ICANN | GNSO

Generic Names Supporting Organization

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

2 June 2021

Status of This Document

This is the Initial Recommendations Report of the GNSO Expedited Policy Development Process (EPDP) Team on the Temporary Specification for gTLD Registration Data Phase 2A that has been posted for public comment.

Preamble

The objective of this Initial Report is to document the EPDP Team's: (i) deliberations on charter questions, (ii) preliminary recommendations, and (iii) additional identified issues to consider before the Team issues its Final Report. The EPDP Team will produce its Final Report after its review of the public comments received in response to this report. The EPDP Team will submit its Final Report to the GNSO Council for its consideration.

Table of Contents

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.

The EPDP Team will not finalize its responses to these questions and recommendations to the GNSO Council until it has conducted a thorough review of the comments received during the public comment period on this Initial Report. At the time of publication of this Report, no formal consensus call has been taken on these responses and preliminary recommendations. This Initial Report did receive the support of the EPDP Team for publication for public comment, mainly as a tool to solicit community input on areas where there remains significant divergence (see chapter 3 for further details). Where applicable, the Initial Report indicates where positions within the Team differ.

Notwithstanding the above, for the purpose of obtaining community input, the EPDP Team is putting forward these preliminary recommendations as well as questions for community consideration (see chapter 3 for further information):

Legal vs. Natural

EPDP Team response to question 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")

Preliminary Rec #1.
No changes are recommended, at this stage, 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").

EPDP Team Question for Community Input #1
Is there new information or inputs that the Phase 2A team has not considered in assessing whether to make changes to the recommendation that Registrars and Registry Operators may, but are not obligated to, differentiate between legal and natural persons?

Preliminary Rec #2.
The EPDP Team recommends that the GNSO Council monitors developments in relation to the adoption and implementation of relevant legislative changes (for example, NIS2), relevant decisions by pertinent tribunals and data protection authorities, as well as the possible adoption of the SSAD to determine if/when a reconsideration of this question (whether changes are required to the EPDP Phase 1 recommendation "Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so") is warranted. The GNSO Council is

expected to consider not only input on this question and any new information from GNSO SG/Cs but also ICANN SO/ACs to help inform a decision on if/when this question is expected to be reconsidered.

EPDP Team Question for Community Input #2
Is this recommendation necessary for the GNSO council in considering future policy work in this area? If yes, in what ways does this monitoring assist the Council?

Preliminary Rec #3.
The following additions are made to the EPDP Phase 1 recommendations:

Recommendation #5

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

Data Elements (Collected & Generated*)	Collection Logic
Registrant Legal Person (Yes/No/Unspecified[1])	[MAY / MUST, IF Contracted Party chooses to differentiate*]

For the purpose of the Legal person and non-personal data field, which is optional for the Registrar to provide to the Registrant to self-designate, Registrars should advise the Registered Name Holder at the time of registration what the consequences are of self-designating as a legal or a natural person and to provide non-personal data only (or provide appropriate consent if personal data is involved), consistent with preliminary recommendation #3, point 4. Recommendation #7[2]

Transfer of Data Elements from Registrar to Registry:

[1] "Unspecified" means that no self-designation has been indicated by the Registered Name Holder or determined by the Contracted Party, that the status of self-designation is unknown, or that the status may be in the process of being confirmed. It does not imply that the information provided is inaccurate. The value of unspecified is the default until either the RNH or Contracted Party perform a procedure at the discretion of the Contracted Party, that would change the value to a YES or a NO.
[2] Do note that the implementation of this recommendation is still pending Board/GNSO Council resolution of the intent in relation to the Thick Whois Consensus Policy".

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

Recommendation #8

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

For Registrars:

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

For Registries:

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

Recommendation #10

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

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

**There are different views within the EPDP Team on whether this data element would need to be redacted in the public RDDS. Some members, for example, believe this data element should be redacted in public RDDS but provided via the SSAD. Other members believe this data element should be published in the public RDDS. As a result, the EPDP Team invites those

providing input during the public comment period to provide their view on this question and, in particular, the rationale for why this data element should be redacted or not and whether the choice to redact or not should be left to the Contracted Party.

