to see how its web-based publication would present meaningful risks to privacy or data security.

* * *

¹⁰⁹ SAC 023: *Is the WHOIS Service a Source for email Addresses for Spammers?* , Executive Summary. Available online at <https://www.icann.org/en/system/files/files/sac-023-en.pdf>

¹¹⁰ In its *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, v2.0*, at paragraph 56, the EDPB explains that this means that “[t]he controller shall by default limit accessibility and give the data subject the possibility to intervene before publishing or otherwise making available personal data about the data subject to an indefinite number of natural persons”. Available online at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf