

Confidential/Registered

Foundation Support Provincial

Fraction Overijssel Party for Freedom

[CONFIDENTIAL]

Steenmeijerstraat 57

7555 NV HENGELLO

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Subject

Decision to impose an administrative 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

Dear [CONFIDENTIAL],

The Dutch Data Protection Authority (hereinafter: AP) has decided to support the Provincial Support Foundation Overijssel Party for Freedom (PVV) (hereinafter: PVV Overijssel) an administrative fine of € 7,500 to be imposed. The AP is of the opinion that the PVV Overijssel in the period from January 14, 2019 to has today failed to commit a personal data breach without undue delay and no later than 72 hours after the PVV Overijssel became aware of the infringement on January 11, 2019, in report to the AP. The PVV Overijssel thus has Article 33, first paragraph, of the General Regulation

Data protection (hereinafter: AVG) violated.

The decision is explained below. Chapter 1 contains the relevant facts and the course of the proceedings. In Chapter 2 describes the legal framework. In chapter 3 follows the assessment of the AP, after which in chapter 4 the amount of the administrative fine is motivated. Finally, chapter 5 contains it operative part and the remedies clause.

1. Facts and procedure

Foundation Support Provincial Party Overijssel Party for Freedom (PVV) has its registered office at Steenmeijerstraat 57, 7555 NV in Hengelo. The foundation has, among other things, the granting of managerial and administrative assistance to the Group (as referred to in Article 5 of the Rules of Procedure of order for the meeting and other activities of the Provincial Council of Overijssel or a

1

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

regulation that replaces it) has the purpose.¹ The foundation also acts under the name 'PVV Overijssel'.²

On January 11, 2019, the AP received a complaint about a possible violation of the GDPR by the PVV Overijssel.³ The complaint means, in short, that on 10 January 2019 the PVV Overijssel received an e-mail message with "Invitation of the supporters evening January 28, 2018" as subject to a group of 101 recipients. In doing so, all recipients of the e-mail message, including the complainant, the list of recipients visible in the mailing list of the e-mail program.

In response to this complaint, the AP has launched an investigation to determine whether the rules contained in the GDPR are set around reporting a personal data breach are complied with by the PVV Overijssel.

In a letter dated 15 May 2019, the AP requested information from the PVV Overijssel.⁴ The PVV Overijssel has

responded in writing to this request on 24 May 2019.⁵

The findings of the investigation are set out in the report 'Investigation not reporting infringement in connection with personal data to the AP by the PVV Overijssel', research report of the department Primary Care Examination (EL), dated November 18, 2019.

In a letter dated December 11, 2019, the AP has an intention to enforce the PVV Overijssel sent together with the aforementioned research report and the underlying documentation, whereby the PVV was also given the opportunity to express its views. The PVV Overijssel has letter dated 28 January 2020 expressed its view in writing.

Based on the report with findings, the underlying documentation and the opinion of the PVV Overijssel, the AP has established the following relevant facts.

A fraction employee of the PVV Overijssel sends an e-mail message on Thursday, January 10, 2019 with the subject "Invitation of the Constituent Evening on January 28, 2018" to 101 addressees. Were here for all recipients of the e-mail message, including the complainant, the e-mail addresses of all addressees visible in the mailing list of the e-mail program.⁶

The text of the email reads:

"Dear friends of the PVV,

1 Extract Chamber of Commerce 14 March 2019, no. 52322017, appendix 7 to the research report.

2 See e.g. print screen website, appendix 6 to the research report.

3 Notification form, appendix 2 to the investigation report.

4 Information request from AP dated 15 May 2019, Appendix 4 to the investigation report.

5 Response from PVV Overijssel of 24 May 2019, appendix 5 to the research report.

6 E-mail correspondence in the period from 10 to 15 January 2019, appendix 3 to the research report.

2/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

On Monday, January 28, 2019, the PVV Overijssel organizes a grassroots evening.

On this evening, the candidates for the Provincial Council elections of 20 March will be announced 2019 presented.

Members of Parliament of the PVV will also be present on this evening.

During this evening, all candidates will introduce themselves and there will be a number of speakers.

After the formal part, we would all like to talk to you and make it a pleasant one night of!

The evening starts at 7.30 pm and the grassroots evening will take place in Hotel van der Valk Hengelo.

