Comments on EDPB guidelines 01/2022 on data subject access, version 1.0: ...

Zwenne, G.J.

COMMENTS

prof dr. G-J. (Gerrit-Jan) ZWENNE[*]

EDPB Guidelines 01/2022 on Data Subject Access, version 1.0, adopted on 18 January 2022

INTRODUCTION

Without a doubt, data subject access rights are among the most useful rights the GDPR provides data subjects to enhance transparency and to facilitate control over the processing of their personal data. At the same time, the exercise of access rights by data subjects gives rise to many complaints and disputes.[1] As a result, there is a lot of detailed and nuanced case law on the scope of access rights and the applicable exemptions. In addition to the judgments of Court of Justice of the European Union, notably *Rijkeboer*,[2] *IND*[3] and *Nowak*,[4] there is also a large volume of court decisions by member states' courts, including judgments of the highest national civil and administrative courts.

Surprisingly, the EDPB Guidelines 01/2022 on Data Subject Access Rights seem to ignore, and in some instances even contradict, member state national courts' decisions on data subject access rights. In that respect, the guidelines raise some interesting questions on the legitimacy and validity of the Guidelines. Indeed, pursuant to Article 70(1)(e) GDPR the European Data Protection Board (hereinafter "EDPB" and also "the Board") can issue guidelines, recommendations and best practices in order to encourage consistent application of the Regulation. But does that imply that the Board can overrule or set aside judgments of national courts? Probably not.

This short note will provide some of the most noticeable examples of statements made in the guidelines that are, to say the least, at odds with well-established case law in the Netherlands. In view of the timeframes set by the Board for this consultation, this analysis cannot be exhaustive. However, it is to be expected that further legal analysis of relevant case law in the Netherlands and other member states will reveal many more cases in which the guidelines deviate from national courts' case law. In any case, such legal analysis is needed and assuming the results of that analysis will be incorporated in version 2.0 of the Guidelines, it is likely to result in less unbalanced and controversial guidelines than that found in the current version 1.0. Most likely, this will do

[*] G-J. (Gerrit-Jan) ZWENNE is a full professor law and digital technologies, Leiden University in the Netherlands and partner at the law firm Pels Rijcken in The Hague, also in the Netherlands.

justice to the rationale expressed in recital 4, i.e. that the right to the protection of personal data, including right to access, is not an absolute right and that must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

EXAMPLE 1: INTENTION DOES MATTER

The Guidelines

In paragraph 13, the Guidelines state that

> "[g]iven the broad aim of the right of access, the aim of the right of access is not suitable to be analysed as a precondition for the exercise of the right of access by the controller as part of its assessment of access requests. Thus, controllers should not assess "why" the data subject is requesting access, but only "what" the data subject is requesting […]. Therefore, for example, the controller should not deny access on the grounds or the suspicion that the requested data could be used by the data subject to defend themselves in court in the event of a dismissal or a commercial dispute with the controller."

At the end of this paragraph is a footnote explaining that

> "this is without prejudice to any applicable national procedural rules adopted in accordance with Art. 23 GDPR, which determine for example the boundaries of the information to be provided to or exchanged between the parties to ongoing (court) proceedings and other ongoing (legal) claims or causes of action arising in the context of that legal relationship."

Comments

Data subjects do not need to substantiate their requests for access to their data held by controllers. Nevertheless, in number of cases Dutch courts, including the Supreme Court (*Hoge Raad*) and the Council of State (*Raad van State*), have decided that the controller was not obliged to comply with the access request as it was evident that the data subject did not request access in order to be aware of, and verify, the lawfulness of the processing (Recital 63 GDPR).

For instance, in a case where the data subject had stated that he submitted his request in the context of legal proceedings he wanted to start against the controller, the District Court of Rotterdam ruled that: [5]

> "The purpose of the access right is to enable the data subject to become aware of the personal data that have been collected about him and to check whether these data are

> correct and have been processed lawfully. At the time of the oral hearing, [the applicant, i.e. data subject] stated that he only submitted these requests in order to prove his innocence with documents relating to procedural files in which he was involved as a litigant. Notably, the applicant's [i.e. data subject]'s objective is not to verify whether his personal data are correct and have been processed lawfully, but to obtain information that he wants to use to provide (further) proof of his innocence in proceedings that he may initiate against the Dutch State. Therefore, the [data subject's] objective is not prompted by the protection of personal data, implying an abuse of rights [*misbruik van recht*]."
>
> [emphasis added]
>
> District Court of Rotterdam 21 January 2020, ECLI:NL:RBROT:2020:515, nr. 4.8.

