MEMORANDUM

|  |  |
| --- | --- |
| **To:** | Internet Corporation for Assigned Names and Numbers, EPDP Team |
| **From:** | Ruth Boardman & Gabe Maldoff |
| **Date:** | 25 January 2019 |
| **Subject:** | Advice on liability in connection with a registrant's self-identification as a natural or non-natural person pursuant to the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") |

**Background**

1. Where registrants are natural persons, most, or all, of the information they provide at registration is personal data. However, many registrants are corporate entities. For these registrants, the registration data only includes personal data if the registrant provides contact details relating to a natural person (e.g. [*firstname.lastname@company.com*](mailto:firstname.lastname@company.com)). If contact details are generic, such as [*info@company.com*](mailto:info@company.com), then the registration data will not include personal data. For the purposes of this memo, we will refer to registrants that do not supply personal data as "non-personal registrants".
2. The current approach is to treat all registrations as if they may contain personal data. However, seeing as non-personal registrants make up a substantial portion of registrants, one solution being discussed is to distinguish these registrants from those that provide personal data. Under this approach, registration details would be made publicly available by default for non-personal registrants.
3. Non-personal registrants would be distinguished by asking registrants to self-identify as such at the time of registration. The EPDP team has concerns that some registrants may mistakenly self-identify as non-personal, even if either they are registering as a natural person or they provide personal contact details on behalf of a corporate entity.
4. The EPDP Team has asked Bird & Bird to advise on whether the relevant parties could be subject to liability under GDPR if they rely on the registrant's inaccurate self-identification. If the answer is yes, the EPDP team has asked us to consider whether there are ways to reduce the risk of liability.

**Analysis**

1. As a starting point, we agree that information concerning legal persons (and not relating to natural persons) is not personal data under the GDPR. Therefore, the relevant parties could make such data publicly available without triggering GDPR concerns.
2. However, some registrants may incorrectly characterise their data. This would cause personal data to be disclosed as if it had been provided from non-personal registrants.
3. Where registrants provide personal data, the relevant parties will "process" it within the meaning of GDPR. The definition of personal data under the GDPR does not depend on whether a controller or processor believes the data it is processing to constitute personal data. Rather, the GDPR's application depends on the fact that personal data is processed, irrespective of any party's intent to process such data.
4. The EPDP's question, therefore, is whether the GDPR will recognise it as reasonable to base a decision on how to process personal data on a technical designation provided by the registrant, which may in some circumstances be erroneous. As we acknowledge that the relevant parties *are* permitted to treat non-personal data differently, in our view, this question requires us to consider whether reliance on the inaccurate designation would violate the Accuracy Principle set out in Article 5 of the GDPR. In addition, we consider what level of transparency is required to enable the parties to rely on the designation in accordance with the Lawfulness, Fairness and Transparency Principle of Article 5(1)(a).

Accuracy Principle

1. Article 5(1)(d) states that personal data must be “*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*”.
2. In Opinion 02/2016 on the publication of personal data for transparency purposes in the public sector,[[1]](#footnote-1) the Article 29 Working Party defined the equivalent principle of the Data Protection Directive[[2]](#footnote-2) as a requirement to take “*every reasonable step … to ensure that data are kept accurate and up to date, having regard to the purposes for which they were collected or for which they are further processed*”.
3. Despite the fact that the Accuracy Principle is a longstanding feature of data protection laws, dating back at least as far as the 1980 OECD Privacy Principles,[[3]](#footnote-3) there is little case law or guidance on its precise meaning.[[4]](#footnote-4)
4. The most comprehensive guidance we could find was from the UK Information Commissioner’s Office (“ICO”). The ICO guidance clarified that the accuracy principle imposes four obligations on a controller:

“*In practice, this means that you must:*

* *take reasonable steps to ensure the accuracy of any personal data;*
* *ensure that the source and status of personal data is clear;*
* *carefully consider any challenges to the accuracy of information; and*
* *consider whether it is necessary to periodically update the information*”

(ICO Guide to the GDPR, Principle (d): Accuracy).[[5]](#footnote-5)

