ECLI:NL:RBAMS:2023:5074

Authority	Amsterdam Court
Date of decision	10-08-2023
Date of publication	17-08-2023
Case number	AMS 22/5458
Areas of law	Administrative law
Special features	First instance - plural
Content indication	DPG Media B.V. (DPG) has been fined by the Authority Personal Data Protection Authority (AP) for breaching Article 12(2) of the General Data Protection Regulation (GDPR). The violation consists of the fact that DPG asked data subjects who made a request outside DPG's online login environment, namely via the online contact form, by mail or by letter, to exercise their right to inspect or erase their personal data, to confirm their identity with a copy of their ID by default and in advance. DPG appealed to the court. The court ruled that there was a breach of Article 12(2) of the AVG. DPG used too rigid a procedure for identifying data subjects, which in any case created an unnecessary obstacle in advance. The court found that AP was not entitled to impose the fine in this case under these specific circumstances. The appeal is upheld.
Findings	Rechtspraak.nl

Excerpt

AMSTERDAM COURT

Administrative law

Case number: AMS 22/5458

judgment of the multiple chamber of 10 August 2023 in the case between DPG

Media B.V., established in Amsterdam, plaintiff (DPG)

(Agents: [name 1] and [name 2]),

and

Personal Data Authority, defendant

(Agents: [name 3] and [name 4]).

Process

By decision of 14 January 2022 (the primary decision), the defendant imposed a fine of €525,000 on DPG for breaching Article 12(2) of the General Data Protection Regulation (GDPR).[1]

By decision of 4 October 2022 (the contested decision), the defendant declared DPG's objection to that decision unfounded.

DPG filed an appeal. The defendant filed a statement of defence.

The hearing took place on 29 June 2023. DPG was represented by its authorised representatives, mr. van der Velde (lawyer), mr. van Breda (head of legal affairs of DPG), mr. Heerink (lawyer at DPG). The defendant was represented by its agents.

Considerations

Background

1. DPG is - among other things - a publisher of magazines, journals and books. DPG acquired Sanoma Media Netherlands B.V. (Sanoma) on 1 October 2021. These proceedings focus on the period when Sanoma was still independent, before the acquisition by DPG. The court will hereinafter always refer to "DPG", even if it was Sanoma at the time.

2. DPG processes personal data, such as the name, address and place of residence of clients who, for example, have taken out a subscription to one of the magazines published by DPG. In that context, DPG may also have financial data, such as a bank account number.

3. On 29 January 2019, the DPG received a request from the Respondent for information on its current policy on requests for access and/or erasure of personal data, where a copy of an identity document was requested. This was prompted by five complaints the defendant had received in the period from September 2018 to January 2019.

4. On 18 February 2019, DPG provided a written explanation. Subsequently, on 3 July 2019, the defendant requested DPG to respond to the individual complaints. DPG responded to the complaints on 17 July 2019.

5. On 7 October 2021, the defendant sent DPG the '*Investigation Report on Requesting a Copy ID in Requests for Inspection or Deletion at DPG Media Magazines B.V., formerly Sanoma Media Netherlands B.V.*' dated 29 September 2021. In that report, the defendant concluded that

DPG with its policy and its active promotion of it hindered the right of inspection and erasure, thereby creating unnecessary barriers to the exercise of these rights. For this reason, according to the defendant, there was a violation of Article 12(2) of the AVG during the period from May 2018 to 18 June 2021.

6. By letter dated 7 October 2021, the defendant sent an intention of enforcement to DPG, giving it the opportunity to submit an opinion. DPG submitted a view on 16 November 2021, after which the defendant issued the primary decision on 14 January 2022.

Decision-making defendant

7. In the primary decision, upheld in the contested decision, the defendant imposed an administrative fine of €525,000 on DPG. The defendant bases this on the fact that DPG breached Article 12(2) of the AVG. The violation consists of the fact that DPG asked data subjects who made a request outside the online login environment of DPG, namely via the online contact form, by mail or by letter, to exercise their right to inspect or delete their personal data, by default and in advance to confirm their identity with a copy of their identity document. DPG made this request without assessing beforehand whether the relevant requester could be identified in another, less intrusive way. With this practice, according to the defendant, DPG did not facilitate the exercise of the right to inspection and erasure by the standards of Article 12(2) of the AVG. The defendant saw no reason to deviate from the basic penalty.

