Confidential/Registered

DPG Media Magazines B.V.

attn. the board

PO Box 1900

2130 JH Hoofddorp

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

Decision to impose a fine

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authority data.nl

Dear Sir / Madam,

The Dutch Data Protection Authority (AP) has decided to contact DPG Media Magazines B.V. (DPG) a

administrative fine of € 525,000. The AP has come to the conclusion that DPG with its policy

and its active propagation has hindered the right of access and erasure of data subjects.

DPG has raised unnecessary barriers to exercising these rights. Because of this,

DPG acted in violation of Article 12, second paragraph, of the General Data Protection Regulation

(GDPR).

The AP explains the decision in more detail below. Chapter 1 is an introduction and chapter 2 contains the facts.

In Chapter 3, the DPA assesses whether personal data is being processed, the processing responsibility and the violation. In chapter 4 the (height of the) administrative fine and Chapter 5 contains the operative part and the remedies clause.

1

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

1 Introduction

1.1 Organization involved

This decision relates to DPG Media Magazines B.V. (DPG), located at Capellalaan 65 te Hoofddorp.1 DPG is a media house that publishes and exploits magazines, magazines and books. on April 20 2020 is the statutory name of Sanoma Media Netherlands B.V. changed to DPG Media Magazines B.V.2 DPG's activities have remained unchanged.

In the period from May 2018 to January 2019, the AP received complaints about the conduct of DPG with requests for access to and requests for erasure of personal data of data subjects (hereinafter: 'complainants'). According to the complainants, DPG asked for a copy of the complainants' ID for verification of their identity, as a condition for (further) processing their request for access or deletion.

The AP subsequently investigated DPG's policy regarding retrieval and processing of a copy of the proof of identity with submitted requests for access to or deletion of personal data. The AP focused the investigation solely on DPG's policy and conduct with regarding access and deletion requests that are made outside the secure login environment of an account DPG were submitted. This concerns requests that data subjects receive by letter, e-mail or via a web form submitted. DPG's policy and course of action with regard to requests that were submitted within an account's digital login environment, fell outside the scope of the research.

1.2 Process

During the investigation, the AP requested information from DPG and the complainants. The AP also has DPG requested to respond separately to the complaints concerned. DPG complied with these requests.

In a letter dated October 7, 2021, the AP sent DPG an intention to enforce and underlying report with findings. On 16 November 2021, DPG sent a letter to this effect point of view. Finally, at the request of the AP, DPG has additional information on December 16, 2021 provided.

1 Chamber of Commerce number: 33133064.

2 Where necessary, reference will be made to Sanoma Media Netherlands B.V.

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

2. Facts

2.1 Customer data

DPG published magazines to which customers could take out a subscription. DPG sent to as a result of subscriptions concluded for this purpose, magazines to its customers. In this context it had the name, address and residence details of its subscribers. Also DPG about financial data (bank details) of its subscribers.3 From persons who had subscribed to a newsletter or who had applied for a School Desk account4, DPG about at least part of this data, such as a name and e-mail address.

In the complainants' matters, it appears that DPG approached the complainants in several ways:

- Some complainants had (had) a subscription with DPG;
- One complainant also had or had an account with Schoolbank.nl and;
- One complainant indicated that he was not a subscriber, but only advertised (for Libelle, among others).

received at her home address, presumably after leaving contact details with a

DPG website or magazine.

2.2 Digital customer database

DPG supplied products to its customers mainly by sending (among other things) magazines.

In this context, DPG used the aforementioned data to send these products by post or e-mail.

to be able to send e-mail. The same applied to the advertising printed matter that DPG sent.

DPG has stated to the AP that it stores the data in a digital customer database.5 This is also apparent

from the fact that an online profile of the data subject could be created using this data. See

for this the printout below from the website of DPG.6

3 AP research report of September 29, 2021, p. 5.

4 The online platform www.schoolbank.nl was owned by DPG until 2020.

5 AP research report of September 29, 2021, p. 4 and 6.

6 AP research report of September 29, 2021, p. 5.

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

2.3 DPG . Privacy Policy

The privacy policy stated that the privacy policy applied to the processing of data

by, among others, Sanoma Media Netherlands B.V. (now: DPG) and that Sanoma Media Netherlands B.V.

was the controller for the processing of personal data for its Dutch

brands (including the Belgian activities of VT Wonen).7

2.4 Policy regarding access and removal requests

2.4.1. The general working method of DPG in the research period

Data subjects can request access and erasure from DPG as referred to in Articles 15 and 17 of the GDPR

Submit. Data subjects can submit these requests in two ways:

1) The most common way was by submitting such a request within the digital login environment of a DPG account of the data subject. As stated in section 1.1 of this decision, this method fell outside the scope of the investigation, as this method of submission no copy of ID was requested.

