Confidential/Registered

DPG Media Magazines B.V.

Attn. the board

Post box 1900

2130 JH Hoofddorp

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Subject

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

authoritypersonal data.nl

Ir/Madam,

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

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

and actively promoting it has hindered the right of access and data erasure of data subjects.

DPG has created unnecessary barriers to the use of these rights. This has

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 AP assesses whether personal data is being processed, the

controller and the violation. In chapter 4 the (level of the) administrative

penalty worked out and chapter 5 contains the operative part and the remedy 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 in

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 May 2018 through 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 an identity document from the complainants for

verification

of their identity, as a condition for (further) processing their request for access or erasure.

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 exclusively on DPG's policies and practices

with regard to access and erasure requests that are made outside the secure login environment of an account

DPG were submitted. This concerns requests made by the data subject by letter, by e-mail or by e-mail

web form submitted. DPG's policies and practices regarding requests that

were submitted within the digital login environment of an account were outside the scope of the

research.

1.2 Process flow

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

In a letter dated October 7, 2021, the AP sent DPG an enforcement intention and attached it basis report with findings. On November 16, 2021, DPG has issued a written response to this viewpoint given. Finally, DPG has additional information at the request of the AP 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 that context it had the name, address and place of residence of its subscribers. Also had DPG about financial data (bank details) of its subscribers.3 Of persons who had registered registered for a newsletter or who had applied for a Schoolbank account4, DPG about at least part of this data, such as a name and e-mail address.

In the complainants' cases, it appears that DPG approached the complainants in different ways:

- Some complainants had (had) a subscription with DPG;
- One complainant also had (had) an account with Schoolbank.nl and;

- One complainant indicated that he had not been 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 in particular by sending (among other things) magazines.

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

to be able to send 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 also appears

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

printout below from the DPG.6 website

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

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

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

6 AP research report of 29 September 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 responsible for the processing of personal data for her Dutch

brands (which also included the Belgian activities of VT Wonen).7

2.4 Policy Regarding Access and Deletion Requests

2.4.1. DPG's general working method during the research period

Data subjects can request access to 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, since in this method of no copy of ID was requested.

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

DPG used when processing requests for access to and deletion of personal data submitted outside of an account login environment 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 ID. If the data subject had a request via the online form submitted, you were immediately automatically asked for a copy of an identity document provide. If the request was submitted by e-mail, DPG sent an e-mail with it request to provide a copy of the ID. DPG indicated that a request will only be submitted in treatment was taken after a copy of an identity document was provided.9

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

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

9 Ditto.

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

When asked, DPG described this standard procedure towards the AP as follows. "When
someone asks via our online contact form to inspect and/or delete the data that we hold
have processed that person, the request for a
send a copy of proof of identification with the request.
The request remains open pending the copy of proof of identity. As soon as we receive a request from an applicant
have received a copy of proof of identity and the details of the applicant correspond to the
data of the customer registered with us, we will carry out the request for deletion. Applicant
will subsequently also receive confirmation of the processing of the request submitted by him."
DPG also indicated in its privacy statement that in such a case 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 that DPG had with the complainants after receiving the digital requests for inspection and
deletion, protecting the copy was also not indicated by DPG as a possibility.12 This in
unlike requests submitted by post, which 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, based on Article 12, paragraph 6, of the GDPR, it felt entitled to continue
to establish the identity of those involved by means of a copy of an identity document, before DPG
proceeded to provide access to or delete the personal data of the
data subject.14
Only if it was established on the basis of a copy of an identity document that the person concerned was the one who made the
requested, this request was executed. DPG therefore stated – in the event that a
request was submitted outside the login environment – the identity of the data subject is solely fixed on
on the basis of a copy of the proof of identity to be provided.
10 Research report AP of 29 September 2021, p. 8.
11 Ditto.