DPG position

8. DPG argues, in brief, that the defendant erred in concluding that DPG's practice constituted a violation of Article 12(2) of the AVG, because the defendant misinterpreted the article's standard. DPG's policy further did allow for customisation, which was put into practice. Examples of this can be found in the investigation report. DPG further argues that the imposition of the fine violates the *lex certa principle*. Finally, DPG argues that the imposition and level of the administrative fine violates the principle of proportionality.

Court assessment

9. In this case, the court assesses whether the defendant was entitled to impose the fine. The court does so on the basis of DPG's grounds of appeal.

Article 12(2) of the AVG

10. The court first notes that the fine as imposed by the defendant relates specifically to the policy on requests for access or erasure of personal data, which were made outside the login environment of DPG. It is established between the parties that the vast majority of requests for access or erasure were made within the login environment. The defendant has no comments with regard to the handling of those requests. The question at issue in these proceedings is whether the defendant was right to take the position that, with its policy with regard to requests made outside the login environment, DPG did or did not sufficiently facilitate the exercise of the rights of data subjects within the meaning of Article 12(2) of the

AVG. To this end, the court first discusses what DPG's policy on this point entailed and what the term 'facilitation' means within the meaning of Article 12(2) of the AVG.

11.1. DPG's policy on requests outside the login environment at the time was that - in a nutshell - a copy of identity proof was requested by default and in advance for every request. This is evident, among other things, from the privacy statement then in the court file. Upon receiving a request to inspect or delete personal data, DPG always asked for a copy of an identity document. If the request was submitted via the online form, this occurred automatically. If the request was submitted by e-mail, an e-mail was returned by DPG requesting a copy of an identity document. A request was not processed until a copy of an identity document was provided. The privacy statement and procedure were on DPG's website and DPG confirmed in the letter dated 17 July 2019 that it used this procedure. The privacy statement further stated that a protected copy, where the Citizen Service Number and photograph had been made unrecognisable, could be provided and was sufficient. DPG did not explicitly mention this possibility yet in cases where it asked an applicant to send a copy of the identity document after the applicant did not send a copy with the contact form.

11.2. For the interpretation of the term 'facilitate' in Article 12(2) of the AVG, the court looks to the preamble of the AVG, in particular recitals 59 to
64. Partly against this background, the court reads the regulation as meaning that 'facilitating' means that a data controller must provide an arrangement that allows for the exercise of the rights under the AVG, such as the right of inspection and erasure, on the understanding that there must be no unnecessary impediments to the exercise of these rights. The Respondent rightly pointed out that, in addition, there is an obligation on the controller to verify the identity of the person requesting access. The controller must take all reasonable measures to this end. This will be a barrier, but it should not be unnecessary. The principles of proportionality, subsidiarity and data minimisation will have to be observed when making and implementing the arrangements.

12. The court therefore finds, that there is an area of tension regarding the 'facilitation' of the right of inspection and the obligation of identification. After all, under the AVG, DPG is obliged to give applicants access to the personal data processed about them, whereby no unnecessary obstacles may be created, but at the same time DPG is obliged to identify applicants, to prevent personal data being provided to the wrong person (data breach), which can be obstructive. It is not possible to draw a rigid line, applicable to all cases, in advance, between what is and is not allowed in this context in fulfilling the identification obligation and what should be considered unnecessarily obstructive and what is not. On this point, as considered above, the principles of proportionality, subsidiarity and data minimisation come into play. Among other things, this depends on what personal data an organisation processes. It is undisputed between the parties - and the court assumes as well - that more sensitive data must be safeguarded with more security measures.

13. Against this background, the court considers the following regarding DPG's policy on requests for access or erasure outside the login environment.

14. The court shares DPG's view that a copy of an identity document is not in itself an unreasonable means of identifying a person. This has also been confirmed by the Administrative Law Division of the Council of State (the Division).[2] However, in the cases referred to here, DPG always asked for a copy of the proof of identity and did not process a request as long as no copy had been provided. This while - as discussed at the hearing - it was not in all cases about (very) sensitive personal data of DPG's clients and it was in

at least in some of the cases, it was also possible to achieve identification of applicants by other, less intrusive, means than providing a copy of an identity document (such as identification via e-mail, which was later introduced as a standard arrangement). It must be assumed that the identity document to be provided also often contained more personal data than necessary to identify the applicant, such as a Citizen Service Number, a photograph and a document number. This is not in line with the principle of data minimisation. Although the privacy statement stated that the Citizen Service Number and photograph could be shielded, DPG did not mention this possibility if it requested a copy of an identity document.