Similarly, on the access right of Art. 12 of the Data Protection Directive 95/46, the Dutch Supreme Court (*Hoge Raad*) ruled that the controller does not have to comply with an access request if that request is not submitted for the purpose of verifying whether the data are correct and lawfully processed:

> "To the extent relevant here, Directive 95/46/EC [...] which has been implemented by the Data Protection Act, allows the data subject to verify whether her personal data are accurate and have been processed lawfully, in order to protect the data subject's right to privacy. Such verification may then lead to rectification, erasure or blocking of the data. The present claim of the plaintiff [i.e. data subject] is aimed at obtaining information for the purpose of the present proceedings and not for the purpose of Directive 95/46/EC (unlike, for example, the case in the CJEU judgment of 20 December 2017) [..]. Therefore, this is not personal data within the meaning of that Directive. Cf. the aforementioned judgment of the CJEU of 17 July 2014, paragraphs 44-46. The Court of Appeal therefore correctly held that the plaintiff [i.e. data subject] cannot derive from the Data Protection Act a right to the provision of [...] the medical analysis."
>
> [emphasis added]
>
> Supreme Court 16 March 2018, ECLI:NL:HR:2018:365, nr. 3.3.3.

Similar deliberations can be found in Judgments of the Council of State (*Raad van State*). E.g Council of State 6 November 2019, ECLI:NL:RVS:2019:3754, nr. 8.

In another case, the Court of Appeal of The Hague (*Gerechtshof Den Haag*) was a bit more lenient and held that the data subject can have other interests, but only in addition to the purpose of verifying the correctness of the data and lawfulness of the processing:

> "With respect to the fact that [the data subject] may also have had another interest, namely obtaining the data in order to use them in legal proceedings [...] This does not imply that he is abusing this right. After all, under these circumstances it cannot be assumed that [the data subject] is exercising his right for another purpose than that for which it was granted.
>
> [emphasis added]
>
> Court of Appeal of The Hague 31 October 2017, ECLI:NL:GHDHA:2017:3011, nr. 7.

Conclusion

The statements made in paragraph 13 of the Guidelines are at odds with well-established case law in the Netherlands. The footnote placed at the end of paragraph 13 of the guidelines provides for a bit a nuance, but evidently does not sufficiently take into account developments in national case-law.

EXAMPLE 2: SPECIFICATION OF ACCESS REQUESTS

The guidelines

In paragraph 35 the Guidelines discuss access requests:

> Data subjects have the right to obtain, with the exceptions mentioned below, full disclosure of all data relating to them (for details on the scope, see section 4, para. Error! Reference source not found.) [sic]. Unless explicitly requested otherwise by the data subject, a request to exercise the right of access shall be understood in general terms, encompassing all personal data concerning the data subject. Limiting access to part of the information may be considered in the following cases:
>
> [...]
>
> In situations where the controller processes a large amount of data concerning the data subject, the controller may have doubts if a request of access, that is expressed in very general terms, really aims at receiving information on all kind of data being processed or on all branches of activity of the controller in detail. These may arise in situations, where there was no possibility to provide the data subject with tools to specify their request from the beginning or where the data subject did not make use of them. The controller then faces problems of how to give a full answer while simultaneously avoiding the creation of an overflow of information for the data subject that the data subject is not interested in and cannot effectively handle. There may be ways to solve this

> problem, depending on the circumstances and the technical possibilities, for example by providing self-service tools in online contexts (see section 5 on the layered approach). If such solutions are not applicable, a controller who processes a large quantity of information relating to the data subject may request the data subject to specify the information or processing to which the request relates before the information is delivered (see Recital 63 GDPR). This exceptional situation may exist for example in case of a company with several fields of activity or a public authority with different administrative units, if the controller found that numerous data relating to the data subject are processed in those branches as well as in cases where the controller has been collecting data upon frequent activities of the data subject for years.

Comments

The guidelines seem to disregard the fact that in practice many data subject access requests are phrased in very general and broad terms, requesting all personal data processed within the organization of the controller, be it in customer and/or personnel management systems, visitor registration, CCTV systems, back-up tapes, personal email archives of employees working in the organization of the controller, etc.

It goes without saying that complying with such broadly worded requests would require a disproportionate effort by the controller, not only to find the requested data but also to subsequently assess whether copies of such data can be provided without adversely affecting the rights and freedoms of others (Art. 15(4) GDPR).

The solutions suggested by the guidelines, 'self-service tools in online contexts', may work in some instances for some controllers, but definitely not for the majority of them. It seems very impractical, if not completely inconceivable, that most controllers are able to develop and apply tools that allow the data subject access to all systems used by the controller, including visitor registrations, CCTV systems, back-up tapes, etc.