12 AP research report of 29 September 2021, appendix 1 always under A and E.

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

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

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

DPG did not have other ways of establishing 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 access requests from ending up with a person who does not have this information
information should have been available.15

When asked, DPG indicated that in the period from January 1, 2019 to June 1, 2019, it received approximately 11,000
customer questions and
received customer requests related to the topic of privacy, and that the majority of them
erasure requests. According to DPG, approximately 9400 of these requests were made within the secure
login environment of an account (in which case there was no need to provide a copy of the proof of identity
are provided) and only a small number of deletion requests were made outside the login environment
submitted, namely approximately 60 requests.16

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

In its investigation, the AP has concluded that the method of requesting a
copy of proof of identity submitted with a request for access to or deletion of personal data
outside the login environment of an account - since the statutory name change on April 20, 2020
continued.17 On 18 June 2021, the AP also established that DPG's privacy and cookie policy
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 opinion, the AP has determined that as of December 17, 2020 DPG is not
no longer asks for a copy of proof of identity when requesting access to or deletion of
personal data outside the login environment of an account. DPG has since sent a verification email
to be able to establish the identity of an applicant.19 DPG has adopted its privacy statement accordingly
adapted this new working method and published on October 18, 2021.20

2.4.3 The complaints

The AP received five complaints about the way in which DPG interpreted requests for access to or erasure
of personal data. These five complainants all requested access to or erasure of
personal data submitted to DPG by means of the online contact form or by e-mail. One complainer
requested DPG to access personal data and four complainants requested their erasure
personal data.21

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

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

17 Ditto.

18 Research report AP of 29 September 2021, p. 9 and appendix 7.

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

20 Opinion DPG of 16 November 2021, p. 11; Letter dated 16 December 2021 from DPG to the AP, response to AP
information request
from November 25, 2021; https://privacy.dpgmedia.nl/document/privacystatement.

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

In all cases, that applied to DPG – immediately after the submission of the request by the complainants – to the complainants

requested the provision of a copy of an identity document as a condition for (further) registration

handle the requests submitted.22

Four complainants did not respond to DPG's request to provide proof of identity. DPG

subsequently did not process these deletion requests. A number of complainants had already applied directly

DPG indicated that they were not willing to provide a copy of their ID because they

considered this to be an 'excessive remedy'.23 One complainant did send a copy of an identity document to DPG.

However, this complainant did not receive any inspection from DPG after sending a copy of the proof of identity.

DPG indicated that the copy of the ID was mistakenly not linked to the account of the

complainant and asked again for a copy of ID. Subsequently, the complainant submitted a complaint to the AP.24

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

At least four of the complaints submitted showed that DPG, in cases where no copy of the

proof of identity was provided, did not comply with the requests submitted for deletion of

personal data. DPG subsequently did not (further) process the requests.25 This working method

also finds support in DPG's statement at the time of the investigation:

“The moment someone requests access to and/or removal of the

data that we have processed from that person, the contact form will automatically appear in the contact form

request to send a copy of identification with the request. (…)

If a request for inspection and/or deletion is sent without a copy of proof of identity, the

customer service in response to the requester. (…)

The request remains open pending the copy of proof of identity. As soon as we receive a request from an applicant

have received a copy of proof of identity and the details of the applicant correspond to the

data of the customer registered with us, we will carry out the request for deletion. Applicant

subsequently also receives confirmation of the processing of the request submitted by him. (…)”26

22 See also sections 2.4.1 and 2.4.2.

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

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

25 Ditto.

26 Ditto.

Date

January 14, 2022

Our reference

[CONFIDENTIAL]

3. Assessment

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 the Dutch brands of DPG, 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 responsible 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 party responsible for the purpose and the means certain for the processing of personal data in relation to submitted requests for access to and deletion of personal data. It appears from these statements that DPG independently determined which data had to be provided by applicants for access and erasure requests (means) and why that information had to be provided (purpose).27