2) Another way, which this decision does refer to, was to submit a request for access to and deletion of personal data outside the login environment of the account. This could be done through an online form on the DPG website (then www.sanoma.nl), by e-mail or by letter.8

When processing requests for access to and erasure of data, DPG used:

personal data submitted outside the login environment of an account the following standard method.

Upon receipt of a request for access to or erasure of personal data, DPG asked the data subject always ask for a copy of an identity document. If the data subject had a request via the online form submitted, were immediately automatically asked to provide a copy of an identity document provide. If the request was submitted by e-mail, an e-mail was sent by DPG with the request to provide a copy of the identity document. DPG indicated that a request only treatment was taken, after a copy of an identity document was provided.9

7 AP research report of September 29, 2021, p. 6-7.

8 AP research report of September 29, 2021, p. 7.

9 Ditto.

When asked, DPG described this standard procedure towards the AP as follows. "When

someone via our online contact form asks for access to and/or deletion of the data we have from
have processed that person, the request for an email will automatically appear in the contact form
to send a copy of identification along with the request.
The request remains open pending the copy of the identity document. As soon as we receive a . from an applicant
have received a copy of proof of identity and the applicant's details correspond to the
data of the customer registered with us, we will carry out the request for deletion. Applicant
will then also receive confirmation of the processing of the request submitted by him."
DPG also indicated in its privacy statement that in such a case it was always asked for a copy of
a (valid) proof of identity to identify the applicant.10 DPG stated in its privacy
statement and on the website section that contained Q&As about – among other things – privacy the following:11
In the communication DPG had with the complainants after receipt of the digital requests for access and
deletion, shielding the copy was also not indicated by DPG as a possibility.12 This in
unlike requests submitted by post, where DPG stated in its privacy statement
that a protected copy (where, among other things, the citizen service number and photo become unrecognizable
made) was sufficient.13
DPG has stated that on the basis of Article 12, sixth paragraph, of the GDPR it felt entitled to
to establish the identity of those involved by means of a copy of an identity document, before DPG
proceeded to grant access to or delete the personal data of the
person concerned.14
Only if it has been established on the basis of a copy of an identity document that the person concerned was the person who
requested, this request was complied with. DPG therefore stated – in cases where a
request was submitted outside the login environment – the identity of the person concerned is only fixed on
based on a copy of the identity document to be provided.
10 AP research report of September 29, 2021, p. 8.
11 Ditto.
12 AP research report of September 29, 2021, appendix 1, always under A and E.

13 AP research report of 29 September 2021, appendix 4 'Sanoma website'.

14 AP research report of September 29, 2021, p. 8.

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

DPG did not have any other means of establishing the identity, she stated. In all cases, after
receipt of the request asked for a copy of the identity document. This was necessary according to DPG
to prevent data from ending up with a person who does not have access to this information
data should be available.15

When asked, DPG indicated that in the period from January 1, 2019 to June 1, 2019, it had approximately 11,000 customer
questions and
received customer requests related to the subject of privacy, and that the majority of these
requests for erasure. According to DPG, approximately 9,400 of these requests were processed within the secure
login environment of an account (in which case no copy of the proof of identity was required)
are provided) and only a small number of deletion requests were made outside the login environment
submitted, i.e. approximately 60 requests.16

2.4.2 DPG's general working method after the statutory name change as of April 20, 2020

In its investigation, the AP concluded that the method with regard to asking a
copy of an identity document with a request for access to or erasure of personal data -submitted
outside the login environment of an account- since the statutory name change is on April 20, 2020
continued.17 On June 18, 2021, the AP also determined that the privacy and cookie policy of DPG
it is indicated that DPG asks for a valid proof of identity from the person who wants his rights
exercise.18

In response to DPG's view, the AP has determined that DPG will not

longer asks for a copy of an identity document when requesting access to or erasure of

personal data outside the login environment of an account. DPG has since sent a verification email to

to be able to establish the identity of an applicant.19 DPG has prepared its privacy statement in accordance with

adapted this new method and published on October 18, 2021.20

2.4.3 The complaints

The AP received five complaints about the way in which DPG responded to requests for access to or deletion

of personal data. These five complainants all had a request for access to or deletion of

personal data done at DPG by means of the online contact form or by e-mail. One complainant

DPG requested access to personal data and four complainants requested erasure of their

personal data.21

15 AP research report of September 29, 2021, p. 8.

16 AP research report of September 29, 2021, p. 9.

17 Ditto.

18 AP research report of September 29, 2021, p. 9 and Appendix 7.

19 Letter of 16 December 2021 from DPG to the AP, answer to the AP information request of 25 November 2021.

20 DPG opinion of 16 November 2021, p. 11; Letter of 16 December 2021 from DPG to the AP, answer to AP information

request

from November 25, 2021; https://privacy.dpgmedia.nl/document/privacystatement.