The address: Bornsestraat 400, 7556 BN Hengelo.

Because we want to know how many people we can expect, we request that you contact us by e-mail.

e-mail to let us know if you are coming and with how many people.

Please send to secretariaat@pvvoverijssel.nl stating your name and the number persons.

We look forward to seeing you! See you on the 28th!

Yours sincerely,

PVV Overijssel.”

In response to this invitation, the complainant sent the PVV Overijssel the following day a request for him

from the mailing list and to confirm it as such. In addition, the complainant gives - in summary

displayed – indicates that making available all e-mail addresses of serious carelessness

testifies in view of the privacy rules. In an email dated January 11, 2019, the employee of the PVV

Overijssel responded with an apology and confirmed that the complainant's data had been removed from the list. On 15

In January 2019, the complainant again received a message from the PVV Overijssel with the same invitation

for the event on January 28, 2019, this time without revealing invitee email addresses

goods. Once again, the complainant requests that his contact details be deleted.⁷

The AP has not yet received a report from the PVV Overijssel, so the violation is still pending continues.

2. Legal framework

Pursuant to Article 2, paragraph 1, of the GDPR, this Regulation applies to the whole or in part automated processing, as well as to the processing of personal data contained in a file included or intended to be included therein.

Pursuant to Article 4 of the GDPR:

1. "Personal Data": any information relating to an identified or identifiable natural person ("the data subject"); is considered identifiable a natural person who can directly or indirectly be identified, in particular by an identifier such as a name, a identification number, location data, [...].

7 E-mail correspondence in the period from 10 to 15 January 2019, appendix 3 to the research report.

3/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

2. "Processing": an operation or set of operations relating to personal data or a set of personal data, whether or not carried out by automated processes [...].

7. "Controller": a [...] legal entity that, alone or jointly with others, achieves the purpose of and determines the means of processing personal data; [...].

12. "Personal Data Breach" means a security breach that occurs accidentally or on unlawfully leads to the destruction, loss, alteration or unauthorized disclosure of or the unauthorized access to data transmitted, stored or otherwise processed.

Pursuant to Article 33, paragraph 1, of the GDPR, the controller will file a breach connection with personal data has taken place, without unreasonable delay and, if

possible, no later than 72 hours after he has become aware of it, to the corresponding Article 55 competent supervisory authority unless it is unlikely that the breach related to personal data poses a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by a justification for the delay.

Recitals 75 and 76 of the GDPR state, inter alia, the following. The risk to the rights and freedoms of persons can result from personal processing that results in material and immaterial damage. This risk is particularly felt if the processing can lead to discrimination, among other things and reputational damage. This risk can also be felt if personal data is processed from which shows what someone's political opinion is. Risk assessment must take into account with both the likelihood and the severity of the risk to the rights and freedoms of data subjects. The risk must be determined on the basis of an objective assessment. In addition, should be determined whether the processing involves a risk or a high risk.

For example, it follows from the above considerations that appropriate protective measures must be taken, which belong to the processing of personal data with such a load as a political opinion.

3. Review

3.1 Processing of personal data and material scope GDPR

The aforementioned e-mail message dated 10 January 2019 concerns an invitation to a grassroots evening on January 28, 2019⁸ and is addressed to a group of 101 addressees, indicated therein as "friends of the PVV". The e-mail addresses are visible to all invitees in the address line of the email e-mail.⁹ These e-mail addresses contain combinations of a first and last name, initial(s) and last name, first and/or last name with a number, letters and/or numbers that cannot be used as a (personal) name indicate, as well as info addresses, et cetera.

⁸ The subject line of the e-mail states '2018'. This is an apparent clerical error.

⁹ E-mail correspondence in the period from 10 to 15 January 2019, appendix 3 to the research report.

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

(Part of) the recipients of the aforementioned e-mail can be recognized or can be recognized immediately be reduced by a single search function.

Now on the basis of this data a natural person, including the complainant, can become directly or indirectly identified, they qualify as personal data within the meaning of Article 4, opening words, and under 1, of the GDPR.

As noted above, data on political views qualifies as

so-called 'special categories of personal data' as described in Article 9, first paragraph, of the AVG.