In view of the foregoing, the AP determines that DPG is the controller within the meaning of Article 4, part 7, of the GDPR for the processing of personal data relating to the submitted request 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 monitor the exercise of
facilitate the rights of the data subject 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 further 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 and rectification or erasure of
personal data and, if applicable, to obtain it free of charge, as well as to exercise the right to object. […]

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

Recital 63 of the GDPR states, among other things, the following:

A data subject must have the right to access the personal data collected about him, and to exercise that right
simple and at reasonable intervals, so that he can become aware of the processing and the
check its legality. […]

Based on the above, the controller must have an arrangement to:
enabling data subjects to exercise their rights more easily and simply. A
The controller may not create unnecessary barriers for data subjects to do so
to exercise the aforementioned rights. When a controller has a policy that the
interferes with the exercise of the aforementioned rights and actively propagates this policy, there may be
violation of article 12, second paragraph, of the AVG.28

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

an indispensable paragraph 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 data

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

In addition, when verifying the identity of a requester, the controller must verify the

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

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

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

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

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

The data requested to verify the applicant's identity must be proportionate

to the purpose to be served with the processing thereof (proportionality). And this goal cannot be any less

disadvantageous, less drastic way (subsidiarity).

It is disproportionate to require a copy of an identity document as the identity of the data subject

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

proof of identity poses a major risk to the security of personal data. In addition, the

controller are not sure that the copy is authentic and the owner of the

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

IDs by roommates and counterfeit copies of IDs.

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

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

significant way to identify. And that this policy is geared to (among other things) the risk for the

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

29 See Article 32 of the GDPR.

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

3.2.2. Judgement

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

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

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

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

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

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

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

a petitioner.

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

whether DPG (already) had other (identifying) (contact) information and without taking into account

take into account the nature and amount of personal data, the AP is of the opinion that data subjects do not stop

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 forwarded 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, paragraph 6, of the GDPR. But DPG asked for one in advance

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

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

unnecessary threshold was created around the submission of requests for access and deletion

personal data.

DPG's policy has also hindered the complainants in practice

requests for inspection and deletion.31 The complaints submitted show that this working method of DPG

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

copy of their ID. The refusal to provide a copy of the ID

provision resulted in DPG not (further) responding to the requests of a number of complainants for that reason

took treatment. The policy and its implementation by DPG therefore cast with regard to those complainants

actually constitutes an obstacle to exercising the right of access or erasure.

In particular, the AP would like to note that the condition used by DPG to submit a

copy of proof of identity with a request from a data subject was disproportionate to the nature and

amount of personal data about which a request was made. In addition, organizations

only process the citizen service number if this is stipulated in a specific law. When querying

a copy of the proof of identity emphasizes this all the more, because it is recommended by the national government to

be careful when providing (shielded) copies of the proof of identity. This

after all, the 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

providing a copy of an identity document entails a risk.32

3.3 DPG's view and AP's response

DPG has expressed a view on the research findings of the AP. The AP sets the

DPG's view is briefly explained below, accompanied by a response from the AP.

3.3.1 Necessity of a copy of proof of identity

In its view, DPG states that the identity of a small group of those involved cannot be verified

determined from personal security data, as the information they provide

has not already been verified/linked to information in DPG's systems (because they are not logged in). A

applicant who submits a request for access or deletion outside the secure environment must therefore

provide additional information. In this way, DPG can check and demonstrate that this person has a

appeal to access or delete the personal data (i.e. qualifies as a

31 See section 2.4.3.

32 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/identification/identity-proof.

data subject) and DPG has a legal basis to store any personal data it processes

delete its request or provide it to this requester (i.e. determine whether the requester has the

data subject is who it claims to be).

As long as DPG cannot determine the identity of the applicant, the GDPR is not applicable, according to DPG

application.33 For the handling of the AVG request, it is sufficient that DPG indicates that it is not able to

establish the identity of the applicant and ask for additional information. That last one right there

compliance with Article 12, second paragraph, second sentence, of the AVG.