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

For clarity, the existence of this standardized data element does not require a Contracted Party to differentiate between legal / natural person type or personal / non-personal data.[3] As part of the implementation, it should be considered whether for those Contracted Parties that choose not to differentiate, the data field is not visible in RDDS or automatically set to "unspecified".

EPDP Team Question for Community Input #3

1. Should a standardized data element be available for a Contracted Party to use? If yes, why? If no, why not? Why is harmonization of practices beneficial or problematic?
2. If yes, what field or fields should be used and what possible values should be included, if different from the ones identified above? Aspects of the recommendation that the EPDP Team is looking for specific input on having been marked above with *, indicating the options that are under consideration.
3. If such a standardized data element is available, MUST a Contracted Party who decides to differentiate use this standardized data element or should it remain optional for how a Contracted Party implements this differentiation?

EPDP Team response to question ii - What guidance, if any, can be provided to Registrars and/or Registries who differentiate between registrations of legal and natural persons.

Preliminary Rec #4.

The EPDP Team recommends that Contracted Parties who choose to differentiate based on person type SHOULD follow the guidance[4] 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).

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

[4] 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.

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,[5] 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 a standardized data element in the RDDS, SSAD or their own data sets that would indicate the type of person it concerns (natural or legal) and, if legal, also the type of data it concerns (personal or non-personal data). Such flagging would facilitate review of disclosure requests and automation requirements via SSAD and the return of non-personal data of legal persons by systems other than SSAD (such as Whois or RDAP). A flagging mechanism may also assist in indicating changes to the type of data in the registration data field(s).
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)[6] 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.[7] 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.

[5] 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.
[6] 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.
[7] See also https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

EPDP Team Question for Community Input #4

1. Does this guidance as written provide sufficient information and resources to Registrars and Registry Operators who wish to differentiate? If not, what is missing and why?
2. Are there additional elements that should be included?
3. Are there legal and regulatory considerations not yet considered in this Initial Report, that may inform Registries and Registrars in deciding whether and how to differentiate, and if so, how?
4. If a Registrar or Registry Operator decides to differentiate, should this guidance become a requirement that can be enforced if not followed ("MUST, if Contracted Party decides to differentiate")?

Feasibility of Unique Contacts

EPDP Team response to question i - Whether or not unique contacts to have a uniform anonymized email address is feasible, and if feasible, whether it should be a requirement.

The EPDP Team recognizes that it may be technically feasible to have a registrant-based email contact or a registration-based email contact.[8] Certain stakeholders see risks and other concerns[9] 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.[10]

EPDP Team response to question 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

Preliminary Rec #5.
The EPDP Team recommends that Contracted Parties who choose to publish a registrant- or registration-based email address in the publicly accessible RDDS should ensure appropriate safeguards for the data subject in line with relevant guidance on

[8] 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.
[9] 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.
[10] 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.

anonymization techniques provided by their data protection authorities and the appended legal guidance in this recommendation (see Annex E).

EPDP Team Question for Community Input #5
Does this guidance as written provide sufficient information and resources to Registrars and Registry Operators who wish to publish a registrant- or registration-based email address? If not, what is missing and why?

Following the publication of this Report, the EPDP Team will: (i) carefully review public comments received in response to this publication, (ii) continue to review the work-in-progress with the community groups the Team members represent, and (iii) continue 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.

1.2 Conclusions and Next Steps

This Initial Report will be posted for public comment for 45 days. After the EPDP Team's review of public comments received on this Report, the EPDP Team will update and finalize this Report as deemed necessary for submission to the GNSO Council.

1.3 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 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 E.

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;[11] (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 the EPDP Team's legal advisors, Bird & Bird.

[11] 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 & Preliminary Recommendations

The EPDP Team will not finalize its responses to the Council questions and recommendations to the GNSO Council once it has conducted a thorough review of the comments received during the public comment period on this Initial Report. At the time of publication of this Report, no formal consensus call has been taken on these responses and preliminary recommendations. This Initial Report did receive the support of the EPDP Team for publication for public comment, mainly as a tool to solicit community input on areas where there remains significant divergence which have been identified below.[12] Where applicable, differing positions have been reflected in the Report. Furthermore, specific questions that the EPDP Team is looking for input on have been called out in relation to each of the preliminary recommendations identified below. Commenters are encouraged to focus their input on these questions as well as to make specific proposals for what changes or additions the EPDP Team should consider as it finalizes its report.