The AP has established that with the sending of the email of January 10, 2019, there has been processing of personal data revealing political views as referred to in Article 9, paragraph 1,

of the GDPR. As indicated by the PVV Overijssel in a letter of 24 May 2019, the recipients of the invitation for the grassroots evening was previously reported to the PVV Overijssel and indicated to be interested in receiving invitations.¹⁰ The view of the PVV Overijssel that the reasons for interest in receiving e-mail messages such as invitations to

activities, can be diverse, the AP does not share. Being interested in a meeting of the PVV

Overijssel does not rule out the possibility that there are also interested parties who, from their political point of view, are interested in this

want to attend a meeting. The AP takes into account that this refers to the "constituency". Until

Finally, the AP points out that the PVV Overijssel does not exclude interested parties below who want to attend this evening because of their political views.

Based on the above, the AP concludes that personal data of

persons who express a political opinion.

3.2 Controller

In the context of the question of whether Article 33(1) of the GDPR is being complied with, it is important to determine who can be regarded as the controller as referred to in Article 4, opening words, and under 7 of the AVG. For this, it is decisive who has the purpose of and the means for the processing of personal data determines.

The PVV Overijssel is a foundation that aims to provide administrative and administrative assistance to the fraction of the PVV in the Provincial Council of Overijssel.¹⁰ The PVV Overijssel has no group relationship with another legal entity, such as the Party for Freedom association. Exclusively the board represents the foundation.¹¹

¹⁰ Letter PVV Overijssel of 24 May 2019, appendix 5 to the investigation report.

¹¹ Extract Chamber of Commerce 14 March 2019, no. 52322017, appendix 7 to the research report.

¹² See deed of establishment of the Foundation Support Provincial Party Overijssel Party for Freedom (PVV), deed date 15 March 2011, consulted on 29 August 2019, Annex 8 to the research report.

5/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

Every contribution posted on the website <https://www.pvvoverijssel.nl/> relates exclusively to the provincial politics of the province of Overijssel. All contributions are posted on behalf of 'Partij voor de Freedom Overijssel'. Various image fragments from Youtube are shown on the website public appearances of the PVV Overijssel shared. All this published media is by the account 'PVV Overijssel' posted on Youtube. Only the PVV Overijssel can also be contacted via the website become. The AP concludes from this finding that website management is in the hands of the PVV Overijssel. The supporters of the PVV Overijssel are formed by donors, volunteers and sympathizers. To

to be able to unite and mobilize the PVV Overijssel recruits volunteers. In addition, the PVV Overijssel gave substance to the active electability of the PVV in the province of Overijssel by, among other things, to recruit candidates in three municipalities of the province for the electoral list of the PVV for the municipal elections of 2018. The PVV Overijssel has the participation of the PVV in this municipal elections in Overijssel in the municipalities of Almelo, Enschede and Twenterand coordinated.¹³

The aim of recruiting volunteers and candidates for the 2018 municipal elections has led the PVV Overijssel designed by placing a web form on its website in which, among other things Name and address details, e-mail address, the availability for the City Council and/or volunteer, and the upload of a CV must be processed by the PVV Overijssel.¹⁴

In its letter of 24 May 2019¹⁵, the PVV Overijssel stated in response to the request for information from the AP¹⁶ indicated that she organizes various activities and worked with various mailing lists. The she has sent an invitation for the grassroots evening to people who have previously reported to her and have expressed an interest in receiving invitations. By a human error of a group employee, the e-mail addresses were visible to everyone who used the relevant received invitation. The PVV Overijssel says it has learned from this and internally appropriate to have taken measures.

From the foregoing, the AP concludes that the PVV Overijssel independently determines which resources it uses deems necessary to reach and activate its supporters in Overijssel. One of these resources is sending email. The PVV Overijssel has control over the way in which the personal data are processed and sets the purpose and means of the data processing in it framework of this activity.

Based on the above, the AP designates the PVV Overijssel as the controller as referred to in Article 4, preamble, and under 7, of the GDPR.

¹³ Print screen, appendix 6 to the research report.

¹⁴ Print screen, appendix 6 to the research report.