It is exactly for this reason that Dutch courts found that the data subject is required to specify such access requests (cf. Recital 63 GDPR). In many instances they explicitly ruled that access requests cannot be used for so-called 'fishing expeditions'. The controller is only required to provide access to the extent that the data subjects have sufficiently specified their requests.

For instance, already in 2014, the Appeals Court of 's-Hertoghenbosch (*Gerechtshof 's-Hertoghenbosch*) ruled that:

> [Appellants, i.e. data subjects] literally request to order Rabobank [controller] to provide [appellants, i.e. data subjects] with "copies and/or excerpts of all (emphasis added:

court) documents upon which the personal data of [appellants] and/or their companies appear.

The [appellants' i.e. data subjects] request thus relates to a large number of records, while there is no more than a suspicion that the requested records contain more or different personal data of [appellants, i.e. data subjects] than those already provided to them.

This wording is so unspecific that Rabobank [controller] is forced to search through all (digital) documents to be found at its premises, not one excepted, in order to select those documents in which (each time) at least one of the personal data of [appellants, i.e. data subjects] appears, and to incur costs in that respect.

With this the Court of Appeal is of the opinion that the access request from the [appellants] is so unspecified that it should be considered as an inadmissible 'fishing expedition.

This means that, in so far as Rabobank [controller] had not yet complied with the request, the requests of [appellants, i.e. data subjects] must be rejected because of their indeterminacy."

[emphasis added]

Appeals Court 's-Hertoghenbosch, 11 December 2014, ECLI:NL:GHSHE:2014:5221, overw. 7.12.5-9.

In that specific case, the data subject submitted an appeal to the Supreme Court (*Hoge Raad*). The Supreme Court did not review this case for procedural reasons (ECLI:NL:HR:2016:508). However, in his opinion Advocate-General Wuisman explained that is his view the appeal was unfounded:

"[W]ith the term 'fishing expedition' the Court of Appeal does not intend to indicate more than that the request of the applicant [i.e. data subject] is too extensive and consequently it would be too costly to search through all documents present at Rabobank, including documents of a digital nature. And that, in all reasonableness, cannot be required of Rabobank [controller]"

[emphasis added]

AG Wuisman van 15 January 2016, ECLI:NL:PHR:2016:1, nr. 2.9.1

Moreover, four years later the same Appeals Court ruled similarly:

> "In the case at hand, there is no concrete and – also in the light of the information already provided – further substantiated request. This implies that the Court of Appeal also considers the present case to be a case of a 'fishing expedition', since [the appellant, i.e. data subject] has (or at least should be deemed to have) only made a general request without even the slightest clarification as to what he, given the information already provided to him [...], wishes to have more clarity about."
>
> Appeals Court 's-Hertoghenbosch, 1 February 2018, ECLI:NL:GHSHE:2018:363, nr. 3.7.6.

Many other judgments contain similar considerations. For instance, in its judgment of 20 June 2019, the District Court of Amsterdam found that

> "the access request is worded so broadly that it is too indefinite to be complied with."

And also that:

> "fully complying with [the applicant's, i.e. data subjects'] request for all processed personal data [...] would not only be almost practically impossible but would also entail a far too extensive and thus costly search by the [controller]."
>
> [emphasis added]

Interestingly, the 'layered approach' suggested by the Guidelines is to some extent already applied by some Dutch courts, inter alia by the District Court of Midden-Nederland:

> In the case of a broadly formulated access request, the [controller] can, in principle, only be required to perform a general search for the most common personal data (including name and address details). This is different in the case of a more specifically formulated request. In such a situation [the controller] can be required to conduct a more thorough investigation. In the plaintiff's [i.e. data subject's] case there was a very generally formulated request. Therefore, contrary to the plaintiff's [data subject's] opinion, there was no reason for the [controller] to also search for other – less obvious – personal data [..]"
>
> District Court of Midden-Nederland 15 June 2020, ECLI:NL:RBMNE:2020:2222, nr. 12

Conclusion

Evidently, the approach suggested by the Guidelines substantially deviates from the approaches adopted by courts in the Netherlands.