3. 1 Legal vs Natural

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

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

In addressing these questions, the EPDP Team started with a review of all relevant information, including (1) the study undertaken by ICANN org,[13] (2) the legal guidance provided by Bird & Bird, and (3) the substantive input provided on this topic during the

[12] Following a review of public comments, the EPDP Team will take a formal consensus call before producing its Final Report.

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

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

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

public comment forum on the addendum. Following the review of this information, the EPDP Team identified a number of clarifying questions, that, following review by the EPDP Team's legal committee, were submitted to the Bird & Bird (see https://community.icann.org/x/xQhACQ). The EPDP Team reviewed the responses from Bird & Bird and applied the advice received in its recommendations below.

EPDP Team response to Question i.

The EPDP Team discussed this question extensively. As a starting point, the EPDP Team notes that the GDPR[14] and many other data protection legislations set out requirements for protecting personal data of natural persons. It does not protect the non-personal data of legal persons. At the same time, the EPDP Team recognizes that the European Data Protection Board ("EDPB") has advised ICANN in a July 2018 letter that "the mere fact that a registrant is a legal person does not necessarily justify unlimited publication of personal data relating to natural persons who work for or represent that organization," and that "personal data identifying individual employees (or third parties) acting on behalf of the registrant should not be made publicly available by default in the context of WHOIS".[15]

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

- Some EPDP Team members are of the view that differentiation should be required for many reasons that benefit the public. First, a significant percentage of domain names are registered by legal entities and the GDPR generally does not protect their domain name registration data. Further, to the extent that personal information is included in such registration data, the legal guidance received[16] indicates that it is likely to be "low sensitivity" because it relates to an employee's work details rather than their private life. Given the surge in internet-based crimes (including ransomware demands that cripples public infrastructure), publishing the registration data of legal entities would aid law enforcement, consumer protection, and cybersecurity professionals' ability to quickly and more effectively investigate illicit activities facilitated by the DNS. Second, requiring registrars to publish the domain name registration data of legal entities would also significantly reduce the challenges associated with obtaining responses to disclosure. Third, publishing legal persons' data based on differentiation instead of consent significantly reduces the Contracted Parties' liability. Hence, publishing legal persons' data based on differentiation rather

[14] "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."
[15] 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
[16] See paragraph 14.3 of the Bird & Bird Memorandum - March 2021 questions regarding legal personhood, consent etc.

than consent could be considered a best practice. Finally, the legal guidance[17] received stated that if the proper safeguards are followed, the legal risks associated with such publication, even in the event of inadvertent mistakes, seem low. Hence, on balance, the public interest favors differentiating between registrations of legal and natural persons. In these EPDP members' view, no evidence has been put forward that confirms or quantifies claims that operational or financial burdens on Contracted Parties would result from such a practice

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

For the purpose of obtaining community input, the EPDP Team is putting forward the following preliminary recommendations:

[17] See paragraph 14.1 – 14.6 of the Bird & Bird Memorandum - March 2021 questions regarding legal personhood, consent etc

Preliminary Rec #6.
No changes are recommended, at this stage, 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").

EPDP Team Question for Community Input #1
Is there new information or inputs that the Phase 2A team has not considered in assessing whether to make changes to the recommendation that Registrars and Registry Operators may, but are not obligated to, differentiate between legal and natural persons?

Preliminary Rec #7.
The EPDP Team recommends that the GNSO Council monitors developments in relation to the adoption and implementation of relevant legislative changes (for example, NIS2), relevant decisions by pertinent tribunals and data protection authorities, as well as the possible adoption of the SSAD to determine if/when a reconsideration of this question (whether changes are required to the EPDP Phase 1 recommendation "Registrars and Registry Operators are permitted to differentiate between registrations of legal and natural persons, but are not obligated to do so") is warranted. The GNSO Council is expected to consider not only input on this question and any new information from GNSO SG/Cs but also ICANN SO/ACs to help inform a decision on if/when this question is expected to be reconsidered.

EPDP Team Question for Community Input #2
Is this recommendation necessary for the GNSO council in considering future policy work in this area? If yes, in what ways does this monitoring assist the Council?

