MEMORANDUM

|  |  |
| --- | --- |
| **To:** | Internet Corporation for Assigned Names and Numbers, EPDP Team |
| **From:** | Ruth Boardman & Gabe Maldoff |
| **Date:** | 13 February 2019 |
| **Subject:** | Advice on the inclusion of "city" in publicly available Whois data |

1. **Questions presented**
   1. Is the data provided by the Registered Name Holder ("**RNH**") for the “City” field in the RNH’s address personal data? To what extent is there a risk under GDPR that the publication and/or disclosure of the RNH-identified “City” could result in inadvertent disclosure of personal data (which may affect the policy of whether it should be redacted from the data that is made publicly available in Whois), or contribute to making the Registered Name Holder more identifiable? Please note that the EPDP is considering a recommendation to allow the publication of the City, State/Province and Country, while redacting the contact’s name, street address, email address, postal code, telephone number. What are the bases in the GDPR, its official advisories and interpretations, and in practices similar to our own for making such a determination?
   2. If the city field is personal data and therefore must be redacted, is there a lawful basis under Art. 6(1)(f) for publishing a subset of the data submitted by the registered name holder that includes the city name, where the legitimate interest is that those pursuing legal claims can determine jurisdictional issues prior to asserting the claim where that interest overcomes the rights of all registrants in not having their personal data published. (This proposed legitimate interest was gleaned from the transcript in Toronto.)
2. **Is the "City" field personal data?**

Definition of personal data

* 1. The GDPR defines personal data as "*any information relating to an identified or identifiable natural person (‘data subject’)*". A person is considered "*identifiable*" if she "*can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".
  2. The definition of personal data has not changed substantially from the Data Protection Directive, other than to specifically reference online identifiers and location data.[[1]](#footnote-1) Therefore, Opinion 4/2007 from the Article 29 Working Party ("**WP29**") on the concept of personal data remains relevant.
  3. According to this Opinion, a person may be considered **identifiable** by reference to strong identifiers, such as names, social security numbers, government identification numbers, etc., or "*by a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs (age, occupation, place of residence, etc.)*".
  4. Recital 26 confirms that whether an individual is identifiable must be assessed based on "*all the means reasonably likely to be used, such as singling out, either by the controller or by another person*". As stated in Opinion 4/2007, "*This means that a mere hypothetical possibility to single out the individual is not enough to consider the person as 'identifiable'. If, taking into account “'all the means likely reasonably to be used by the controller or any other person', that possibility does not exist or is negligible, the person should not be considered as 'identifiable', and the information would not be considered as 'personal data'*".
  5. A consequence of this analysis is that data may be personal data in the possession of one party, but not another. The analysis must take account of whether "*one has access to additional information*" that would permit identification. For example, in *Breyer v Bundesrepublik Deutschland*, the Court of Justice of the European Union ("**CJEU**") held that a dynamic IP address *could* be considered personal data if the online media services provider would be able to access additional identifying information from the internet service provider (ISP) to be able to identify the individual behind the dynamic IP address. In the possession of the ISP, however, the data was clearly personal.
  6. When analysed from the point of view of registries, registrars and/or ICANN (the "**relevant parties**"), the "city" field of the RNH's address will be personal data if the RNH is a natural person since it conveys information that relates to a person who is identifiable to the relevant parties. As ICANN has previously concluded, this will not be personal data when it relates to a RNH that is a legal person, but not a natural person.
  7. A further question, more relevant here, is whether a controller can publish information that is personal data in its possession, but with elements removed, on the basis that the redacted information will not be identifiable to the recipients (which could be the public at large). This approach has been considered possible in a number of cases in the UK (starting with *Common Services Agency v Scottish Information Commissioner (Scotland)*).
  8. However, we do not think this approach assists here. The *Breyer* case makes clear that information will be considered personal data if there are legal channels by which a party could obtain additional information to identify the data subject, and where the party is reasonably likely to do so:

"*Although … German law does not allow the internet service provider to transmit directly to the online media services provider the additional data necessary for the identification of the data subject, it seems however, subject to verifications to be made in that regard by the referring court that, in particular, in the event of cyber attacks legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the* *internet service provider and to bring criminal proceedings. … Directive 95/46 must be interpreted as meaning that a dynamic IP address ... constitutes personal data within the meaning of that provision, in relation to that provider,* ***where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person***" (emphasis added).