21 AP Research Report of September 29, 2021, p. 9.

In all cases, DPG - immediately after the submission of the request by the complainants - to the complainants

requested to provide a copy of an identity document as a condition for (further) in

processing the submitted requests.22

Four complainants did not comply with DPG's request for proof of identity. DPG subsequently did not process these deletion requests. A number of complainants had already DPG indicated that they were not willing to provide a copy of their ID because they considered this to be 'too heavy'.23 One complainant did send a copy of an identity document to DPG. However, this complainant did not receive inspection from DPG after sending a copy of the proof of identity. DPG indicated that the copy of the ID was inadvertently not linked to the account of the complainant and again asked for a copy of proof of identity. After this, the complainant lodged a complaint with the AP.24

2.4.4 DPG's working method with regard to complaints during the investigation period

At least four of the complaints submitted showed that DPG, in the cases where no copy of the proof of identity was provided, did not comply with the requests submitted for erasure of personal data. DPG subsequently did not (further) process the requests.25 This method also finds support in DPG's statement at the time of the investigation:

“The moment someone asks via our online contact form for access to and/or removal of the data that we have processed from that person, then the contact form will automatically appear in the contact form request to send a copy of identification along with the request. (…)

If a request for inspection and/or removal is sent without a copy of proof of identity, the customer service in response to the applicant. (…)

The request remains open pending the copy of the identity document. As soon as we receive a . from an applicant have received a copy of proof of identity and the applicant's details correspond to the data of the customer registered with us, we will carry out the request for deletion. Applicant will then also receive confirmation of the processing of the request submitted by him. (…)”26

22 See also paragraphs 2.4.1 and 2.4.2.

23 AP research report of September 29, 2021, p. 10.

24 AP research report of September 29, 2021, p. 10.

25 Ditto.

26 Ditto.

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

3. Review

3.1 Personal data and the controller

DPG processed, among other things, its name, address, place of residence and/or e-mail address
customers/subscribers for one of DPG's Dutch brands, or of persons who have an account
had on Schoolbank.nl. With this data, DPG was able to identify natural persons. DPG processed
thus personal data within the meaning of Article 4(1) of the GDPR.

The AP has further established that the privacy policy stated that Sanoma Media Netherlands B.V.
was the controller for the processing of the personal data for the Dutch
brands and that the privacy policy applied to all DPG products and services. In the
privacy policy also included how a data subject could access his data and how a
data subject could have his data deleted.

Furthermore, it appears from statements by DPG that it actually acted as the person responsible for the purpose and the means
certain for the processing of personal data in relation to submitted requests for access to and
erasure of personal data. It is apparent from these statements that DPG independently determined which
data had to be provided by applicants for access and erasure requests (substance) and
why those data had to be provided (purpose).27

In view of the foregoing, the AP establishes that DPG is the controller within the meaning of Article
4, section 7, of the GDPR for the processing of personal data relating to the submitted
requests for access to and erasure of personal data.

3.2. Facilitate rights of data subjects

3.2.1 Legal framework

Pursuant to Article 12, paragraph 2, of the GDPR, the controller must exercise

facilitate the data subject's rights under Articles 15 to 22 of the GDPR. It

right of access to personal data (Article 15 of the GDPR) and the right to erasure

personal data (Article 17 of the GDPR) are included.

