

Confidential/Registered

Provincial Support Foundation

Party Overijssel Party for Freedom

[CONFIDENTIAL]

57 Steenmeijerstraat

7555 NV HENGELO

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

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

authority data.nl

Dear [CONFIDENTIAL],

The Dutch Data Protection Authority (hereinafter: AP) has decided to inform the Provincial Support Foundation

Faction 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 14 January 2019 to

has failed to present 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, at the latest

report to the AP. The PVV Overijssel therefore has Article 33, first paragraph, of the General Regulation

Violation of data protection (hereinafter: GDPR).

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

1. Facts and process

Foundation Support Provincial Faction 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 administrative and administrative assistance to the Group (as referred to in Article 5 of the Rules 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) for the purpose.¹ The foundation also publishes 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 the PVV Overijssel sent an e-mail on January 10, 2019. e-mail message with "Invitation Affiliate Evening 28 January 2018" as subject to a group of 101 recipients. For all recipients of the e-mail, including the complainant, the list of recipients visible in the mailing list of the e-mail program.

As a result of this complaint, the AP has launched an investigation to determine whether the rules laid down in the GDPR regarding reporting a personal data breach have been 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 of 11 December 2019, the AP to the PVV Overijssel has an intention to enforce sent together with the aforementioned investigation report and the underlying documentation, whereby the PVV was also given the opportunity to express its views. The PVV Overijssel has letter of 28 January 2020 has given its opinion in writing.

Based on the report with findings, the underlying documentation and the opinion of the PVV Overijssel, the AP comes to the conclusion of the following relevant facts.

A fraction employee of the PVV Overijssel will send an e-mail message on Thursday, January 10, 2019 with the subject 'Invitation of supporters evening 28 January 2018' to 101 addressees. Here were for all recipients of the e-mail, including the complainant, the e-mail addresses of all recipients visible in the mailing list of the e-mail program.⁶

The text of the email reads:

“Dear friends of the PVV,

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

2 See, among other things, 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 of PVV Overijssel of 24 May 2019, appendix 5 to the investigation 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 March 20th will be announced 2019 presented.

Members 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 are all happy to talk to you and make it a cozy one night of!

The evening starts at 19.30 pm and the supporters evening will take place in Hotel van der Valk in Hengelo.

The address: Bornsestraat 400, 7556 BN Hengelo.

Because we want to know how many people we can expect, we request that you send us an e-mail. 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!

Sincerely,

PVV Overijssel.”

In response to this invitation, the complainant sends the request for him to the PVV Overijssel the next day from the email list and confirm it as such. In doing so, the complainant – in summary displayed – indicating that the provision of all e-mail addresses of serious carelessness bears witness to the privacy rules. By e-mail of January 11, 2019, the employee of the PVV responds Overijssel to this with an apology and confirms that the complainant's data has been removed from the list. at 15 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 the email addresses of invitees visible goods. Once again, the complainant requests that his contact details be removed.⁷

To date, the AP has not received a report from the PVV Overijssel, so that the violation is still continues.

2. Legal framework

Pursuant to Article 2(1) of the GDPR, this Regulation applies to all or part of automated processing, as well as to the processing of personal data that are in a file included or intended to be included therein.

Pursuant to Article 4 of the GDPR, the following definitions apply:

1. “Personal data”: any information about an identified or identifiable natural person (“the data subject”); considered identifiable is a natural person who can directly or indirectly be identified, in particular by means of 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” means a [...] legal entity that, alone or jointly with others, fulfills the purpose of and determine the means of processing personal data; [...].

12. “Personal Data Breach” means a breach of security committed by accident or on unlawfully leads to the destruction, loss, alteration or unauthorized disclosure of or unauthorized access to data transmitted, stored or otherwise processed.