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

[18] Note, the NCSG members believe that the EPDP Team should not be providing guidance as such. These members are of the view that it is best for the Contracted Parties to develop guidance on their own and provide the same to their peers.

In the following recommendation, the EPDP Team outlines how a Contracted Party that wants to differentiate can do so by using a standardized data element. While the EPDP Team is seeking specific feedback on a number of questions in relation to such a possible standardized data element, the EPDP Team has not foreclosed the option of having additional options added to the field in the future, e.g., legal person - personal information present, etc. In other words, the EPDP Team recommends that the additional data element be extensible, in principle.

Do note that some EPDP Team members are of the view that the use of such a standardized data element should be obligatory for those Contracted Parties that decide to differentiate, while other EPDP Team members are of the view that because there is no requirement to differentiate, there should not be a requirement to use a standardized data element, and a Contracted Party should be able to determine itself how to implement such a differentiation[19].

For the purpose of obtaining community input, the EPDP Team is putting forward the following preliminary recommendation:

Preliminary Rec #8.
The following additions are made to the EPDP Phase 1 recommendations:

> Recommendation #5
>
> The following optional data element (optional for the Registrar to offer to the Registrant and collect) is added to the data elements table:

Data Elements (Collected & Generated*)	Collection Logic
Registrant Legal Person (Yes/No/Unspecified[20])	[MAY / MUST, IF Contracted Party chooses to differentiate*]

[19] The Registry Stakeholder Group team members have expressed a specific objection to the inclusion of this preliminary recommendation. In their view, the more acceptable option is to include such a suggestion relating to consistent labelling and handling of potential flags within the body of the voluntary guidance (e.g. Preliminary Recommendation #3.3).

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

For the purpose of the Legal person and non-personal data field, which is optional for the Registrar to provide to the Registrant to self-designate, Registrars should advise the Registered Name Holder at the time of registration what the consequences are of self-designating as a legal or a natural person and to provide non-personal data only (or provide appropriate consent if personal data is involved), consistent with preliminary recommendation #3, point 4. Recommendation #7[21]

Transfer of Data Elements from Registrar to Registry:

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

Recommendation #8

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

For Registrars:

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

For Registries:

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

[21] Do note that the implementation of this recommendation is still pending Board/GNSO Council resolution of the intent in relation to the Thick Whois Consensus Policy".

Recommendation #10

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

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

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

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

For clarity, the existence of this standardized data element does not require a Contracted Party to differentiate between legal / natural person type or personal / non-personal data.[22] As part of the implementation, it should be considered whether for those Contracted Parties that choose not to differentiate, the data field is not visible in RDDS or automatically set to "unspecified".

EPDP Team Question for Community Input #3

1. Should a standardized data element be available for a Contracted Party to use? If yes, why? If no, why not? Why is harmonization of practices beneficial or problematic?
2. If yes, what field or fields should be used and what possible values should be included, if different from the ones identified above? Aspects of the recommendation that the EPDP Team is looking for specific input on having been marked above with *, indicating the options that are under consideration.

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

3. If such a standardized data element is available, MUST a Contracted Party who decides to differentiate use this standardized data element or should it remain optional for how a Contracted Party implements this differentiation?

EPDP Team response to Question ii.

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

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

- EPDP-p1-IRT:[23] "Publication", "Publish", and "Published" means to provide Registration Data in the publicly accessible Registration Data Directory Services.
- EPDP-p1-IRT:[24] "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:[25] Disclosure: The processing action whereby the Controller accepts responsibility for release of personal information to third parties upon request.

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

Scope of GDPR and other data protection legislation

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

[23] See https://docs.google.com/document/d/1SVFkoI6RmrVVz--RrVLSOj1bmz1qLb7_JTuvt7At4Uo/edit
[24] Idem
[25] See https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-2-20feb19-en.pdf

as the data provided by legal persons may include personal data that is protected under data protection law, such as GDPR.