DPG also considers it necessary to request a copy of proof of identification. According to DPG, this

effectively limits the risk that DPG will provide a copy of the personal data or

deletes personal data of the 'wrong' data subject, which would entail a violation of

Article 6 of the GDPR. The use of a copy of an identity document is the least intrusive way to verify the

identity can be properly established and is, moreover, geared to the real risk to the rights and

freedoms of persons.34 Without a copy of an identity document, the identity of an applicant can according

DPG cannot be (properly) determined and DPG may not be determined on the basis of Articles 5 and 6 of the

AVG refuse to act on 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

were identifiable or not. The jurisprudence quoted by DPG in which judgment has been given

about the identification of an individual in the context of article 15 of the GDPR and 35 of the Protection Act

personal data (Wbp) is therefore not relevant to the AP in this case. That's a copy of one

proof of identity may be necessary in an individual case between a citizen and the government

does not mean that requesting this in advance is necessary in all cases.

The AP further disagrees with DPG's statement that it is necessary in all cases to have a copy of the identity document of the applicant. It is up to DPG to check for itself first what data it already has on the applicant. If no less drastic way of identification is possible, a controller can request a shielded 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 data such as subscriber number or e-mail address necessary.35 In addition, DPG currently uses the modified method in which a verification email is sent to verify the identity of a requester to establish. Processing copies of identity documents containing sensitive data such as the citizen service number, photo, height and nationality is in this case precisely 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 29 September 2021, appendix 1 always under E.

data minimization and lawfulness (article 5, paragraph 1 at sub c and article 6 of the GDPR). That DPG at required a copy of the - moreover non-shielded - proof of identity in advance to be able to do so at all processing a request does not facilitate the exercise of the rights of data subjects.

3.3.2 Facilitating understanding

DPG indicates that the AP states in its investigation report that Article 12, paragraph 2, of the AVG means that the controller should facilitate the exercise of the rights of data subjects to make. However, DPG is of the opinion that the AP has not been proved right in this explanation in an AP

quoted judgment of a preliminary relief judge. According to DPG, 'facilitating' means that a
controller does not (unnecessarily) hinder the exercise of these rights and 'possibly
must make."36 DPG further states that the Belgian supervisor of the GDPR in its Dutch-language
sample letter for GDPR requests included as standard that data subjects receive a copy of the
can send an identity card. Finally, DPG reproaches the AP for not (explicitly) waiving it sooner
has made a point of view in a letter of a case from 2003 from its legal predecessor the Board
personal data protection (CBP).37

The AP does not agree with DPG's view. First, in its investigative report, the AP has
relevant judgment of the District Court of Gelderland cited as an example for another statement.
Namely in case a controller has a policy that restricts the exercise of the said
obstructs 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 has the discussion of 'facilitating'
'making it easier' is not considered relevant in that case, because obstruction is in any case not possible
be 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 believes that 'facilitating' should be understood as
that the controller must have an arrangement in place to enable data subjects
make their rights unfettered, easier and simple to exercise.

The AP is also of the opinion that the quotes from a CBP letter from 2003 quoted by DPG are a unilateral
conjure up an image of the contents of that letter. In this letter, the Dutch DPA rejects a request for mediation between
two parties off. 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 has quoted the following from this letter: "In the opinion of the Dutch DPA, the importance of properly determining the
the applicant's identity should not be too quickly set aside in favor of faster or easier treatment of an applicant
access request. […] In certain cases (such as in this case), the person concerned does not want to send a copy of the proof of
identity because there
personal data. If the person concerned does not want to send a copy of an identity document, there is always the option to do

so

the person concerned or his authorized representative shows the proof of identity on site to the responsible party 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 made illegible."