* 1. In the case of Whois, it is clear that rights holders (and others who meet the relevant criteria set out in any eventual ICANN Consensus Policy) who have used Whois data to identify a domain name which is of interest, will be able to access the information needed to identify the RNH from the relevant parties. Following *Breyer*, it *is* reasonably likely that the natural persons to whom public Whois data relates will be identifiable – accordingly, public Whois data about natural persons should be regarded as personal. The inclusion of the "city" field does not change the fact that the published data will be regarded as personal data; it simply means that more personal data will be published.
  2. Rather, the main issue is whether the additional inclusion of the "city" field is justified on the basis of the interests of rights holders in more efficiently determining whether to file claims against RNHs.

1. **Is there a legitimate interest in publishing the "City" field?**
   1. In order to satisfy Article 6(1)(f), the CJEU articulated a three-part test in *Valsts policijas Rigas regiona parvaldes Kartibas policijas parvalde v* Rigas *pašvaldibas SIA ‘Rigas satiksme’* (the "***Rigas***" case): there must be (a) an identified legitimate interest, (b) the processing must be "*necessary*" to pursue that interest, and (c) the rights and interests of the data subject must not outweigh the legitimate interest pursued by the controller.
   2. The WP29 Opinion 06/2014 *on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* remains relevant for interpreting these requirements.
   3. In addition, the GDPR requires controllers to conduct and document their balancing assessments, which analyse whether each of the three elements above is satisfied.[[2]](#footnote-2)

Overview of requirements

* 1. **Legitimate interest.** For an interest to be legitimate, the WP29 concluded that it must be lawful, sufficiently clearly defined to permit the controller to balance it with individual interests, and not be speculative. The recitals to the GDPR include examples of processing which will be for a legitimate interest, including to prevent fraud (Recital 47) and to ensure network and information security, such as preventing unauthorised access to networks and denial of service attacks (Recital 49). The Recitals also state that sharing data for internal administrative purposes *may* be a legitimate interest (Recital 48).
  2. The *Rigas* case is particularly relevant for the EPDP Team. In it, the CJEU found that there is a legitimate interest in a third party obtaining details of someone who damaged their property in order to take legal proceedings against that person. In addition, in *Camera di Commercio, Industria, Aritigianato e Agricoltura di Lecce v. Salvatore Manni* (the "***Manni***" case), the CJEU held that the Lecce Chamber of Commerce could publish data concerning bankruptcies and corporate liquidations – *in an identifiable form* – in part to protect the legitimate interests of third-parties that do business with those who have previously declared bankruptcy.
  3. **Necessary.** "N*ecessary*" does not mean it must be the only or even the least intrusive method. Rather, the analysis for necessity is linked to the concept of proportionality.
  4. In *Österreichischer Rundfunk and others*, the CJEU held that "*the adjective 'necessary' in Article 8(2) of the Convention implies that a 'pressing social need' is involved and that the measure employed is 'proportionate to the legitimate aim pursued'*". Opinion 06/2014 *on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* further explained the concept of necessity by reference to a judgment of the European Court of Human Rights[[3]](#footnote-3) which states, "*the adjective 'necessary' is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable' …*".
  5. This was also addressed in *Google Spain v AEDP*, where the CJEU held that processing cannot be considered "*necessary*" if the personal data is "*inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes*". In *South Lanarkshire Council v Scottish Information Commissioner*,[[4]](#footnote-4) the UK Supreme Court assessed this requirement of European Community law as follows: "*It is well established in community law that, at least in the context of justification rather than derogation, 'necessary' means 'reasonably' rather than absolutely or strictly necessary … necessity is well established in community law as part of the proportionality test*".
  6. **Balancing test.** Satisfying the balancing test requires an assessment of the strength of the interest pursued balanced against the potential risks for data subjects. This element of the test usually requires detailed analysis of the facts and circumstances. Opinion 06/2014 provides helpful guidance on weighing each side of the balance:
     1. Analysis of the strength of the interest:

"*In general, the fact that a controller acts not only in its own legitimate (e.g. business) interest, but also in the interests of the wider community, can give more 'weight' to that interest. The more compelling the public interest or the interest of the wider community, and the more clearly acknowledged and expected it is in the community and by data subjects that the controller can take action and process data in pursuit of these interests, the more heavily this legitimate interest weighs in the balance.*

"*On the other hand, 'private enforcement' of the law should not be used to legitimise intrusive practices that would, were they carried out by a government organisation, be prohibited pursuant to the case law of the European Court of Human Rights on grounds that the activities of the public authority would interfere with the privacy of data subjects without meeting the stringent test under Article 8(2) of the ECHR*"*.*

* + 1. The WP29 lists five factors to consider when assessing the impact on data subjects:
       1. *Assessment of impact.* The controller must consider not only adverse outcomes on individuals, but also other broader consequences for data subjects: "*Relevant 'impact' is a much broader concept than harm or damage to one or more specific data subjects. 'Impact' as used in this Opinion covers any possible (potential or actual) consequences of the data processing*".
       2. *Nature of the data.* This factor requires consideration of the level of sensitivity of the data as well as whether the data is already publicly available.
       3. *The way the data is processed.* The manner in which the data will be processed affects the balance of interests. Of particular relevance, the WP29 states, "*whether the data are publicly disclosed or otherwise made accessible to a large number of persons*" is an important consideration if "*[s]eemingly innocuous data, when processed on a large scale and combined with other data may lead to inferences about more sensitive data*".
       4. *The reasonable expectations of the data subject.* Whether an individual is likely to expect the processing activity will affect the balance of interests. This concept also appears in Recital 47 of the GDPR, which states, "*the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place*".
       5. *The status of the controller and data subject.* Finally, the assessment must take into consideration the negotiating power and any imbalances in authority between the controller and the data subject. Thus, this analysis changes depending on both the status and authority of the controller and the relative power of the data subject.

Analysis

* 1. First, CJEU case law supports finding a legitimate interest where processing of personal data will permit rights-holders to more easily vindicate their rights.
     1. For example, in the *Rigas* case, a taxi passenger opened the door of the taxi into a passing trolley, causing damage to the trolley. When the trolley operator's insurer sought to obtain information on the identity of the passenger from the police, the police refused to provide such information on data protection grounds. On this set of facts, the CJEU held "*there is no doubt that the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest*".
     2. Similarly, in the *Manni* case, the CJEU held that the Chamber of Commerce could publish of a register of individuals that had declared bankruptcy in pursuit of the legitimate interests of third-parties who may be affected by doing business with such individuals. This case demonstrates that not only do rights holders have legitimate interests, but the more prospective interest in allowing others to assess risk would also constitute a legitimate interest.
  2. In our view, "*necessity*" does not require a demonstration that there are no other less intrusive means of achieving the result.[[5]](#footnote-5) However, the relevant parties would nonetheless need to show that publishing the "city" field is proportionate. In effect, and consistent with CJEU practice, the analysis of necessity is often combined with the balancing test below.
  3. We understand that the policy development process is, in essence, an attempt to analyse these issues and propose a solution for achieving the appropriate balance based on input from a wide array of stakeholders.
  4. When conducting this assessment, a key issue for ICANN and the relevant parties to consider is to what extent the publication of the "city" field results in a significant benefit for rights holders. From our preliminary analysis, it seems that the benefits may be marginal in the EU, as IP rights tend to be national rather than local. It seems that only in limited situations, such as where the rights holder is asserting a claim of passing off, could the fact that a domain was registered in a specific city be relevant to the claim. In these situations, the fact that a domain was registered locally will usually not be a determining factor, but would be useful information.
  5. We understand from discussion in the EPDP Team meetings that the precise location of registration may be more relevant in other jurisdictions (such as the US). This preliminary analysis suggests that this data will be relevant for some registered name holders only – whereas the change in policy would result in the "city" field being published universally, with the result that the "city" field could be published in situations where it is very unlikely to deliver any benefit. The relevant parties would need to do more to demonstrate the benefit of publishing the "city" field.
  6. Against these benefits, the relevant parties must consider the risks of publication to the rights and interests of the data subjects. Publishing the "city" field could adversely impact some RNHs.
     1. First, the express purpose of this policy would be to allow rights holders to more efficiently determine when to pursue a claim. Therefore, presumably this means that publishing the city field could result in some RNHs facing claims they would not otherwise face because of the additional step in needing to obtain further information about their location.