Recital 59 of the GDPR clarifies the standard in Article 12 of the GDPR:

Arrangements should be in place to enable the data subject to exercise his rights under this Regulation

easier to exercise, such as mechanisms to request, in particular, access to, rectification or erasure of

personal data and, if applicable, obtain it free of charge, as well as to exercise the right of objection. […]

27 AP research report of September 29, 2021, appendix 1, always under E.

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

Recital 63 of the GDPR states, among other things:

A data subject must have the right to access the personal data collected about him and to exercise that right

easily and at reasonable intervals, so that he can become aware of the processing and the

can verify its legitimacy. […]

Based on the above, the controller must have an arrangement to

enable data subjects to exercise their rights more easily and simply. A

The controller may not create unnecessary barriers for data subjects to

to exercise the aforementioned rights. When a controller has a policy that the

hinders the exercise of the aforementioned rights and actively promotes this policy, there may be

violation of Article 12, second paragraph, of the GDPR.28

Verifying the identity of a natural person who makes a request for access or erasure is

an indispensable section of a regulation within the meaning of Article 12, second paragraph, of the GDPR. A

after all, the controller is obliged to ensure appropriate security of the

personal data processed by it, including against unauthorized or unlawful processing.29

In addition, when verifying the identity of an applicant, the controller must

observe the principle of data minimization as referred to in Article 5(1)(c) of the GDPR.

It follows that when verifying the applicant's identity in the context of the exercise

of his/her rights, the personal data requested by a controller is adequate

should be relevant and limited to what is necessary for the purposes for which they are

incorporated. In doing so, the principles of proportionality and subsidiarity must be observed.

The requested data to verify the identity of the applicant must be proportionate

to the purpose to be served by the processing (proportionality). And this goal can not be less

disadvantageous, less intrusive way (subsidiarity).

It is disproportionate to require a copy of an identity document if the identity of the person concerned

can be verified in another way. In addition, the processing of copies of

identity documents pose a major risk to the security of personal data. In addition, the

controller cannot be sure that the copy is authentic and the owner of the

identity card is actually the applicant, for example through (unauthorized) access to

identity cards by housemates and forged copies of identity cards.

All of the foregoing amounts to a controller's policy regarding

to exercise the rights of data subjects must be arranged in such a way that a data subject is at least

must be identified in a significant manner. And that this policy is geared to (among other things) the risk to the

28 See also ECLI:NL:RBGEL:2020:3159, recitals 9.7 and 9.8.

29 See Article 32 of the GDPR.

rights and freedoms of persons, also in view of the nature and amount of data of which access or deletion is requested and the context in which the request is made. In many cases this will mean that as much as possible primarily on the basis of personal data that controller has already processed, the identity of the requester can be established. Should a controller, despite the initial request and by the data subject, personal data provided still have reasons to doubt the identity of the natural person person making the request, the controller may, pursuant to Article 12, sixth paragraph, of the GDPR, ask the data subject for additional information. Article 12, sixth paragraph, of the GDPR sees therefore mainly on individual cases, in which there are reasons to doubt the identity. In that case, Article 12(6) of the GDPR allows a controller to request additional information necessary to establish the applicant's identity, provided he can demonstrate that he cannot verify the identity of the data subject without additional information. But here too, the controller may only request (additional) information that is necessary. Here too, the above-mentioned principles of proportionality and subsidiarity.

3.2.2. Rating

The AP has established in chapter 2 that DPG always requests a copy outside the login environment of accounts of an identity document.30 DPG made this request regardless of any (contact) information at DPG was available about the data subject and without regard to the nature and quantity personal data of which access or erasure has been requested. Furthermore, DPG's working method was arranged that if a copy of the identity document was not provided by the person concerned, the request for inspection or erasure was not (further) processed for that reason. If the person concerned does provided a copy of the identity document, this meant that DPG was unnecessarily sensitive to

was processing data (such as the citizen service number).

In view of the above legal framework, any regulation regarding the exercise of

rights of data subjects are arranged in such a way that a data subject must behave in the least intrusive manner

can identify. In the opinion of the AP, this means that DPG will inform a data subject as much as possible

primarily on the basis of personal data that DPG must already identify. An example

this may be a subscriber/customer number in combination with a name and address and/or e-mail address of

a petitioner.

Now that DPG required a copy of an identity document from those involved as standard without first checking

to check whether DPG (already) had other (identifying) (contact) information and without account

taking into account the nature and amount of personal data, the DPA is of the opinion that data subjects do not

could easily and simply claim their rights under the GDPR. With others

30 For example, via an automatic request that appeared in the contact form or a follow-up e-mail.

words, DPG did not ask for a copy of the ID based on a concrete assessment

per individual case as referred to in Article 12(6) of the GDPR. But DPG asked in advance for a

copy of ID, as this was current policy. This DPG policy and actively promoting it

of it on, among other things, the website and through DPG's customer service, ensured that a

unnecessary barrier was created around the submission of requests for access to and erasure of

personal data.