15 Letter PVV Overijssel dated 24 May 2019, appendix 5 to the research report.

16 Information request from AP dated 15 May 2019, Appendix 4 to the investigation report.

6/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

3.3 Obligation to report personal data breaches to the AP

3.3.1 Personal Data Breach

Pursuant to Article 33(1) of the GDPR, the controller reports the breach

connection with personal data without unreasonable delay and, if possible, no later than 72 hours after it

has taken note of it, to the supervisory authority competent in accordance with Article 55,

unless the personal data breach is not likely to pose a risk to the

rights and freedoms of natural persons.

For the question of whether there has been a violation of the duty to report within the meaning of Article 33(1) of the GDPR,

is first of all important to determine whether the sending of the e-mail of 10 January 2019 constitutes

of a so-called breach of security within the meaning of Article 4, preamble and under 12, of the

AVG.

What should be clear is that a breach is some kind of security incident. As indicated

Article 4, preamble and under 12, of the GDPR, however, only applies if there is a

personal data breach. The consequence of such a breach is that the

controller will not be able to guarantee that the principles relating to the

processing of personal data as described in Article 5 of the GDPR are complied with. This

highlights the difference between a security incident and a personal data breach –

it essentially means that all personal data breaches are security incidents

but that not all security incidents are necessarily breaches related to

are personal data. It is noted that a security incident is not limited to threat models where an organization is attacked from the outside, but also includes incidents resulting from internal processing.¹⁷

On January 10, 2019, a party employee of the PVV Overijssel sends an e-mail message with a invitation for a grassroots evening to a group of 101 recipients. This was for all recipients of the e-mail message, including the complainant, the e-mail address of addressees visible in the mailing list of the e-mail program. The PVV Overijssel acknowledges in its response of 24 May 2019 to the AP that this was highly undesirable and should never have happened.

In view of the above, the sending of the e-mail with the subject “Invitation of the Supporters evening January 28, 2018” to a group of 101 addressees on January 10, 2019 by the PVV Overijssel as a breach of security, which inadvertently resulted in an unauthorized provision of personal data to all recipients of the e-mail. In the opinion of the AP this constitutes a personal data breach as referred to in Article 4, part 12, of the GDPR.¹⁸

¹⁷ Guidance on personal data breach notification under Regulation 2016/679, p. 8.

¹⁸ Cf. sample direct marketing email, Guidance on Personal Data Breach Notification pursuant to Regulation 2016/679, p. 39.

7/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

3.3.2 Notification obligation to the AP

The notification obligation as laid down in Article 33(1) of the GDPR is mainly aimed at this encouraging controllers to take immediate action in the event of a breach, the breach to limit, restore the compromised personal data if possible and the

supervisory authority for advice. Due to the breach within the first 72 hours of the

supervisory authority, the controller can satisfy itself that

decisions about whether or not to notify individuals are correct.¹⁹

3.3.2.1 The moment at which the PVV Overijssel became aware of the infringement

Following the sending of the e-mail from the PVV Overijssel on 10 January 2019, the complainant has

January 11, 2019 responded and the PVV Overijssel requested to remove his e-mail address from its address file

to delete. The complainant also informs the PVV Overijssel that making all e-mails available

e-mail addresses and thereby traceable personal data shows serious carelessness. On this

the PVV Overijssel responded with an email on January 11, 2019 with apologies. Therefore, the PVV

Overijssel took note of the infringement in any event on 11 January 2019.²⁰

3.3.2.2 Personal data breach risk assessment

The GDPR imposes a notification obligation on all controllers, unless it is unlikely

that an infringement poses a risk to the rights and freedoms of natural persons. This must per

be assessed on a case-by-case basis.²¹

According to the PVV Overijssel, the AP refers in part 3.4.222 of its investigation report

to the "Guidelines for Personal Data Breach Notifications under

Regulation 2016/679', wrongly starts from the concept 'that the personal data breach

poses a risk to the rights and freedoms of natural persons." In the Guidelines (page 26)

however, the term is used: 'that the infringement poses a high risk to the rights and freedoms of

natural persons.' According to the Guidelines, therefore, a normal risk is not

sufficient, it must be a high risk, according to the PVV Overijssel.

The AP believes that the PVV Overijssel assumes an incorrect reading of the Guidelines. In there

a distinction is made between the report to the AP and the report to the person(s) involved:

"IV. Assessment of the risk and high risk

A. Risk as a reason for reports/announcements

¹⁹ Guidance on personal data breach notification under Regulation 2016/679, p. 18.