If the relevant parties can demonstrate sufficient benefits of publication, this additional risk to RNHs is unlikely to preclude ICANN from adopting this policy. As the *Manni* case demonstrates, the CJEU is prepared to recognise a legitimate interest in allowing other parties to protect their rights, even if that requires disclosure of personal data to a broader set of parties than those who have present claims to pursue.

* + 1. Second, it seems to us that the disclosure could have risks for RNHs beyond merely the threat of claims from rights holders. In limited circumstances, it may be the case that the publication of an RNH's city could result in a unique threat to the RNH. For example, consider a blog that publishes content deemed to be illegal or offensive in a particular jurisdiction – such as a blog discussing the writer's sexuality in a place where this is illegal or considered immoral, or discussing a political views that are a threat to the orthodoxy. It *may* be the case that publishing the city where the domain is registered could increase the risks faced by the writer by increasing the likelihood of identification.

We do not have enough information about the likelihood that this could occur to be able to conclude that this would prohibit publication of the "city" field. However, it is a factor which should be considered by the EPDP Team. As Whois data was published in a clearly identifiable form for many years, the relevant parties may have a better understanding of whether the types of consequences described above actually do materialize.

* 1. Taking all the above into consideration, the relevant parties may be able to satisfy the legitimate interests test for the publication of the "city" field. However, this is not clear to us from the information available so far. In particular:
     1. further information will be required to show that the benefits to rights holders are sufficiently meaningful as to justify universal publication of city field, rather than being of use in very limited cases; and
     2. more information on the potential impact on the rights and interests of data subjects is needed.
  2. The relevant parties would then need to conduct a detailed assessment of the facts and circumstances to determine whether the interests pursued outweigh those of data subjects.
  3. It may be that further analysis will conclude that there is justification. Our survey of similar practices among other top-level domain systems reveals that practices across the European Union are mixed. For example, the database of .eu domains does what the EPDP Team has proposed, by the "city" field, but not providing the full address or name of the RNH. By contrast, databases of UK and German country code domains do not provide the "city" field, while France and Belgium provide full address details (and even the name) of the RNH. Given the range of practices, it may be that others were able to satisfy themselves that the balance of interests favoured the rights holders or that there were other interests at stake we have not considered here.

1. The Data Protection Directive defined personal data as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". [↑](#footnote-ref-1)
2. *See* Article 29 Working Party Guidelines on transparency under Regulation 2016/679 (WP260 rev.01). [↑](#footnote-ref-2)
3. Silver & Others v United Kingdom of 25 March 1983. [↑](#footnote-ref-3)
4. [2013] UKSC 55. [↑](#footnote-ref-4)
5. Such a strict interpretation might preclude the publication of the "city" field on this basis since rights holders likely could access the "city" field, even if not published, when they sought to pursue legitimate claims. [↑](#footnote-ref-5)