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

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

and of the processing are important. The CPB has also stated that with a written request for inspection by a lawyer a copy of the lawyer's identity document is in principle not required 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 on site to the person responsible, according to the CPB. Finally, it had - considering the long time that has elapsed since 2003, DPG has been on its way to GDPR as of May 24, 2016 and its entry into force as of May 25, 2018 (again) from the applicable legal and regulations and to act in accordance with them; especially now one more far-reaching digitized society (fifteen years later) has unfortunately meant that the providing personal data is not without risk. The AP has been providing information on its website for some time now extensive information about the rules for identification.40 A Belgian model letter, which incidentally contains a protected copy if an option is given in addition to, for example, an assigned customer number, does that not off.

3.3.3 Method of identification

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

copy of the proof of identity had no other means of establishing the identity. Data Subjects
could, according to DPG, choose to submit a request through his/her account. In addition gold
according to DPG, the working method is that if the applicant refused to provide a copy of proof of identity,
the privacy officer was consulted and a copy of proof of identity was not deemed necessary when
verification of the identity could take place in another way. Finally, DPG states that through its
former privacy statement has actively propagated 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 ID, then they should not be forced to do so
to create an account on the DPG website. This is also an (unnecessary) obstacle to this
data subjects to be able to exercise their rights under the GDPR. This will be done internally at DPG at a later stage
consultation with the privacy officer took place, as DPG states but does not substantiate with evidence, the AP believes
not relevant to the opinion on the policy communicated by DPG to the parties involved in advance
performed. Incidentally, this statement is not consistent with what DPG stated during the investigation
about its policy.

Finally, the AP cannot follow DPG in stating that it has actively propagated the policy to use
make a shielded copy of your ID. DPG has indicated in its privacy statement that
only a protected copy is sufficient for requests by post. Via the contact form, the e-mail and in
DPG does not accept the case that a person concerned refused to provide a copy of an identity document
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/topics/identification/identity-proof.

3.3.4 Article 12, paragraph 6, of the GDPR

DPG believes that the AP's statement included in the investigation report that a
controller the identity of the requester (up to inspection or erasure) “beyond reasonable doubt”
wants to determine in order to prevent a data breach or abuse of rights, an incomplete, incorrect
interpretation of the GDPR. According to DPG, the 'reasonable doubt' test of Article 12, paragraph 6, of the GDPR comes
does not apply if the controller cannot verify the identity of the applicant at all
to establish.

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
thereafter does not provide any additional data that would make it possible to identify him, other than his article
15 to 20 of the GDPR do not apply in that case. Admittedly, for another reason, the
AP concludes that Article 12, paragraph 6, of the GDPR in the present assessment of the violation
is irrelevant.

3.3.5 Complaints

DPG believes that the AP wrongly included five complaints in its investigation and assessment.
The complaints are not or insufficiently related to the findings of the DPA on the basis of which they made the complaint
violation establishes that DPG is acting in violation of Article 12, paragraph 2, 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 is a reflection of
the way in which DPG has implemented its policy on the rights of data subjects. From every complaint
it appears that Sanoma, or parts that fell under Sanoma, were charged at the time for handling a
request a copy of the identity document required and that the complainants have this as an obstacle
experienced.

3.4 Conclusion

The AP comes to the conclusion that DPG was insufficiently exercising its rights at the time of the infringement

of those involved 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 authority to impose a fine on DPG. Given the seriousness of the violation and the extent to which this can be attributed to DPG, the AP deems the imposition of a fine appropriate. The AP motivates this in the following.

4.2 Penalty Policy Rules of the Dutch Data Protection Authority 2019

Pursuant to Article 58, second paragraph, opening words and under i and Article 83, fifth paragraph, of the GDPR, read in connection with Article 14, third paragraph, of the UAVG, the AP is authorized to inform 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 the total worldwide annual turnover in the previous financial year, whichever is higher.

The AP has established Fining Policy Rules regarding the implementation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.41 In the Penalty 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 bandwidth between €300,000 and €750,000 and a basic fine of €525,000.