DPG's policy has also in practice – with regard to complainants – hindered the

requests for inspection and erasure.31 It appears from the complaints submitted that this working method of DPG

resistance, which resulted in the complainants (in a number of cases) being unwilling to

provide a copy of their ID. Refusal to provide a copy of the identity document

As a result, DPG did not (further) comply with the requests of a number of complainants for that reason took treatment. The policy and its implementation by DPG therefore threw up with regard to those complainants actually constitute an obstacle to the exercise of the right of access or erasure.

In particular, the AP would like to point out that the condition used by DPG to submit a copy of an identity document with a request from a data subject was disproportionate to the nature and amount of personal data about which a request has been made. In addition, organizations may only process the Citizen Service Number if this is stipulated in a specific law. When requesting a copy of the proof of identity is all the more important, because the central government recommends: to be careful when providing (protected) copies of the identity document. This document contains sensitive personal data. The combination of data listed on the proof of identity also makes identity fraud possible. The AP also points out on its website that it is providing a copy of an identity document poses a risk.32

3.3 DPG opinion and AP . response

DPG has put forward a view on the investigation findings of the AP. The AP puts the DPG's view is briefly described below, accompanied by a response from the AP.

3.3.1 Need for copy of identity document

In its view, DPG states that the identity of a small group of those involved cannot be determined by personal security credentials, as the information they provide not already verified/linked to information in DPG's systems (because they are not logged in). A the applicant who submits a request for access or erasure outside the secure environment must therefore provide additional information. In this way DPG can verify and demonstrate that this person has a right to inspect or delete the personal data (i.e. qualifies as a

31 See section 2.4.3.

32 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/identiteitsgedrag.

data subject) and DPG has a legal basis to process any personal data it processes on
delete or provide this requester's request (i.e. determine whether the requester has the
is who it claims to be).

As long as DPG cannot establish the identity of the applicant, the GDPR does not apply according to DPG
application.33 For the processing of the GDPR request, it is sufficient for DPG to indicate that it is unable to
establish the identity of the applicant and request additional information. That last one right
compliance with Article 12, second paragraph, second sentence, of the GDPR.

DPG also deems it necessary to request a copy of proof of identification. According to DPG, on this
effectively limits the risk that DPG will provide a copy of the personal data or
remove personal data from the 'wrong' data subject, which would entail a violation of
Article 6 of the GDPR. The use of a copy of your identity document is the least intrusive way to
identity and is also geared to the real risk to the rights and
freedoms of persons.34 Without a copy of proof of identity, the identity of an applicant cannot be
DPG cannot be (properly) established and DPG may not be established pursuant to Articles 5 and 6 of the
GDPR refuse to comply with such requests as desired by the requester.

The AP does not follow DPG's view. The AP emphasizes that in this decision it has assessed on
how DPG has facilitated the rights of data subjects and not whether certain individuals ultimately
could or could not be identified. The case law cited by DPG in which a decision was made
on the identification of an individual under Article 15 of the GDPR and 35 of the Protection Act
personal data (Wbp) is therefore not considered relevant by the AP in this case. That a copy of a
proof of identity may be necessary in an individual case between a citizen and the government, makes
It does not mean that asking for this in advance is necessary in all cases.

The AP further disagrees with DPG's statement that it is necessary in all cases to make a copy to obtain the identity document from the applicant. It is in the way of DPG to check yourself first find out what information it already has about the applicant. If no less intrusive means of identification is possible, a controller may request a protected to show proof of identity. DPG itself also stated during the investigation that in some cases a customer can already identify on the basis of name and address, sometimes additional information such as subscriber number or e-mail address is necessary.35 In addition, DPG currently uses the adjusted method whereby a verification email is sent to verify the identity of a requester determine. Processing copies of identity documents containing sensitive data such as the Citizen Service Number, photo, height and nationality in this case is contrary to the principle of

33 DPG refers to ECLI:NL:RBOVE:2021:1296, r.o. 8.

34 DPG refers to ECLI:NL:RVS:2020:2833, r.o. 5.2.

35 AP research report of September 29, 2021, appendix 1, always under E.

data minimization and lawfulness (Article 5(1)(c) and Article 6 of the GDPR). That DPG at has required a copy of the - moreover unprotected - proof of identity in advance to processing a request does not facilitate the exercise of the rights of involved.