20 See e-mail correspondence in the period from 10 to 15 January 2019, appendix 3 to the research report.

21 Guidance on personal data breach notification under Regulation 2016/679, p. 9.

22 This means 3.5.2 Risk assessment.

8/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

Although the GDPR introduces the obligation to report a breach, this is not the case in all circumstances obliged:

☐ A breach must be reported to the competent supervisory authority unless it unlikely to pose a risk to the rights and freedoms of natural persons means.

☐ A breach is only communicated to the person if it is likely that they will have a high poses a risk to rights and freedoms.”²³

In the investigation report, the AP found that the PVV Overijssel was obliged to report the infringement report to the AP. In that context, it must therefore be assessed whether it is unlikely that the infringement poses a risk to the rights and freedoms of natural persons.

In its opinion, the PVV Overijssel also disputes that there is such a risk. To that end it argues, among other things, that the processing is only a processing of ordinary, not being special personal data is concerned. The PVV Overijssel states that it is unlikely that physical, material or immaterial damage arises and that it has rightly established with regard to the infringement that the infringement is not likely to pose a risk to the rights and freedoms of natural persons persons. According to the PVV Overijssel, it was not obliged to report the infringement to the AP.

The AP considers the following in this regard. In the Guidelines, with reference to the recitals 75 and 76 of the GDPR, identified factors that are important in the assessment of risks,

namely: nature of the infringement; nature, sensitivity and extent of the personal data; ease with which persons can be identified; seriousness of consequences for persons; special features of the person; special characteristics of the controller; the number of people affected; and general points. The nature and sensitivity of the personal data affected by the breach compromised are an important factor in this. Usually, the more sensitive the data, the larger the risk of harm to those involved.²⁴ When the breach relates to personal data which shows a political opinion, material or immaterial damage (such as discrimination and reputational damage) for the persons whose data is the subject of the breach as likely be considered.²⁵

The email sent on January 10, 2019 to 101 recipients contains email addresses with personal data of the data subjects. For this, the AP has considered that there is processing of personal data revealing political views. Considering the subject and the target group of the e-mail, an invitation to a constituency meeting of a political party, as well as the contents of that meeting, it is most likely that the addressees will include persons of interest have in the ideas of the PVV. Such information could have consequences for a current or future social position. Furthermore, the Guidelines regarding the

23 Guidance on personal data breach notification under Regulation 2016/679, p. 26.

24 Guidance on personal data breach notification under Regulation 2016/679, p. 28 ff.

25 Guidance on personal data breach notification under Regulation 2016/679, p. 26 and 27.

9/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

factor 'special characteristics of the controller' indicated that the nature and role of the controller and its activities may affect the risk of a breach

means for individuals. For example, a political organization processes special categories of personal data, meaning there is a greater threat to individuals if their personal data has been breached.

This implies a greater responsibility on the part of the political organization for a high level of protection. Finally, it is noted in this context that the infringement is a affects a relatively large number of people, namely (part of) those involved behind the mailing list of interested in invitations to activities of the PVV Overijssel.

Given these circumstances, there is no question that the breach is not likely to pose a risk means for the rights and freedoms of the data subjects. The PVV Overijssel was therefore held to the to report a violation to the AP.

3.3.2.3 Latest date on which PVV Overijssel should have reported the infringement to the AP

Now that the PVV Overijssel has become aware of the infringement in connection with with the personal data, she had a report without unreasonable delay and at the latest within 72 hours have to do to the AP as the competent supervisory authority. The PVV Overijssel therefore had an appearance had to report to the AP on January 14, 2019, but has failed to do so to date.

In view of the foregoing, the AP is of the opinion that PVV Overijssel has violated Article 33, first paragraph, of the AVG violated by failure to make the personal data breach without unreasonable delay and at the latest within 72 hours after PVV Overijssel became aware of the infringement, to be reported to the AP.

4. Fine

4.1 Introduction

If a controller fails to notify a personal data breach from the supervisory authority, despite meeting the requirements of Article 33 of the GDPR is met, the supervisory authority is offered a choice in which all is at its disposal standing corrective action should be considered, as well as the imposition of a fine.