D. Although the GDPR does not cover the processing of personal data which concerns legal persons, GDPR Principles, some of which are described below, may still apply if a natural person's personal data is processed as part of the differentiation process and should be factored in as appropriate by Contracted Parties. Consistent with the Principles set forth in Article 5 of the GDPR:
   a. Lawfulness, Fairness and Transparency: "Any processing of personal data should be lawful, fair, and transparent. It should be clear and transparent to individuals that personal data concerning them are collected, used, consulted or otherwise processed, and to what extent the personal data are, or will be, processed." The transparency principle "concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing . . . [26]

      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."[27]
   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."[28]
   c. Data Minimization: "Limit the amount of personal data collected to what is necessary for the purpose."[29]
   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."[30]

[26] 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);

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

[28] 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-regulatio n-gdpr/principles/purpose-limitation/)

[29] 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_a nd_by_default_v2.0_en.pdf) and GDPR Article 5.1 (c).

[30] 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_a nd_by_default_v2.0_en.pdf

Relevant EPDP Phase 1 Recommendations[31]

E. Per EPDP Phase 1[32] Recommendation #6, "as soon as commercially reasonable, Registrar must provide the opportunity for the Registered Name Holder to provide its Consent to publish redacted contact information, as well as the email address, in the RDS for the sponsoring registrar".

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

Relevant EPDP Phase 2 Recommendations

G. Per Phase 2[33] Final Report Recommendation #9.4.4, which addresses automation of SSAD processing: "the EPDP Team recommends that the following types of disclosure requests, for which legal permissibility has been indicated under GDPR for full automation (in-take as well as processing of disclosure decision) MUST be automated from the time of the launch of the SSAD (…) No personal data on registration record that has been previously disclosed by the Contracted Party." This Recommendation 9.4.4 focuses generally on automating disclosure for registration records that do not include personal data.[34]

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.

[31] 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.

[32] 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.

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

[34] 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.

Proposed Guidance[35] [36]

For the purpose of obtaining community input, the EPDP Team is putting forward the following preliminary recommendation:

Preliminary Rec #9.
The EPDP Team recommends that Contracted Parties who choose to differentiate based on person type SHOULD follow the guidance[37] 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).

8. 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,[38] and (ii) at the time the Registrant updates its contact information or without undue delay after the contact information is updated.
9. 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.
10. As part of the implementation, Registrars should consider using a standardized data element in the RDDS, SSAD or their own data sets that would indicate the type of person it concerns (natural or legal) and, if legal, also the type of data it concerns (personal or non-personal data). Such flagging would facilitate review of disclosure requests and automation requirements via SSAD and the return of non-personal data of legal persons by systems other than SSAD (such as Whois or RDAP). A flagging mechanism may also assist in indicating changes to the type of data in the registration data field(s).
11. Registrars should ensure that they clearly communicate the nature and consequences of a registrant identifying as a legal person. These communications should include:

[35] Note, the NCSG members believe that the EPDP Team should not be providing guidance as such. These members are of the view that it is best for the Contracted Parties to develop guidance on their own and provide the same to their peers. At the same time, the IPC, ALAC and GAC members have advocated that there should be mandatory requirements i.e. consensus policy, not merely guidance/best practices.
[36] Some EPDP Team members have indicated a preference for using the term "best practices", while other EPDP Team members have indicated that the development of "best practices" is typically reserved for industry bodies. ICANN org in its response (see hereunder) has indicated that from an implementation perspective, there would not be a difference whether this is called "guidance" or "best practice". Commenters on the Initial Report are encouraged to weigh in on what terminology is deemed most appropriate and why.
[37] 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.
[38] 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.

a. An explanation of what a legal person is in plain language that is easy to understand.
b. Guidance to the registrant (data subject)[39] 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.[40] This is also consistent with section 3.7.7.4 of the Registrar Accreditation Agreement (RAA).

12. 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.
13. Registrants (data subjects) must have an easy means to correct possible mistakes.
14. 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.

EPDP Team Question for Community Input #4

1. Does this guidance as written provide sufficient information and resources to Registrars and Registry Operators who wish to differentiate? If not, what is missing and why?
2. Are there additional elements that should be included?
3. Are there legal and regulatory considerations not yet considered in this Initial Report, that may inform Registries and Registrars in deciding whether and how to differentiate, and if so, how?
4. If a Registrar or Registry Operator decides to differentiate, should this guidance become a requirement that can be enforced if not followed ("MUST, if Contracted Party decides to differentiate")?