3.3.2 Facilitating the concept

DPG indicates that the AP states in its investigation report that Article 12, second paragraph, of the GDPR means that the controller should facilitate the exercise of data subjects' rights to make. However, DPG is of the opinion that the AP has not been proved right in this explanation in an AP

cited judgment of a preliminary relief judge. According to DPG, 'facilitation' entails that a
controller does not (unnecessarily) hinder the exercise of these rights and 'possibly'
should make'.36 DPG further states that the Belgian GDPR supervisor in its Dutch-language
sample letter for GDPR requests has included as standard that data subjects have a copy of the
can send an identity card. Finally, DPG accuses the AP that it did not (explicitly) distance itself earlier
has made a point of view in a letter from a case from 2003 from its legal predecessor the College
protection of personal data (CBP).37

The AP does not agree with DPG's view. First, in its investigation report, the AP has identified the
The relevant ruling of the Gelderland District Court is cited as an example in another statement.
Namely in case a controller has a policy that the exercise of the aforementioned
hinders rights and also actively promotes this policy, there is a violation of Article 12, second paragraph,
of the GDPR.38 Secondly, the relevant preliminary relief judge also discussed whether 'facilitation'
making 'easier' includes not considered relevant in that case, because impediment is in any case not possible
are regarded as facilitating the right of access.39 The AP is therefore based on Article 12,
second paragraph of the GDPR and recitals 59 and 63 of the GDPR consider that "facilitation" should be understood as such
that the controller should have an arrangement in place to enable data subjects to
allow their rights to be exercised unimpeded, easier and simpler.

The AP is also of the opinion that the quotes quoted by DPG from a CBP letter from 2003 constitute a unilateral
evoke the contents of that letter. In this letter, the Dutch DPA rejects a request for mediation between
two parties. The Dutch DPA has considered that when determining the identity, the nature of the data

36 DPG refers to ECLI:NL:RBGEL:2020:3159, r.o. 9.8.

37 DPG quoted the following from this letter: "In the opinion of the Dutch DPA, the importance of properly determining the
the applicant's identity cannot be set aside too quickly in favor of a faster or easier treatment of a
access request. […] In certain cases (such as in this case) the person concerned does not want to send a copy of the identity
document because there
personal data. If the person concerned does not want to send a copy of an identity document, there is always the possibility

that

the person concerned or his authorized representative shows the identity document on site to the responsible person and in this way obtains access.

[…] It is also conceivable that [the controller] will be satisfied with a copy of a passport on which, for example, the social security number has been defaced."

38 ECLI:NL:RBGEL:2020:3159, r.o. 9.7.

39 ECLI:NL:RBGEL:2020:3159, r.o. 9.8.

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

and of the processing are important. The CPB has also stated that in the event of a written request for inspection by a lawyer a copy of the lawyer's identity document is in principle not necessary under Article 37, second paragraph, of the Wbp. It is also an option for the data subject or his authorized representative to show proof of identity to the person responsible on site, according to the CPB. Finally it had, - in view of the long time elapsed since 2003, on the road from DPG to come into force of the GDPR as of May 24, 2016 and its entry into force as of May 25, 2018 (again) from the applicable law. to ascertain and act in accordance with regulations; all the way now far-reaching digitized society (fifteen years later) has unfortunately entailed that the providing personal data is not without risk. The AP has been indicating on its website for some time now: extensive information about the rules for identification.40 A Belgian model letter, where, incidentally, a protected copy if an option is given next to, for example, an assigned customer number, do not off.

3.3.3 Method of identification

DPG does not agree with the statement of the AP included in the investigation report that DPG is outside a

copy of the identity document had no other means of establishing the identity. Those involved could, according to DPG, choose to submit a request via his/her account. In addition, according to DPG, the procedure is that if the applicant refused to provide a copy of proof of identity, the privacy officer was consulted and a copy of ID was deemed unnecessary when verification of identity could take place in another way. Finally, DPG states that through its former privacy statement has actively promoted the policy to use a protected copy of ID.

The AP also does not follow this view of DPG. If data subjects do not contact us via the contact form or by e-mail want to provide a copy of their identity card, then they should not be forced to do so to create an account on the DPG website. This is also an (unnecessary) obstacle for data subjects to exercise their rights under the GDPR. That at a later stage internally at DPG consultation with the privacy officer took place, as DPG states but does not substantiate with evidence, the AP . considers not relevant for the assessment of the policy propagated by DPG to those involved in advance conducted. Incidentally, this statement does not correspond with what DPG stated during the investigation about its policy.

Finally, the AP cannot follow DPG in the statement that it has actively propagated the policy of using making a protected copy of identity document. DPG has stated in its privacy statement that only with requests by post a protected copy is sufficient. Via the contact form, e-mail and in the case that a person involved refused to provide a copy of an identity document, DPG has no idea pointed out that it was a protected copy. This also follows from the communication submitted between DPG and complainants.