In its opinion, the PVV Overijssel has explained and substantiated why it is of the opinion that it is not was obliged to report to the AP. She is therefore of the opinion that there is no basis

for the imposition of a measure or administrative fine. Insofar as the AP shares the views of the PVV

Overijssel would not follow, it makes an explicit and motivated appeal to Article 7 'Relevant

factors" of the Fining Policy Rules.²⁶

²⁶ Policy rules of the Dutch Data Protection Authority of 19 February 2019 with regard to determining the amount of administrative fines (Fine Policy Rules of the Dutch Data Protection Authority 2019), Government Gazette no. 14586, March 14, 2019.

10/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

The AP notes the following in this regard. By sending an invitation to a constituency evening in which for all recipients of the e-mail message, the list of recipients is visible in the mailing list of the e-mail program, the PVV Overijssel has provided unauthorized insight into all e-mail e-mail addresses and in all names of the recipients, being persons with an interest in the ideas of the PVV. By sending the e-mail are therefore personal data revealing political views appear shared with all recipients of the e-mail and has violated the right of respect privacy and the right to the protection of personal data of a large number data subjects who have lost control of their personal data as a result. It failure to report this personal data breach to the AP in a timely manner is, in the opinion of the AP, a serious violation. That the PVV Overijssel has no report of this made because it concerned people who indicated that they would like to receive mail periodically,²⁷ makes that's no different.

The AP sees reason to make use of its power to impose a fine under Article 58, second paragraph, preamble and under i and Article 83, fourth paragraph, of the GDPR, read in conjunction with Article 14, third paragraph, of the UAVG, on the PVV Overijssel.

Pursuant to article 83, paragraph 4, under a, of the AVG, violations of article 33 of the AVG are subject to administrative fines of up to €10,000,000 in accordance with paragraph 2 or, for a company, up to 2% of the total worldwide annual turnover in the previous financial year, if this figure is higher.

4.2 Fining Policy Rules of the Dutch Data Protection Authority 2019 (Fining Policy Rules 2019)

The AP has established Fining Policy Rules 2019 regarding the implementation of the aforementioned power to imposing an administrative fine, including determining the amount thereof.

Pursuant to Article 2, under 2.1, of the Fining Policy Rules 2019, the provisions regarding violation of which the AP can impose an administrative fine not exceeding the amount of € 10,000,000 [...] in annex 1 classified in category I, category II or category III. In Annex 1, the violation of Article 33, first paragraph, of the AVG classified in category III.

Pursuant to Article 2.3 of the Fining Policy Rules 2019, the AP sets the basic fine for violations for which a statutory maximum fine of € 10,000,000 applies [...] fixed within the period stipulated in that article penalty bandwidths. The following applies to violations in category III of Appendix 1 of the 2019 Fining Policy Rules a fine bandwidth between €300,000 and €750,000 and a basic fine of €525,000.

Pursuant to Article 6 of the Fining Policy Rules 2019, the AP determines the amount of the fine by the amount from the basic fine upwards (up to a maximum of the bandwidth of the offense linked penalty category) or down (to at least the minimum of that

27 Letter PVV Overijssel dated 24 May 2019, appendix 5 to the research report.

11/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

bandwidth). The basic fine is increased or decreased depending on the extent to which the factors referred to in Article 7 of the Fining Policy Rules 2019 give cause to do so.

Pursuant to Article 7 of the Fining Policy Rules 2019, the AP, without prejudice to Articles 3:4 and 5:46 of the General Administrative Law Act (Awb) takes into account the following factors derived from Article 83, second paragraph, of the AVG, in the Policy Rules referred to under a to k:

- a. the nature, gravity and duration of the breach, taking into account the nature, scope or purpose of the processing in question as well as the number of data subjects affected and the extent of the harm suffered by them injury;
- b. the intentional or negligent nature of the breach;
- c. the measures taken by the controller [...] to mitigate the losses suffered by data subjects limit damage;
- d. the extent to which the controller [...] is responsible in view of the technical and organizational measures he has implemented in accordance with Articles 25 and 32 of the GDPR;
- e. previous relevant breaches by the controller [...];
- f. the degree of cooperation with the supervisory authority to remedy the breach and limit the possible negative consequences thereof;
- g. the categories of personal data affected by the breach;
- h. the manner in which the supervisory authority became aware of the breach, in particular whether, and if so, to what extent, the controller [...] has notified the breach;
- i. compliance with the measures referred to in Article 58, second paragraph, of the GDPR, insofar as they are earlier in respect of the controller [...] in question in relation to the same matter have been taken;
- j. adherence to approved codes of conduct in accordance with Article 40 of the GDPR or of approved certification mechanisms in accordance with Article 42 of the GDPR; and
- k. any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial gains made, or losses avoided, which may or may not result directly from the breach result.

