MEMORANDUM

|  |  |
| --- | --- |
| **To:** | Internet Corporation for Assigned Names and Numbers, EPDP Team |
| **From:** | Ruth Boardman & Gabe Maldoff |
| **Date:** | 22 January 2019 |
| **Subject:** | Advice on providing notice to technical contacts as part of the domain name registration process pursuant to the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") |

1. The EPDP Team has asked two questions relating to the domain name registration process. The first question, addressed in this memo, is whether it is sufficient to require the Registered Name Holder ("RNH") to provide notice to the technical contact on the registrar's behalf where the technical contact and the RNH are not the same person, or whether the registrar must obtain the technical contact's consent.
2. Article 13 of the GDPR sets out the controller’s obligation to provide notice where the controller collects the data directly from data subjects. Under Article 13, the relevant information must be provided "*at the time when personal data are obtained*".
3. Article 14 applies where the controller obtains the personal data indirectly – i.e. where it has "*not been obtained from the data subject*". Article 14 generally requires controllers to provide data subjects with the same categories of information as Article 13. However, Article 14 differs from Article 13 in several respects:
	1. **Minor differences in the content of the information to be provided**: Article 14 requires the controller to identify the sources of personal data as well as the categories of personal data that will be processed. These elements are not required under Article 13.
	2. **Timing of notice**: notice must be provided to data subjects "*within a reasonable period after obtaining the personal data*" but not later than within one month or upon first communication with the data subject or disclosure to another recipient – whichever comes first.
	3. **Broader exceptions to the notice requirement**: Controllers are exempt from Article 13 notice requirements only if the data subject already has the information or EU or Member State legislation enacted pursuant to Article 23 exempts the controller from providing notice. By contrast, under Article 14, in addition to the exemptions above, controllers may be exempt if a binding obligation of professional secrecy applies (for example, a lawyer would not need to provide notice if it would violate her client's confidentiality) or if providing the information would be "*impossible or would involve disproportionate effort*":

"*Paragraphs 1 to 4* [which set out the required content of the notice] *shall not apply where and insofar as … the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes … . In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available*" (Article 14(5)(b)).

1. Both Article 13 or 14 impose an obligation on the controller to "*provide*" the relevant information, unless an exemption applies. The European Data Protection Board ("EDPB") interprets this obligation strictly:

"*Both Articles 13 and 14 refer to the obligation on the data controller to “provide the data subject with all of the following information...” The operative word here is “provide”.* ***This means that the data controller must take active steps to furnish the information in question to the data subject or to actively direct the data subject to the location of it (e.g. by way of a direct link, use of a QR code, etc.)****. The data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app*" (EDPB Guidelines on transparency under Regulation 2016/679 (emphasis added)).

1. This obligation must be read in conjunction with Article 12, which states, "*The controller shall take* ***appropriate measures*** *to provide any information referred to in Articles 13 and 14 … in a concise, transparent, intelligible and easily accessible form, using clear and plain language*" (emphasis added). Also relevant to the query is the general obligation, set out in Article 24(1), “*to be able to demonstrate that processing is performed in accordance with this Regulation*”.
2. Where the RNH provides the registrar with personal data concerning another person who will be the technical contact, Article 14 applies because the registrar will not receive the technical contact’s personal data from her directly.
3. The proposal to require the RNH to provide notice to the technical contact on the registrar’s behalf will allow the registrar to satisfy its obligations under Article 14, but only if the notice is actually provided.
4. If the notice is not provided, the registrar may be able to file a claim against the RNH for non-compliance with a contractual duty, but it will not be able to show that Article 14 was met. The registrar would need to be able to demonstrate that its means of providing notice was an “*appropriate measure*” under Article 12, which in our view will be difficult here given the high likelihood that RNHs will not comply.
5. Moreover, even if the RNH does fulfil her duty, the registrar will not be able to "*demonstrate*" that it has met its obligations under Article 14. If an individual or data protection authority asked for evidence that notice was provided to a given data subject, the registrar would not be able to meet this burden. A controller relying on such an arrangement would likely seek to impose an obligation on the third-party to retain the relevant records and to permit the controller to audit the third-party’s processes. It is not practical for a registrar to impose this on RNHs.
6. Nor will registrars be exempt from providing notice due to impossibility or disproportionate effort.
	1. Providing notice is not impossible. To rely on the exemption for impossibility, the controller must demonstrate there are “*factors that actually prevent it from providing the information in question to data subjects*” (EDPB Guidelines on transparency). It is not impossible in this case for registrars to provide notice because they have contact details for the technical contacts on file.
	2. The EDPB Guidelines interpret the exemption for disproportionate effort very narrowly. Citing the reference in Article 14(5) to research purposes, the guidelines state that “*this exception should not be* ***routinely*** *relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes*”.
	3. As the intended processing in this case is not for any of the listed purposes, registrars will not be able to rely on the exemption. While in our view, there is scope to argue that the EDPB’s interpretation is overly restrictive – a plain reading of the relevant section suggests that research purposes would be *an* example of when the exception would apply, not the *only* example – we do not recommend raising this point here. The effort required by registrars to provide notice likely would not meet the standard of disproportionate effort even under a more flexible interpretation.[[1]](#footnote-1)
7. In summary, if RNHs are required to provide notice to technical contacts on behalf of registrars, this will only meet the GDPR’s transparency requirements if such notice is actually provided. Given that there is reason to believe RNHs will not always meet this obligation and registrars will have no means of demonstrating that notice has in fact been provided, this approach will not allow registrars to meet their obligations. To meet Article 14, registrars will need to provide notice to the technical contact within the earlier of one month or first communication with the data subject.
8. If notice is not provided effectively, this could also affect the legal basis for processing.
	1. If registrars will rely on consent, then there is an obligation to "*demonstrate*" that consent has been obtained in compliance with GDPR. For the reasons explained above in relation to notice, it will be difficult for registrars to do this if RNHs obtain consent on their behalf.
	2. If registrars will rely on legitimate interests, then the effective provision of notice will also have an impact. Recital 47 of the GDPR 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*” (emphasis added). In its Guidance on legitimate interests under the equivalent provision of the Data Protection Directive, the Article 29 Working Party recognised that effective transparency is an element to consider when analysing a data subject’s reasonable expectations: “*it is necessary to take account of the factual context rather than simply rely on text in small print*”. Therefore, in our view, the manner in which notice is provided could affect the registrar’s ability to rely on legitimate interests as the legal basis for processing. In particular, if notice cannot be provided in a manner that is effective, this would undermine the argument for legitimate interests with respect to those data subjects.
1. *See, e.g., Dawson-Damer & Ors v Taylor Wessing LLP [2017] EWCA Civ 74*, in which, the UK Court of Appeal addressed the concept of disproportionate effort in in the context of a subject access request. While the court recognized that disproportionate effort implies a balancing test between the controller’s interests and the interests of the data subject, it held that economic costs on the controller alone are not sufficient to show a disproportionate burden. The controller’s effort in addition must be balanced against the “*potential benefit that the supply of the information might bring to the data subject*”. In the words of the court, “*it is not open to a data controller to avoid substantive compliance by arguing that work would be expensive or time-consuming. The cost of compliance is the price data controllers pay for processing data*”. [↑](#footnote-ref-1)