40 https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/identificatie/identiteitsgedrag.

Date

January 14, 2022

Our reference

3.3.4 Article 12, sixth paragraph, of the GDPR

DPG finds the statement of the AP included in the investigation report that a

controller the identity of the requester (for access or erasure) “beyond reasonable doubt”

want to determine to prevent a data breach or abuse of rights, an incomplete, incorrect

interpretation of the GDPR. The 'reasonable doubt' test of Article 12, sixth paragraph, of the GDPR comes, according to DPG

does not arise if the controller cannot identify the requester at all

determine.

The AP does not follow DPG's argument. If the controller is unable to verify the identity

of a data subject, he shall inform the data subject thereof. When the data subject

does not subsequently provide additional data that would allow it to be identified, then its article

15 to 20 of the GDPR do not apply in that case. Although for another reason, the

AP concluded that Article 12, sixth paragraph, of the GDPR in the present assessment of the violation

is not relevant.

3.3.5 Complaints

DPG believes that the AP wrongly included five complaints in its investigation and assessment.

The complaints do not relate, or not sufficiently, to the findings of the AP on the basis of which they

violation finds that DPG is acting in violation of Article 12, second paragraph, of the GDPR. DPG requests the

AP therefore does not include these complaints in an enforcement decision.

The AP will not grant this request. The communication between the complainants and DPG reflects

the way in which DPG has implemented its policy on the rights of data subjects. Out of every complaint

it appears that Sanoma, or parts that fell under Sanoma, at the time for the processing of a

request required a copy of the ID and that the complainants see this as an obstacle

experienced.

3.4 Conclusion

The AP comes to the conclusion that at the time of the infringement, DPG was not sufficiently exercising its rights

of stakeholders has facilitated. As a result, DPG acted in violation of Article 12, second paragraph, of the GDPR.

4. Fine

4.1 Introduction

DPG has acted in violation of Article 12, second paragraph, of the GDPR. The AP makes for the established violation of its power to impose a fine on DPG. Given the seriousness of the violation and the extent to which it can be blamed on DPG, the AP considers the imposition of a fine appropriate. The AP justifies this in the following.

4.2 Fine policy rules of the Dutch Data Protection Authority 2019

Pursuant to Article 58, second paragraph, preamble and under i and Article 83, fifth paragraph, of the GDPR, read in in connection with article 14, third paragraph, of the UAVG, the AP is authorized to give DPG in the event of a violation of Article 12 of the GDPR to impose an administrative fine of up to € 20,000,000 or, for a company, up to 4% of total worldwide annual turnover in the previous financial year, whichever is higher.

The AP has established fine policy rules regarding the interpretation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.41 In the Fines policy rules have been chosen for a category classification and bandwidth system.

Violation of Article 12, second paragraph, of the GDPR is classified in category III. Category III has a fine range between €300,000 and €750,000 and a basic fine of €525,000.

4.3 Fine amount

4.3.1 Seriousness of the violation

Under the principle of transparency, the controller should exercise the

facilitate the rights of the data subject. It is essential for data protection that data subjects
an easy way to exercise their rights under the GDPR. As a result, the data subject is
enabled to easily take cognizance of which personal data a
controller processed. A proper interpretation of the right of access is also necessary
to exercise other rights, such as the right to rectification and the right to erasure.
In its view, DPG states that a balancing of the interests in this case should at most lead to a
reprimand. If it concerns a minor infringement, the AP can opt for a fine instead of a fine
reprimand. In view of the present violation, however, in the opinion of the AP there was a
serious infringement, in which DPG has insufficiently facilitated the rights of data subjects. The AP considers it
41 Stcrt. 2019, 14586, March 14, 2019.