Pursuant to Article 33(1) of the GDPR, the controller must, in the event of an infringement connection with personal data has taken place, without undue delay and, if

possible, no later than 72 hours after he has become aware of it, to report it to the 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 provide, inter alia, as follows. The risk to the rights and freedoms of individuals may result from personal processing that results in material and immaterial damage. This risk is particularly felt if the processing can lead to, among other things, discrimination and reputational damage. This risk can also be felt if personal data is processed from which shows what a person's political opinion is. Risk assessment should take into account with both the likelihood and 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, it should be determined whether the processing involves a risk or a high risk.

It follows from the above considerations, for example, that appropriate protective measures must be taken, which are associated with the processing of personal data with such a connotation as a political view.

3. Review

3.1 Processing of personal data and material scope of the GDPR

The aforementioned e-mail of January 10, 2019 concerns an invitation for 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 e-mail.⁹ These e-mail addresses contain combinations of a first and last name, initial(s) and surname, 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 reads '2018'. This is an obvious misspelling.

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 immediately or can be identified with this be traced back by a single search function.

Now based on this data, a natural person, including the complainant, can be identified 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 about political opinions qualifies under the GDPR as so-called 'special categories of personal data' as described in Article 9, first paragraph, of the GDPR.

The AP has established that with the sending of the e-mail of January 10, 2019, there is the processing personal data from which political views appear as referred to in Article 9, first paragraph, of the GDPR. As the PVV Overijssel indicated in a letter dated 24 May 2019, the recipients of the invitation to the constituency evening reported earlier 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. 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, wish to attend the meeting. The AP takes into account the fact that this is referred to as the "followers". Until Finally, the AP points out that the PVV Overijssel also does not exclude that interested parties below are willing to attend this evening because of their political views.

Based on the above, the AP concludes that the processing of personal data of persons expressing a political opinion.

3.2 Controller

In the context of the question whether Article 33(1) of the GDPR is 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 GDPR. It is decisive for this who determines 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.¹¹ The PVV Overijssel has no group relationship with another legal entity, such as the Party for Freedom association. Exclusively the board represents the foundation.¹²

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

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

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

5/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

Every contribution posted on the website <https://www.pvverijssel.nl/> relates exclusively to the provincial policy of the province of Overijssel. All contributions are posted on behalf of 'Party for the Freedom Overijssel'. On the website, various image fragments, originating from Youtube, are public appearances of the PVV Overijssel shared. All this published media is through the account 'PVV Overijssel' posted on Youtube. Only the PVV Overijssel can 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 made up of donors, volunteers and sympathizers. To to be able to unite and mobilize them, the PVV Overijssel recruits volunteers. In addition, the PVV

Overijssel gave substance to the active eligibility of the PVV in the province of Overijssel by, among other things, in three municipalities of the province to recruit candidates for the electoral list of the PVV for the municipal elections of 2018. The PVV Overijssel has herein the participation of the PVV in municipal elections in Overijssel in the municipalities of Almelo, Enschede and Twente and coordinated.¹³

The goal of recruiting volunteers and candidates for the 2018 municipal elections has the PVV Overijssel designed by placing a web form on its website in which, among other things, Name and address details, e-mail address, availability for 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 has responded to the AP16's request for information indicated that she organizes different activities and worked with different 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 had the relevant received an invitation. The PVV Overijssel says it has learned from this and internally appropriate have taken measures.

From the foregoing, the AP concludes that the PVV Overijssel independently determines which resources they use considers it 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 is processed and sets the purpose and means of the data processing in the framework of this activity.

On the basis of the above, the AP designates the PVV Overijssel as the controller if 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 investigation 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 breaches of personal data to the AP

3.3.1 Personal data breach

Pursuant to Article 33(1) of the GDPR, the controller shall notify the infringement connection with personal data without undue delay and, if possible, no later than 72 hours after he has taken cognizance of it, to the supervisory authority competent in accordance with Article 55, unless it is not likely that the personal data breach poses a risk to the rights and freedoms of natural persons.