15. In the court's view, DPG's policy thus did not provide sufficient scope to meet the requirements of proportionality and subsidiarity. In the District Court's opinion, DPG applied too rigid a procedure for identifying applicants, which created an unnecessary obstacle in advance for at least some of the requests. It was found that in practice, there did exist more room when applicants, after making the request, proceeded to complain that they had to provide a copy of their proof of identity. In the court's view, however, that was too late. DPG could and should have designed its process so that there was more scope at an earlier stage to take into account all relevant circumstances, including the nature of the request and the information sought. For example, in the case of a simple request to stop receiving promotional material, requiring a (shielded) copy of identity proof as a condition for considering that request will usually not be proportionate and subsidiary. The procedure should be flexible enough to make such a request more approachable.

16
The court therefore concludes that DPG's policy does not comply with the provisions of Article 12(2) of the AVG.

17. In doing so, the court did not follow the claimant's reliance on the *lex certa principle*. According to established case law of the Division, the *lex certa principle*, which is enshrined in, inter alia, Article 7 of the ECHR, requires the legislator, with a view to legal certainty, to define the prohibited conduct as clearly as possible.[3] In this respect, it should not be lost sight of the fact that the legislator sometimes defines prohibited conduct with a certain vagueness, consisting of the use of general terms, in order to prevent conduct worthy of punishment from falling outside the scope of that description. Such vagueness may be unavoidable, because it is not always foreseeable in what way the interests to be protected will be violated in the future and because, if it is foreseeable, the descriptions of prohibited conduct would otherwise become too refined, with the result that clarity is lost and the interest of the general clarity of legislation suffers as a result.

18. In this case, in the court's view, there is no violation of this principle. The legislator of the AVG had to keep the text sufficiently general to make it usable by all controllers and processors. Although the standard of Article 12(2) of the AVG is open-ended, the standard is not so unclear as to violate the *lex certa principle*. It should have been clear to DPG that the policy in this rigid form could not meet the requirements of proportionality, subsidiarity and data minimisation.

<u>The plea and the amount of the fine</u>

19. Under Article 83(5) of the AVG, the Respondent is authorised to impose a fine for a breach of Article 12 of the AVG. Pursuant to the Fines Policy of the Personal Data Authority (Fines Policy), the breach of Article 12(2) of the AVG falls under Category III. The basic Category III fine is €525,000.[4] When imposing a fine, the defendant must take a number of factors into account. These factors are listed in Article 83(2) of the AVG and Article 7 of the Fines Policy.

20. According to established case law of the Division,[5] when applying the power to impose a fine, an administrative body must adjust the amount of the fine to the gravity of the offence and the extent to which it can be b l a m e d on the offender. In doing so, the circumstances under which the offence was c o m m i t t e d must be taken into account. This is regulated in Article 5:46(2) of the General Administrative Law Act. The defendant has adopted policy rules setting o u t the penalty amounts for the offences. Even if the court has not found the policy unreasonable, when applying it in an individual case, the defendant must assess whether that application is in line with the aforementioned legal requirements for the exercise of the fining power. Always, with regard to the fine, if necessary in addition to or contrary to the p o l i c y , it must be d e t e r m i n e d that it i s proportionate. The court reviews the decision without restraint.

21. The court considers that the defendant should not have r e a c h e d the imposition of the fine in this case without further ado. In the court's view, the defendant did not sufficiently consider the circumstances below.

22. The objective of the AVG is to protect personal data. The identification requirement also serves this purpose. DPG, when making the policy, gave an interpretation of this duty of identification t o ensure that the person making a request is the data subject within the meaning of the AVG. In doing so, it did not treat its duties as a data controller lightly, but merely misjudged t h e required balance between data protection and facilitating other rights under the A V G . To that extent, serious culpability cannot be said to exist. As stated in recital 14
stated, moreover, according to the Division, a copy of an identity document is in itself a good means of identifying someone.