Date
January 14, 2022
Our reference
[CONFIDENTIAL]
the imposition of a reprimand is therefore insufficiently effective, disproportionate and also not a deterrent.
The AP justifies this as follows.
With regard to the nature of the infringement, the AP weighs heavily that regardless of any (contact) information
was available to DPG about the data subject, DPG did not process the requests if the
the person concerned did not provide a copy of the identity document. As a result, those involved not only had to
provide a lot of personal data, but also very sensitive personal data such as a photo and
Citizen service number. Data subjects should not be urged to share personal data
that are not necessary for the exercise of their rights under the GDPR.
Also the systematic – and therefore not incidental – nature of the violation in which DPG has long and
has systematically (actively) propagated its policy, the AP takes into account when determining the seriousness of the
offence. Although DPG no longer asks for a copy of an identity document as of December 17, 2020,

DPG did not adjust its privacy policy on the website until October 18, 2021. As for the
size of the number of affected data subjects, the AP takes into account that the number of data subjects
was limited in relative terms, but extensive in absolute terms. From a sample over a period of 6
months it turned out that it concerned 60 people involved. Given the duration of DPG's working method of 25
May 2018 until October 2021, the AP believes that it must be several hundred people involved
gone. These data subjects, as well as other persons affected by this policy and through various
DPG's means of communication waived their rights, were therefore unnecessarily impeded in the
exercising their rights under the GDPR. DPG's policy has resulted in data subjects who
did not provide their copy of their identity document, were unable to access their
personal data or have not been able to have their personal data deleted.
Based on the above, the AP is of the opinion that there is a serious violation, based on
of which a basic fine of € 525,000 is appropriate. In this case, the AP sees no reason to impose the basic fine
to increase or decrease.

4.3.2 Blame and proportionality

Pursuant to Article 5:46, second paragraph, of the Awb, when imposing an administrative fine, the AP
into account the extent to which this can be blamed on the offender.
DPG argues that it cannot be blamed for the violation, because DPG's actions
compliance with the GDPR. This argument cannot succeed. From absence of culpability is
no way. Now that this is a violation, the AP is allowed to impose an administrative fine
in accordance with established case law presuppose culpability if the perpetrator has been established. DPG has
actively pursued policies that violated the GDPR. DPG has failed to amend that policy in line with the
guarantees that the GDPR gives to, among other things, the right of access and erasure. The AP considers this
blameworthy.

Date

January 14, 2022

DPG further states in its view that it would be contrary to the lex certa principle if the AP would impose a punitive sanction based on open standards. The AP does not follow DPG's view. It hinder the exercise of the rights referred to in Articles 15 to 22 of the GDPR in no case be regarded as facilitating those rights. The legal text of the GDPR, recital 59 and 63 of the GDPR and provide the detailed information about the rules for identification on the AP website sufficient clarity. A professional market party such as DPG may be expected to duly verified of the standards that apply to it and, above all, that it complies with them.

Finally, pursuant to Articles 3:4 and 5:46 of the Awb, the AP assesses whether the application of its policy for determining the amount of the fine in view of the circumstances of the specific case, not to a disproportionate outcome.

The AP is of the opinion that (the amount of) the fine is proportionate.42 In this opinion, the AP has, among other things: the seriousness of the infringement and the extent to which it can be held against DPG are taken into account. Because of the nature of the personal data, the duration of the violation and the consequences of DPG's policy for data subjects, the AP qualifies this breach of the GDPR as serious. Given the financial size of DPG the AP finds the amount of the fine appropriate and deterrent.

In view of the foregoing, the AP sees no reason to set the amount of the fine on the basis of proportionality and the circumstances referred to in the Penalty Policy Rules, to the extent applicable in the present case, increase or decrease.

4.4 Conclusion

The AP sets the total fine at € 525,000.

42 For the motivation, see paragraphs 4.3.1 and 4.3.2.

Our reference

[CONFIDENTIAL]

5. Operative part

The AP explains to DPG Media Magazines B.V. due to violation of Article 12, second paragraph, of the GDPR a administrative fine in the amount of:

€ 525,000 (in words five hundred and twenty-five thousand euros).43

Yours faithfully,

Authority Personal Data,

w.g.

ir. M.J. Verdier

Vice President

Remedies Clause

If you do not agree with this decision, you can return it within six weeks of the date of dispatch of the decide to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. In accordance with Article 38 of the UAVG suspends the effect of the decision to lodge a notice of objection imposition of the administrative fine. For submitting a digital objection, see www.autoriteitpersoonsgegevens.nl, under the heading Objecting to a decision, at the bottom of the page under the heading Contact with the Dutch Data Protection Authority. The address for paper submission is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague.

State 'Awb objection' on the envelope and put 'objection' in the title of your letter.

In your notice of objection, write at least:

- your name and address;
- the date of your notice of objection;
- the reference mentioned in this letter (case number); or attach a copy of this decision;
- the reason(s) why you do not agree with this decision;
- your signature.

43 The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (CJIB). The fine must be in accordance with

Article 4:87(1) Awb to be paid within six weeks. For information and/or instruction about payment, please contact be recorded with the aforementioned contact person at the AP.