EXAMPLE 3: VERIFICATION OF DATA SUBJECT'S IDENTITY

The Guidelines

In instances where the controller has reasonable doubts concerning the identity of the natural person making the access request, the controller may request the provision of additional information necessary to confirm the identity of the data subject (Art. 12(6) GDPR). The Guidelines (particularly para. 73) are right to emphasize that using a copy of an identity document (ID) as a part of the authentication process creates a risk for the security of personal data and may lead to unauthorized or unlawful processing. However, subsequently the Guidelines assert that such using copies should be considered inappropriate and therefore, according to the Guidelines, controllers must implement:

> "a quick and effective security measure to identify a data subject who has been previously authenticated by the controller, e.g. via e-mail or text message containing confirmation links, security questions or confirmation codes."

Comments

Obviously, if the data subject's identity has already been authenticated by the controller, the suggested authentication methods will be preferable to the copy-of-an-ID method. However, the real issue is of course how the controller can verify the data subject's identity in cases where that data subject has *not* already been authenticated. In some instances, possibly the controller could rely on other trusted third parties, for example by asking the data subject to transfer a small sum (e.g. one euro cent) to the bank account of the controller. In other instances, this will not be feasible and other methods need to be applied.

In the Netherlands, there are more than a couple of relevant judgments of the Council of State (*Raad van State*) on this issue. In one, the Council of State ruled that a controller, a municipality, was allowed to request a copy of an ID card:

> "[I]n principle, the municipality has discretionary powers with regard to the manner in which it wishes to establish the identity of the applicant. That discretionary power is determined on the one hand by the principle that the identity must be established properly. On the other hand, it is determined by the fact that establishing the applicant's [i.e. data subject's] identity must not be so prohibitive as to infringe upon the right of the individual to apply freely to the municipality with an access request. The basic principle of requesting a copy of an identity document when requesting access is not considered unreasonable. This guarantees proper identification without infringing on the right of data subjects to apply freely to the municipality".
>
> [emphasis added]

Council of State 9 December 2020, ECLI:NL:RVS:2020:2833, nrs. 5.1-5.2.

On the same day, in another judgment the Council of State found that the controller, another municipality, could not require the data subject to come in person to city hall for identification:

> "The municipality routinely asks individuals who submit a request to erase personal data to stop by the town hall to identify themselves. For [the appellant, i.e. data subject], who lives on the other side of the country, this means that he would have to travel very far. There were other possibilities in this case to establish identity, which would create a lower threshold. For example, the submission of a copy of a passport is in principle considered a reasonable measure to verify identity. See the judgment of today, ECLI:NL:RVS:2020:2833. [The appellant, i.e. data subject] had submitted a copy of an authenticated copy of his passport. The municipality could verify his identity on the basis of this. […] Therefore, the college's demand in this case was not a reasonable measure. The District Court was wrong in finding that the Board could reasonably have required [appellant] to visit the town hall."
>
> [emphasis added]
>
> Council of State 9 December 2020, ECLI:NL:RVS:2020:2915, nr. 5.1; *Cf.* Council of State 9 December 2020, ECLI:NL:RVS:2020:2927, nrs. 6.1-6.3

Conclusion

The Guidelines rightly emphasize that there are security risks connected to the use of a copy of identification documents for authentication purposes. However, the Guidelines do not really have feasible suggestions for alternative authentication methods—in particular in cases where the data subject's identity has not already been verified. Therefore, in view of the judgments of the Council of State (*Raad van State*) and taking into account that many controllers will not have alternative authentication methods, the Guidelines would be more useful if they explain in more detail how such security risks can be mitigated.

FINAL REMARKS

As explained in the introduction, in view of the timeframes set by the Board for this consultation, this note cannot provide for a complete analysis of established national member state case-law. However, it can be expected that further legal analysis of relevant case law in the Netherlands and other member states will reveal many more instances where the guidelines deviate from national courts' case-law. Notably, the guidelines seem to deviate from numerous national court decisions on requests for access to internal and external correspondence (including e-mail and

text messages) and documents prepared for internal discussion purposes, on opinions and views on individuals expressed in documents, the rights and freedoms of others, including economic interests.

Et cetera.

The Hague Leiden Geneva, March 9, 2022

---

[1] Cf. Zanfir-Fortuna, Comments on Art. 15 GDPR, in Kuner et al (eds.), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press 2018, p. 451-452.

[2] College B&W van Rotterdam v. Rijkeboer, Case C- 553/07, Judgment of 7 May 2009, ECLI:EU:C:2009:293.

[3] YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S, Joined Cases C- 141/ 12 and C- 372/ 12, Judgment of 17 July 2014, ECLI:EU:C:2014:2081.

[4][4] Nowak v. Data Protection Commissioner, Case C- 434/ 16, Judgment of 20 December 2017, ECLI:EU:C:2017:994.

[5] All judgements are in Dutch. The texts quoted in this document are the author's (informal) translations.