For the question whether there has been a violation of the reporting obligation within the meaning of Article 33(1) of the GDPR, is first of all important to determine whether the e-mail of January 10, 2019 was sent of a so-called breach of security within the meaning of Article 4, opening words and under 12, of the GDPR.

What should be clear is that a breach is a type of security incident. As indicated Article 4, preamble and under 12, of the GDPR, however, only applies when there is a breach of personal data. The consequence of such infringement 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 Stresses the difference between a security incident and a personal data breach – Essentially, all personal data breaches are security incidents but that not all security incidents are necessarily breaches related to are personal data. It should be noted that a security incident is not limited to

threat models where an organization is attacked from the outside, but also includes incidents arising from internal processing.¹⁷

On January 10, 2019, a party employee of the PVV Overijssel sends an e-mail message with a invitation to a grassroots evening to a group of 101 addressees. This was for all recipients of the e-mail, including the complainant, the e-mail address of recipients 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 Constituents evening January 28, 2018” to a group of 101 addressees on January 10, 2019 by the PVV Overijssel as a breach of security, which has inadvertently led to an unauthorized provision of personal data to all recipients of the e-mail. In the opinion of the AP, this constitutes an infringement in connection with personal data as referred to in Article 4, part 12, of the GDPR.¹⁸

¹⁷ Guidelines for the reporting of personal data breaches under Regulation 2016/679, p. 8.

¹⁸ Cf. example direct marketing mail, Guidelines for the reporting of personal data breaches under 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, first paragraph, of the GDPR, is mainly aimed at encourage data controllers to take immediate action in the event of a breach, the breach contain, restore the compromised personal data if possible and supervisory authority for advice. By committing the infringement within the first 72 hours

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 when the PVV Overijssel became aware of the infringement

Following the sending of the e-mail from the PVV Overijssel on January 10, 2019, the complainant has January 11, 2019 responded and the PVV Overijssel requested his e-mail address from its address file remove. The complainant also informs the PVV Overijssel that making all e-mails available e-mail addresses and thereby traceable personal data is a sign of serious carelessness. to this the PVV Overijssel responded with an e-mail on January 11, 2019 with apologies. Therefore, the PVV Overijssel became aware of the infringement in any case on 11 January 2019.²⁰

3.3.2.2 Risk assessment of personal data breach

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 case to be assessed.²¹

According to the PVV Overijssel, the AP refers in part 3.4.222 of its investigation report to to the “Guidelines for Notifying Personal Data Breach Reports under” Regulation 2016/679’, erroneously based on the concept ‘that the personal data breach’ poses a risk to the rights and freedoms of individuals.” 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 notification to the DPA and the notification to the data subject(s):

“IV. Assessment of risk and high risk

A. Risk as a reason for reports/notifications

¹⁹ Guidelines for the reporting of personal data breaches 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 Guidelines for the reporting of personal data breaches under Regulation 2016/679, p. 9.

22 This is 3.5.2 Risk assessment.

8/16

Date

June 16, 2020

Our reference

[CONFIDENTIAL]

While 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 violation will only be communicated to the person if it is probable that they have a high risk to rights and freedoms.”²³

In the investigation report, the AP found that the PVV Overijssel was obliged to commit 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 disputed that there is such a risk. To that end it argues, inter alia, that the processing is only processing of ordinary, non-special concerns personal data. The PVV Overijssel states that it is therefore unlikely that physical, material or immaterial damage and that it has correctly established with regard to the infringement that the infringement is not likely to endanger 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, which are factors that are important in the assessment of risks, namely: nature of the infringement; nature, sensitivity and scope of the personal data; ease with which

persons can be identified; severity 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. The more sensitive the data, the larger usually the risk of harm to the data subjects.²⁴ When the breach relates to personal data demonstrating a political opinion, material or immaterial harm (such as discrimination and reputational damage) for the persons whose data is the subject of the infringement as probable be considered.²⁵

The email sent to 101 recipients dated January 10, 2019 contains email addresses with personal data of the data subjects. For this, the AP has considered that processing of personal data revealing political views. Given the subject matter and target audience of the e-mail, an invitation to a constituency meeting of a political party, as well as the content of that meeting, it is most likely that among the addressees there are persons who are interested have in the ideas of the PVV. Such information could affect a existing or future social position. Furthermore, the Guidelines on the

²³ Guidelines for the reporting of personal data breaches under Regulation 2016/679, p. 26.