23. In addition, the AVG had only recently come into force during the period at issue, on 25 May 2018. The defendant took action below by email of

29 January 2019 first contacted DPG, to which DPG responded on 18 February 2019. After 18 February 2019, DPG then heard nothing for some time, after which the defendant asked her on 3 July 2019 to respond specifically to the five complaints the defendant had r e c e i v e d . After DPG complied with this request on 17 July 2019, DPG did not hear back until

21 October 2021 only again from the defendant, when it sent the draft report. The court considers that the defendant could have entered into the conversation at an earlier stage and at least suggested that the policy be a m e n d e d . This is all the more urgent as DGP had already explicitly raised the question in its letter of 18 February 2019 as to whether it could continue its policy in this way, while the defendant, especially in the period immediately after the AVG came into force, had also assumed an informative role as a supervisory authority. DPG had also already disclosed its policy in its initial response of 18 February 2019 to such an extent that the defendant could have plainly found already at that time that, in its opinion, the policy violated the provisions of Article 12 of the AVG. A s a result, the protracted nature of the breach referred to by the defendant cannot be held against DPG. In addition, the court also notes that DPG had already changed the policy of its own accord at the time the draft report appeared. From 17 December 2020, DPG no longer routinely and in advance asked for a copy of ID. Although the privacy statement did not change until October 2021, the court finds that the change on 17 December 2020 meant that a copy of I D was no longer requested by default and in advance.

24. Finally, the court considers it important that DPG's policy received a much broader range of requests than the part to which the present decision relates. As already considered, the file and the proceedings at the hearing show that in the vast majority of cases, namely when a data subject requested inspection or erasure of personal data within the login environment, there w a s no violation of Article 12(2) of the AVG. The

involves a relatively small number of requests in this case. Moreover, the defendant has not established in how many of those cases the policy actually led to an unnecessary obstacle in practice, because asking for a copy of the identification document would actually not have been necessary, and in how many cases DPG would have had good grounds to do so. That there was more than a minor breach of the AVG cannot, in the court's view, be established against the background of all the above.

25. In imposing the fine, the defendant did not pay sufficient attention to the aforementioned circumstances. The court held that in view of all these circumstances taken together, the defendant should not have imposed a fine. Perhaps the circumstances could give reason to impose an alternative measure as referred to in Article 58(2) of the AVG, but the Court leaves this further open. It is for the Respondent to consider whether there might still be reason to do so.

Conclusion

26. In view of what has been considered regarding the plea and the level of the fine, the court will uphold the appeal. The court shall set aside the contested decision and revoke the primary decision insofar as it imposed the fine. The court determines that this judgment replaces the decisions to that extent.

27. Declaring the appeal well-founded, the court ordered the defendant to reimburse DPG for the court fees paid by it in the amount of €365.

28. The Court ordered the defendant to pay the legal costs incurred by DPG. Pursuant to the Administrative Costs Decree, the Court fixed these costs at € 1,674 (one point for lodging the notice of appeal, one point for appearing at the hearing, with a value per point of € 837 and a weighting factor of one) for the legal assistance provided by a third party in a professional capacity.

Decision

The court:

- Declares the appeal well-founded.
- Annuls the contested decision insofar as it imposes a fine and revokes the primary decision insofar as it imposed a fine.
- determines that this judgment supersedes.
- orders the defendant to reimburse DPG for the court fee of €365 paid.
- order the defendant to pay the applicant's legal costs in the amount of

€ 1.674,-.

This judgment was delivered by S.D. Arnold, chairman, and M.F. Ferdinandusse and A.K. Glerum, members, in the presence of K.M. Nannan Panday, registrar.

The decision was pronounced in public on 10 August 2023.

registrar

president

is prevented from signing the judgment

Copy sent to parties on:

Legal remedy

An appeal against this ruling may be lodged with the Administrative Jurisdiction Division of the Council of State within six weeks from the date of its dispatch.

If an appeal has been lodged, an application can be made to the appellate court for interim relief.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] See the Division ruling of 9 December 2020, ECLI:NL:RVS:2020:2833, recital 5.2 and the Division ruling of 8 June 2022, ECLI:NL:RVS:2022:1608, recital 4.1.

[3] See, for example, the Division's ruling of 17 April 2019, ECLI:NL:RVS:2019:1235.

[4] Article 2 of the Fines Policy.

[5] See, for example, the Division's decision of 27 January 2021, ECLI:NL:RVS:2021:170, recital 5.1.