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.

[39] 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.
[40] See also https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

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.[41]

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[42] (ii) set the registration data set to automated disclosure in response to SSAD queries and (iii) publish the data (to provide Registration Data in the publicly accessible Registration Data Directory Services).

c. If the Registrant (data subject) has self-identified as natural person or has confirmed that personal data is present, the Registrar does not set that registration data to automated Disclosure and Publication, unless the data subject consents to Publication.[43]

2. Data subject self-identification at time when registration is updated[44]

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.[45]

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.[46]

---

[41] 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.

[42] 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".

[43] 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.

[44] 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).

[45] 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.

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

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[47] (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.[48]
c. If legal person is inferred by the Registrar and subsequently the Registrant (data subject) is informed (per guidance #3 above) and confirms that no personal data is present, the Registrar should (i) contact the provided contact details to verify the Registrant claim[49] (ii) set the registration data set to automated disclosure in response to SSAD queries and (iii) publish the data.
d. If the Registrar has inferred that the Registrant is a natural person or has detected personal data, the Registrar should not disclose registration data unless the Registrant provides consent for publication or the Registrar Discloses the data in response to a legitimate disclosure request.

The EPDP Team recognizes that in all of the above scenarios, there is the possibility of misidentification, which may result in the inadvertent disclosure of personal data. In this regard, the EPDP Team encourages review of the Bird & Bird memo which can also be found in Annex E, especially sections 11.11.1-2, 13, 14.3 and 18.

3.2 Feasibility of Unique Contacts

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

i. Whether or not unique contacts to have a uniform anonymized email address is feasible, and if feasible, whether it should be a requirement.

[47] 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".
[48] 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).
[49] 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".

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".[50]

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.

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.

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

"Registrant-based email contact", means “an email for all domains registered by a unique registrant [sponsored by a given Registrar] OR [across Registrars], [51] which is intended to be pseudonymous[52] data when processed by non-contracted parties.[53]”[54]

"Registration-based email contact", means “a separate single use email for each domain name registered by a unique registrant, which is intended to be anonymous data when processed by non-contracted parties. [55]”

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

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

[52] 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.

[53] 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.

[54] 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.

[55] 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.

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 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.[56]

*Note, during the 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.[57] 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. Nevertheless, if further evidence concerning issues with

[56] 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.
[57] See https://community.icann.org/x/I4GBCQ

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

EPDP-P1 Recommendation #14
In the case of a domain name registration where an "affiliated" privacy/proxy service used (e.g. where data associated with a natural person is masked), Registrar (and Registry where applicable) MUST include in the public RDDS and return in response to any query full non-personal RDDS data of the privacy/proxy service, which MAY also include the existing privacy/proxy pseudonymized email.

EPDP Phase 2 consideration of this topic

The EPDP Phase 2 Final Report noted that:

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

EPDP Team Proposed Responses to Council Questions

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

EPDP Team response to Question i.

The EPDP Team recognizes that it may be technically feasible to have a registrant-based email contact or a registration-based email contact.[58] Certain stakeholders see risks and other concerns[59] that prevent the EPDP Team from making a

[58] 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.
[59] 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.

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.[60]

EPDP Team response to Question ii.

For the purpose of obtaining community input, the EPDP Team is putting forward the following preliminary recommendation:

Preliminary Rec #10.
The EPDP Team recommends that Contracted Parties who choose to publish a registrant- or registration-based email address in the publicly accessible 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 in this recommendation (see Annex E).

EPDP Team Question for Community Input #5

1. Does this guidance as written provide sufficient information and resources to Registrars and Registry Operators who wish to publish a registrant- or registration-based email address? If not, what is missing and why?

[60] 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.

4 Next Steps

4.1 Next Steps

The EPDP Team will complete the next phase of its work, which includes reviewing all public comments received on this Initial Report. Following this review, the EPDP Team will develop its recommendations into a Final Report, which will be sent to the GNSO Council. 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 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".[61] 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

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

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.

