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

The EDPB, in [a July 2018 letter to Göran Marby](https://www.icann.org/en/system/files/correspondence/jelinek-to-marby-05jul18-en.pdf), 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*

[Appendix A of the Temporary Specification](https://www.icann.org/resources/pages/gtld-registration-data-specs-en/#appendixA) 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: (…)*”.

Recommendation #6 of the [EPDP Phase 1 Final Report](https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf), 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.”*

The [EPDP Team Phase 2 Final Report](https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-phase-2-temp-spec-gtld-registration-data-2-31jul20-en.pdf), 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.”*

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**](https://community.icann.org/display/EOTSFGRD/EPDP+-P2+Legal+subteam?preview=/111388744/126428940/ICANN%20memo%2013%20March%202020%20-%20consent.docx)”).

*Legal vs. natural personhood*

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.”*

Bird & Bird has provided advice relevant to this issue, notably in:

* 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**](https://community.icann.org/download/attachments/102138857/Natural%20vs.%20Legal%20Memo.docx?version=1&modificationDate=1548874825000&api=v2)”); and
  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**](https://community.icann.org/download/attachments/111388744/ICANN%20memo%209%20April%202020.pdf?version=1&modificationDate=1588031082000&api=v2)”).

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.

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*

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).

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*

* 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.
  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).
  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.
  4. The Consent Memorandum explained that:
     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
     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*

* 1. 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).
  2. Therefore, *if* any personal data is in fact included in Registration Data, this would be a hopefully rare and unintended event.[[1]](#footnote-1) In short, the GDPR should for the most part be inapplicable except in accidental edge cases.
  3. 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:
     1. Significant steps were taken to verify that the data is not personal data; and
     2. An easy means of correcting mistakes was provided.
  4. 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.[[2]](#footnote-2) This bears some parallels to other EU liability regimes for operators of services online that process – unwittingly – content that violates EU law.[[3]](#footnote-3) As discussed at footnote 6 below, this is arguably recognised in (at least some) decisions of GDPR supervisory authorities.

*Combination*

* 1. 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.
  2. 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.
  3. 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):
     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.
     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? |

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.

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.

Our view is based on the following factors (also bearing in mind GDPR Article 83(2), discussed at paragraph 8 above):

* 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.
  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.
  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.[[4]](#footnote-4)
  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.
  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.
  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*):

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.

Contracted Parties would need to account for postal (“snail mail”) timescales if that medium is used – it may take some time for post to be delivered to the organisation, and then find itself to the right person (who may be out of office, e.g. on annual leave), and then be dealt with by that person. Email would at least not usually suffer from delivery delays; the grace period would then only need to address a possible leave of absence and/or the recipient’s temporary inability to deal with the email for other reasons.

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).

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.

*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.

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*.”

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.

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.

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).

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).

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.

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.

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.

Ultimately, therefore, we cannot presently foresee other measures being required or expected of Contracted Parties, besides those already being discussed in the question posed.

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[[5]](#footnote-5) – 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.

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*”.

\* \* \*

1. Attributable to the Registrant’s own error and/or a failing in the verification mechanisms deployed by a Contracted Party. [↑](#footnote-ref-1)
2. 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. [↑](#footnote-ref-2)
3. See, for example, [Article 14](https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031) of the e-Commerce Directive 2000/31/EC and its transposition into the national laws of EU/EEA Member States and the UK. [↑](#footnote-ref-3)
4. 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. [↑](#footnote-ref-4)
5. 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.*” [↑](#footnote-ref-5)