Pursuant to Article 8.1 of the Fining Policy Rules 2019, the AP may, if the

fine category does not allow for an appropriate punishment in the concrete case, when determining the amount of the fine the fine bandwidth of the next higher category or the fine bandwidth of the apply next to lower category.

Pursuant to Article 9 of the Fining Policy Rules 2019, the AP, when setting the fine, taking into account the financial circumstances of the offender. In case of reduced or insufficient capacity of the offender, the AP can further moderate the fine to be imposed, if, after application of article 8.1 of the policy rules, determination of a fine within the fine range of the next lower category would, in its opinion, nevertheless lead to a disproportionately high fine.

12/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

4.3 Fine amount

According to the AP, the following factors mentioned in Article 7 are particularly relevant in this case determining the fine amount:

- a. the nature, seriousness and duration of the breach;
- b. the intentional or negligent nature of the breach (culpability);
- c. the measures taken by the controller or processor to mitigate the damage suffered by those involved.

4.3.1 Nature, seriousness and duration of the breach

Pursuant to Article 7, preamble and under a, of the Fining Policy Rules 2019, the AP takes into account the nature, the seriousness and duration of the infringement.

The protection of natural persons with regard to the processing of personal data is a fundamental right.

Pursuant to Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16,

Everyone has the right to, paragraph 1 of the Treaty on the Functioning of the European Union (TFEU).

protection of his personal data. The principles and rules regarding the protection of natural persons when processing their personal data must comply with their fundamental rights and freedoms, in particular their right to protection personal data. The GDPR aims to contribute to the creation of an area of freedom, security and justice and of an economic union, as well as to economic and social progress, the strengthening and convergence of economies within the internal market and the well-being of natural persons. The processing of personal data must serve people. The right to protection of personal data is not absolute, but must be considered in relation to its function in society and must, in accordance with the principle of proportionality, against others fundamental rights are considered. Any processing of personal data must be fair and lawful to happen. The personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed. Personal data must be processed in a manner that ensures appropriate security and confidentiality of that data, also to prevent unauthorized access to or the unauthorized use of personal data and the equipment used for processing. With the AVG is an effective protection of personal data is intended.

Reporting breaches should be seen as a means of ensuring compliance with related rules improve the protection of personal data. If a breach related to personal data takes place or has taken place, this may result in physical, material or immaterial damage to natural persons or any other economic or social disadvantage the person in question. Therefore, the controller should, as soon as he becomes aware of a personal data breach to the supervisory authority without delay and if possible within 72 hours notify you of the personal data breach. The supervisor is involved in this to properly perform its tasks and powers, as laid down in the GDPR.

June 16, 2020

Our reference

[CONFIDENTIAL]

The PVV Overijssel believes that the nature and scope of the infringement is limited, now that it is a single e-mail e-mail message with a general indication without any information regarding the data subject is processed differently than the e-mail address.

The AP does not follow the PVV Overijssel in this. It should be stated that the PVV Overijssel van January 14, 2019 to date has not made the legally required notification of this infringement to the AP. Bee in its assessment, the DPA assumes that the infringement concerns 101 persons, which is also mentioned of a special category of personal data, namely those revealing political opinions. The AP considers the violation serious in view of this, but sees no reason to increase the basic fine increase or decrease.

4.3.2 Intentional or negligent nature of the infringement (culpability)

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. Now that this is one violation, it is not required for the imposition of an administrative fine in accordance with established case law²⁸ it is demonstrated that there is intent and the AP may assume culpability if the perpetrator is established.²⁹

The PVV Overijssel believes that there is no intentional or negligent nature of the infringement. She has immediately made the assessment that it should make in accordance with Article 33 of the GDPR upon detection and has ruled on legitimate grounds that there is no obligation to report the infringement to the AP.