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:

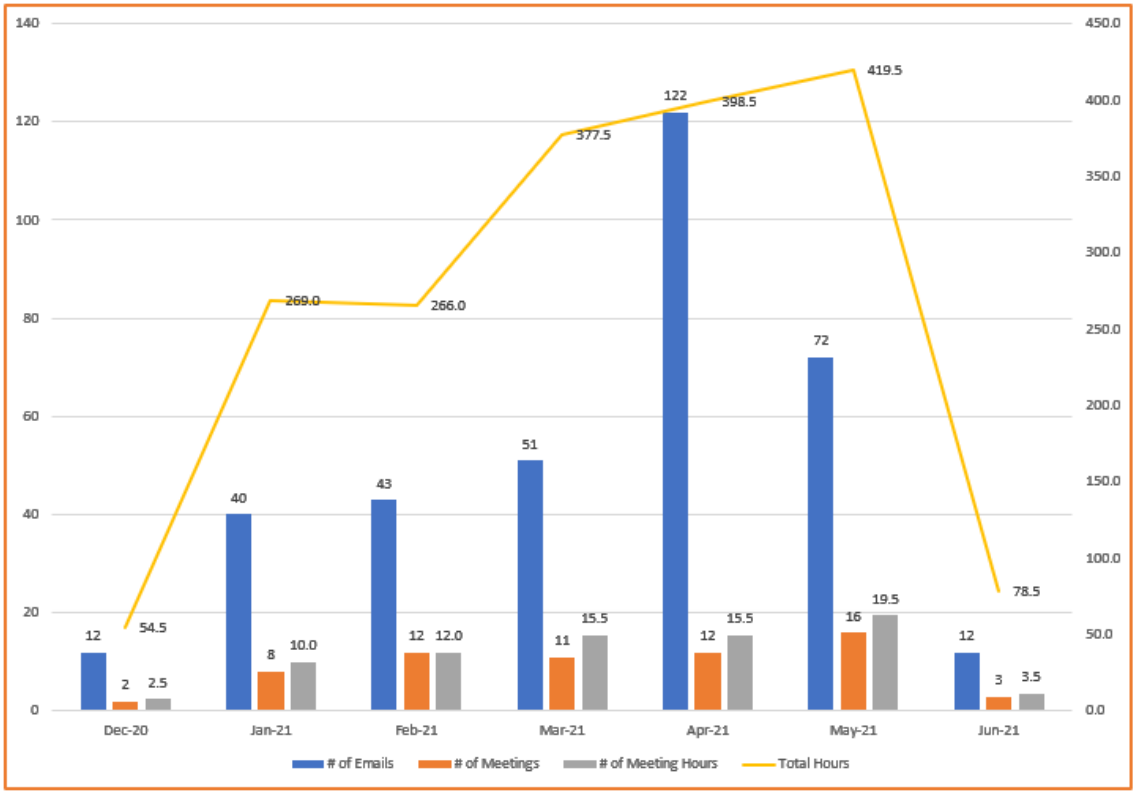
- 24 Plenary Calls for 35.5 call hours for a total of 1447.0 person hours
- 93.5% total participation rate
- Project 74% complete

Legal Committee Meetings:

- 11 Subgroup Calls for 17.5 call hours for a total of 256.5 person hours
- 89.2% total participation rate

Leadership Meetings:

- 27 Leadership Calls for 27.0 call hours for a total of 183.0 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)				**97.9%**	
Alan Greenberg	SOI	15-Nov-2020		95.8%	
Hadia Elminiawi	SOI	15-Nov-2020		100.0%	LC
Commercial Business Users Constituency (BC)				**93.6%**	
Margie Milam	SOI	15-Nov-2020		91.3%	LC
Mark Svancarek	SOI	15-Nov-2020		95.8%	
GNSO Council				**88.3%**	
Brian Beckham	SOI	18-Feb-2021		76.5%	Vice-Chair, LC
Keith Drazek	SOI	12-Mar-2020		100.0%	Chair, LC
Philippe Fouquart	SOI	26-Jan-2021		85.0%	Liaison, LC
Governmental Advisory Committee (GAC)				**84.5%**	
Christopher Lewis-Evans	SOI	19-Nov-2020		91.7%	
Laureen Kapin	SOI	19-Nov-2020		87.5%	LC
Melina Stroungi	SOI	20-Nov-2020		73.9%	LC
ICANN Board				**87.2%**	
Becky Burr	SOI	12-Nov-2020		83.3%	Liaison, LC
Matthew Shears	SOI	12-Nov-2020		91.3%	Liaison
Intellectual Property Constituency (IPC)				**91.7%**	
Brian King	SOI	20-Nov-2020		95.8%	LC
Jan Janssen	SOI	20-Nov-2020		87.5%	LC
Internet Corporation for Assigned Names & Numbers (ICANN)				**95.8%**	
Amy Bivins	SOI	12-Jul-2020		91.7%	Liaison, LC
Brian Gutterman	SOI	12-Oct-2020		100.0%	Liaison
Internet Service Providers and Connectivity Providers Constituency (ISPCP)				**91.7%**	
Christian Dawson	SOI	15-Nov-2020		91.7%	
Thomas Rickert	SOI	15-Nov-2020		91.7%	LC
Non-Commercial Stakeholder Group (NCSG)				**71.4%**	
David Cake	SOI	12-Mar-2020		87.5%	
Manju Chen	SOI	12-Mar-2020		95.8%	
Milton Mueller	SOI	12-Mar-2020		65.2%	
Stefan Filipovic	SOI	12-Mar-2020		20.8%	LC
Stephanie Perrin	SOI	12-Mar-2020		87.5%	LC
<Vacant>					
Registrar Stakeholder Group (RrSG)				**78.6%**	
James Bladel	SOI	15-Nov-2020		40.9%	
Sarah Wyld	SOI	15-Nov-2020		95.8%	
Volker Greimann	SOI	15-Nov-2020		95.8%	LC
Registry Stakeholder Group (RySG)				**98.6%**	
Alan Woods	SOI	15-Nov-2020		100.0%	LC

Marc Anderson	SOI	15-Nov-2020		100.0%	
Matthew Crossman	SOI	15-Nov-2020		95.8%	LC
Security and Stability Advisory Committee (SSAC)				**100.0%**	
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)					
<Vacant>					
<Vacant>					
Commercial Business Users Constituency (BC)					
Steve DelBianco	SOI	15-Nov-2020		95.0%	
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		100.0%	
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		100.0%	
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 - Community Input

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.

Annex E – 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.[62] 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.[63] This bears some parallels to other EU liability regimes for operators of services online that process – unwittingly – content that violates EU law.[64] As discussed

[62] Attributable to the Registrant's own error and/or a failing in the verification mechanisms deployed by a Contracted Party.

[63] 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 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.

[64] 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.

at footnote 66 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 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 date? 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.[65]

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) 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

[65] 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.

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 inaccuracy[66] – 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.

[66] 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.*"

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*".

* * *

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"),[67] 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:

> *'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.*

[67] 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 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:[68]

[68] 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

> "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,[69] 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.

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).[70]

---

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.

[69] 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).

[70] 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

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 supervision[71] 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,[72] 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).

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.

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.

[71] 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."

[72] "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.

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.[73] 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 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").

[73] EDPB July 2018 Letter, at pages 2-3.

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*"[74] / "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."[75] "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), [76] and/or having the ability to collect/connect more data about them (inference and/or linking).[77] 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.[78] 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 man-power, so that the risk of identification appears in reality to be insignificant"[79]. 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), 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.[80]

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

[74] Judgement of the CJEU in Case C-434/16 *Nowak,* ECLI:EU:C:2017:994, at paragraph 35.
[75] GDPR Recital 26
[76] 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.
[77] 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
[78] 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.")
[79] Judgement of the CJEU in Case C-582/14 *Breyer,* ECLI:EU:C:2016:779, at paragraphs 45 and 46.
[80] 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.

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,[81] 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.[82] 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 identifiable individual and not be personal data about that individual, as the information does not relate to them.")[83]

70.5 Moreover, not only do authorities in this field not always place substantial emphasis on *Nowak*, but *if* they were 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)[84] 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

[81] WP 136, at page 10.
[82] https://www.autoriteprotectiondonnees.be/citoyen/vie-privee/lexique
[83] 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
[84] 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

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 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,[85] 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;

[85] 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

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.[86] 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 WHOIS queries is indeed a contributor to the receipt of spam, albeit just one of many".[87]

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

[86] 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."

[87] *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

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".[88]

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.

* * *

[88] 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