1. Of particular relevance here, the Accuracy Principle does not mean that the processing of inaccurate information is automatically in violation. Rather, the focus of this principle is the reasonableness of the steps taken to ensure the data is accurate, and that there are the procedures in place to update and/or rectify data that is found to be inaccurate or out of date.
2. As explained in the ICO guidance, "*The more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy. So if you are using the data to make decisions that may significantly affect the individual concerned or others, you need to put more effort into ensuring accuracy*".
3. In this case, the accuracy of the information will have an impact on data subjects as this one factor will determine whether a data subject's details will be publicly disclosed.
4. The GDPR is not prescriptive in mandating the types of measures a party must put in place to meet this burden. The ICO guidance explains that "*[w]hat is a ‘reasonable step’ will depend on the circumstances and, in particular, the nature of the personal data and what you will use it for*". However, the guidance also states that a controller "*may have to get independent confirmation*" where the impact is particularly significant. The ICO gives the example of an employer that engages employees needing essential qualifications, where there would be a duty on the employer to verify the credentials.
5. If the relevant parties had no reason to doubt the reliability of a registrant's self-identification, then they likely would be able to rely on the self-identification alone, without independent confirmation. However, we understand that the parties are concerned that some registrants will not understand the question and will wrongly self-identify. Therefore, there would be a risk of liability if the relevant parties did not take further steps to ensure the accuracy of the registrant's designation.
6. The relevant parties could reduce this risk by either improving the accuracy of the registrants' self-identification or by introducing measures to independently verify the selection – or both:
   1. **Improving accuracy of self-identification:** Accuracy can be improved any number of ways. Suggestions include:
      1. Ensuring that language they present to registrants is as clear as possible to help avoid mistakes. We understand that the relevant parties are concerned that it will not be possible to develop clear questions that are easily understood in all relevant languages. Here, the Article 29 Working Party Guidelines on Transparency under Regulation 2016/679 ("WP260rev.01")[[6]](#footnote-6) offer a helpful suggestion:

"*If controllers are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/ notices/ policies etc., they can test these, for example, through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies, where appropriate, amongst other things*".

In other words, the relevant parties may consider consulting with focus groups and regulatory bodies to help develop language that will be easily understood. It would also be helpful to test the language to determine whether, in practice registrants understand what is being asked.

* + 1. Another way the parties might address this is to implement periodic checks of the designation. For example (and as further discussed below), confirmation emails could be sent to the registrants and/or technical contacts asking them to re-certify that the contact details do not include personal data.
  1. **Independent verification:** the relevant parties could implement technical measures to identify mis-labelled registrants. For example, to separate corporate entities from natural persons, registrants could be required to provide a corporate registration ID number when registering on behalf of a company. This would allow the registrar to detect internal inconsistencies, such as if a registrant identifies as a corporate entity but is unable to provide a valid ID number. If feasible, technical tools could also be used to assess whether email addresses include an individual's name or appear to be generic.

1. Equally important, the Accuracy Principle requires controllers to ensure that inaccurate personal data can be erased or rectified "*without undue delay*". Therefore, in addition to putting in place measures to help accurately classify registrants, the relevant parties will need to provide a simple means of permitting data subjects to correct an inaccurate designation.

Lawfulness, Fairness and Transparency Principle

1. The core risk of the proposed process is that a registrant's designation could cause personal data to be processed in a particular manner that a data subject may not understand or reasonably expect. In other words, the data subject may not understand the consequences of what would seem to be a technical designation.[[7]](#footnote-7)
2. In its Guidelines on transparency (WP260rev.01), the Article 29 Working Party stated, “*A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what* ***the scope and consequences of the processing*** *entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used. This is also an important aspect of the principle of fairness under Article 5.1 of the GDPR*” (emphasis added).
3. The EDPB placed particular emphasis on the need to explain the consequences of a processing activity where this will not be clear to data subjects: “*In particular, for complex, technical or unexpected data processing, WP29’s position is that, as well as providing the prescribed information under Articles 13 and 14 (dealt with later in these guidelines), controllers should also separately spell out in unambiguous language what the most important* ***consequences*** *of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/ notice actually have on a data subject?*” (emphasis from original).
4. When a registrant identifies as either a natural or a legal person, this self-identification will determine whether the data provided is made publicly available by default. If there is a reasonable risk that data subjects will wrongly self-identify, then failing to make the consequences of the self-identification known to data subjects could result in liability for failing to meet the Lawfulness, Fairness and Transparency Principle.
5. Therefore, in our view, relevant parties will need to ensure that data subjects clearly understand the consequences for them of the registrants' self-identification. This means that the language provided to registrants should explain, separately from any detailed terms and conditions, that self-identifying as a non-personal registrant will result in registration data being made publicly available. Moreover, as addressed in other advice we have provided, the relevant parties will need to ensure that they communicate this information to data subjects that may not be the registrant.
6. The suggestion at para. 19 above of sending a confirmation email to the registrant and technical contact will be useful for meeting this requirement if it confirms the selection and explains whether registration data will be disclosed. To further address the rectification element of the Accuracy Principle, such a confirmation could also include instructions for rectifying an erroneous classification.

1. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp239\_en.pdf. [↑](#footnote-ref-1)
2. The only difference is that Article 6(1)(d) of the Directive did not require the inaccurate data to be erased or rectified “*without undue delay*”. [↑](#footnote-ref-2)
3. The OECD Principles contained a "*Data Quality Principle*", which incorporated a similar concept of accuracy: "*Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date*". [↑](#footnote-ref-3)
4. We were unable to find any case law in the UK, Belgium or Germany directly addressing the meaning of accuracy as relevant to this query within the time we had. We would be happy to check in additional Member States if this would be helpful. [↑](#footnote-ref-4)
5. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/. [↑](#footnote-ref-5)
6. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\_id=622227. [↑](#footnote-ref-6)
7. We understand it may even be the case that the personal contact details are provided by a registrant that is not the data subject. [↑](#footnote-ref-7)