The AP notes that insofar as such a consideration would have already taken place, the PVV Overijssel not performed it correctly. She has as grounds for not reporting the infringement to the AP indicated: "It concerns an invitation that has been sent to people who have previously reported to us and have expressed interest in receiving our invitations." And we did not report this, because it concerned people who indicated periodic

want to receive our mail.” In addition, the PVV Overijssel has indicated in that context that it is “not about an involuntary group of people goes”.³⁰ However, this is not a criterion on the basis of which it would be possible to be concluded that this would be a non-notifiable infringement. At the time that the PVV Overijssel had knowledge of the incident, she had wrongly based on the nature of the provided personal data must make a risk assessment and then report the breach at the AP. PVV Overijssel has nevertheless failed to notify the AP.

28 Cf. CBb 29 October 2014, ECLI:NL:CBB:2014:395, r.o. 3.5.4, CBb 2 September 2015, ECLI:NL:CBB:2015:312, r.o. 3.7 and CBb 7 March 2016,

ECLI:NL:CBB:2016:54, r.o. 8.3, ABRvS 29 August 2018, ECLI:NL:RVS:2018:2879, r.o. 3.2 and ABRvS December 5, 2018, ECLI:NL:RVS:2018:3969, r.o. 5.1.

29 Parliamentary Papers II 2003/04, 29702, no. 3, p. 134.

30 Letter PVV Overijssel dated 24 May 2019, appendix 5 to the research report.

14/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

In view of the foregoing, the AP considers it culpable that the PVV Overijssel did not report to the AP, but sees no reason to do so on the basis of this established culpability to increase or decrease the basic fine amount.

4.3.3 Measures taken to limit the damage suffered by those involved

The PVV Overijssel has indicated that it has its working method and processes immediately after detection adjusted to prevent such an error from being made again and that this measures have proven to be effective.

The AP considers that no measures have been taken to mitigate the (possible) damage suffered by those involved to limit. A political organization such as the PVV Overijssel can be expected to act properly

is aware of the sensitivity of the personal data it processes and an appropriate one level of protection is guaranteed. It was not until after the incident that she indicated that someone internally would be involved proficient in the AVG.

In the circumstances put forward, the AP therefore sees no reason to increase the basic amount of the fine pursuant to Article 7, under c of the 2019 Policy Rules.

4.3.4 Proportionality

Finally, the AP assesses whether the application of its policy for determining the amount of the fine given the circumstances of the specific case, does not lead to a disproportionate outcome. Applying the principle of proportionality means, according to the Fining Policy Rules 2019, that the AP, if necessary, when setting the fine takes into account the financial circumstances of the offender.

The PVV Overijssel has indicated that as a non-profit political foundation it has very limited has financial resources.

The AP considers as follows in this regard. Pursuant to Article 3 of the Foundation's Articles of Association Support Provincial Group Overijssel Party for Freedom, it will be realized purpose of the foundation earmarked capital formed by the financial contribution of the province Overijssel, and what is obtained in another way. According to the Civil Service Assistance Regulation and party support province of Overijssel, the factions receive an annual financial contribution as contribution towards the costs for the functioning of the group. This allowance amounts to maximum € 3,570.00 for each Member of Parliament belonging to that faction plus € 26,460.00 per faction (per 1 January 2019).³¹

31 Ordinance on civil service assistance and party support province of Overijssel 2016, Provincial Gazette no. 33, 2 January 2017 and no. 2734, April 11, 2019.

June 16, 2020

Our reference

[CONFIDENTIAL]

In view of this, the AP considers the capacity of the PVV Overijssel limited and comes to the conclusion that the PVV Overijssel cannot financially bear the fine of € 525,000. On this basis, the AP sees reason to reduce the fine. In this case, the AP considers a fine of € 7,500 appropriate and commanded. In this context, the AP considers that it has not been shown that the PVV Overijssel would not pay this fine can wear.

4.3.5 Conclusion

The AP sets the total fine amount at € 7,500.

5. Operative part

fine

The AP submits to the PVV Overijssel, due to violation of Article 33, first paragraph, of the AVG in the period from 14 January 2019 to the present, imposed an administrative fine in the amount of € 7,500 (in words: seven thousand five hundred euros).³²

Yours faithfully,

Authority for Personal Data,

Mr. A. Wolfsen

Chair

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. Submit it of a notice of objection suspends the operation of this decision. 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.

32 The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (CJIB).