4.3 Fine amount

4.3.1 Severity of the Violation

In the context of the transparency principle, the controller must monitor the exercise of the

facilitating rights of the data subject. It is essential for data protection that data subjects have access to an easy way to exercise their rights under the GDPR. As a result, the data subject enters enabled to easily find out which personal data a processed by controller. Proper implementation of the right of inspection is also necessary to be able to exercise other rights, such as the right to rectification and the right to erasure.

In its opinion, DPG states that a weighing 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, the AP is of the opinion that there was a serious infringement, in which DPG has insufficiently facilitated the rights of those involved. The AP considers it

41 Stct. 2019, 14586, March 14, 2019.

imposing a reprimand is therefore not effective, proportionate or dissuasive.

The AP motivates this as follows.

With regard to the nature of the infringement, the AP weighs heavily that regardless of any (contact) information was available at DPG about the data subject, DPG would not process the requests if the the person concerned did not provide a copy of the proof of identity. As a result, those involved did not have to go alone provide a lot of personal data, but also very sensitive personal data such as a photo and the Citizen service number. Data subjects should not be urged to provide 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 is protracted and has systematically (actively) disseminated its policy, the AP takes into account in 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 accordingly 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 limited in relative terms, but extensive in absolute terms. From a sample over a period of 6 months it turned out that 60 people were involved. Considering the duration of DPG's method of 25 May 2018 to October 2021, the AP is of the opinion that it must be several hundred people involved gone. These data subjects, as well as other persons affected by this policy and through various communication means of DPG waived their rights, were therefore unnecessarily hindered in the exercising their rights under the GDPR. DPG's policy has resulted in those involved have not provided their copy of their ID, have not been able to inspect their personal data or have not been able to have their personal data removed.

Based on the above, the AP is of the opinion that there has been a serious violation, on grounds 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 Section 5:46(2) of the Awb, when imposing an administrative fine, the AP take into account the extent to which this can be attributed to the offender.

DPG argues that it cannot be blamed for the violation, because DPG's conduct has damaged the overall compliance with the GDPR. This argument cannot succeed. Of absence of culpability is no way. Since this is a violation, the AP is allowed to impose an administrative fine in accordance with established case law, assume culpability if the perpetrator is established. DPG has actively pursued a policy that was in conflict with the GDPR. DPG has failed to adapt that policy to the guarantees that the AVG gives to, among other things, the right of inspection and data erasure. The AP considers this culpable.

Date

January 14, 2022

DPG also states in its view that it would be contrary to the lex certa principle if the AP would impose a punitive sanction on the basis of open norms. The AP does not follow DPG's view. It hindering the exercise of the rights as referred to in Articles 15 to 22 of the GDPR can be under no circumstances be regarded as facilitating those rights. The legal text of the GDPR, recital 59 and 63 of the GDPR and provide detailed information about the identification rules on the AP website sufficient clarity. A professional market party such as DPG can be expected to thoroughly ascertained the standards applicable 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 one 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 attributed to 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 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, insofar as applicable in the foregoing case, increase or decrease.

4.4 Conclusion

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

42 For the motivation, see sections 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, paragraph 2, of the AVG a

an administrative fine in the amount of:

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

Yours faithfully,

Authority for Personal Data,

e.g.

ir. M.J. Verdier

Vice President

Remedies Clause

If you do not agree with this decision, you can within six weeks from the date of sending it

decides to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. In accordance

Article 38 of the UAVG suspends the effect of the decision until submitting a notice of objection

imposition of an 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 submission on paper

is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague.

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

Write in your notice of objection at least:

- your name and address;

- the date of your objection;

- the reference referred to in this letter (case number); or enclose a copy of this decision;

- the reason(s) why you disagree with this decision;

- your signature.

43 The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (CJIB). The fine should be accordingly

Article 4:87, first paragraph, Awb must be paid within six weeks. For information and/or instructions about payment, please contact

be recorded with the previously mentioned contact person at the AP.