²⁴ Guidelines for the reporting of personal data breaches under Regulation 2016/679, p. 28 ff.

²⁵ Guidelines for the reporting of personal data breaches 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 persons. 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 means that the political organization has a greater responsibility to

level of protection. Finally, it should be noted in this regard that the infringement

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 infringement is unlikely to pose a risk affects the rights and freedoms of data subjects. The PVV Overijssel was therefore held de to report the infringement 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 been informed of the infringement in connection at least on January 11, 2019 with the personal data, it had a report without undue delay and at the latest within 72 hours must do to the AP as the competent supervisory authority. So the PVV Overijssel had no later than 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 Article 33, first paragraph, of the GDPR by failing to disclose the personal data breach without unreasonable delay and at the latest within 72 hours, after PVV Overijssel became aware of the infringement, to report to the AP.

4. Fine

4.1 Introduction

If a controller fails to notify a personal data breach

from the supervisory authority, despite the fact that the requirements of Article 33 of the

GDPR is complied with, the supervisory authority is given a choice in which all at its disposal standing corrective measures should be considered, as well as the imposition of a fine.

In its view, the PVV Overijssel has explained and substantiated why it is of the opinion that it is not was obliged to make a report to the AP. It is therefore of the opinion that there is no ground for the imposition of a measure or administrative fine. As far as the AP views the PVV

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

factors' of the Fine 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 grassroots evening in which, for all recipients of the e-mail, the list of recipients is visible in the mailing list of the e-mail program, the PVV Overijssel has given 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, therefore, personal data from which political views appear to have been shared with all recipients of the e-mail and the right to respect for 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 provide timely notification of this personal data breach to the AP is a serious violation in the opinion of the AP. That the PVV Overijssel has no report of this made, because it concerned people who indicated that they wish to receive mail periodically,²⁷ makes that's no different.

The AP sees reason to use 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, to impose on the PVV Overijssel.

Pursuant to Article 83(4)(a) of the GDPR, infringements of Article 33 of the GDPR

subject to administrative fines up to € 10,000,000 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 Fine Policy Rules of the Dutch Data Protection Authority 2019 (Fining Policy Rules 2019)

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

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

Pursuant to Article 2.3 of the 2019 Fine Policy Rules, the AP sets the basic fine for violations subject to a statutory maximum fine of € 10,000,000 [...] fixed within the determined in that article penalty bandwidths. For violations in category III of Appendix 1 of the Fine Policy Rules 2019 applies a fine range between €300,000 and €750,000 and a basic fine of €525,000.

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

27 Letter PVV Overijssel dated 24 May 2019, appendix 5 to the investigation 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 2019 Fine Policy Rules give rise to this.

Pursuant to Article 7 of the Fine Policy Rules 2019, the AP keeps 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 GDPR, referred to under a to k in the Policy Rules:

the nature, seriousness and duration of the infringement, taking into account the nature, scope or purpose of the infringement processing in question as well as the number of data subjects affected and the extent of the damage suffered by them injury;

b. the intentional or negligent nature of the infringement;

c. the measures taken by the controller [...] to address the data subjects suffered limit damage;

d. the extent to which the controller [...] is responsible given the technical and organizational measures that he has carried out in accordance with Articles 25 and 32 of the GDPR;

e. previous relevant breaches by the controller [...];

f. the extent to which there has been cooperation with the supervisory authority to remedy the breach and limit the possible negative consequences thereof;

g. the categories of personal data to which the breach relates;

h. the manner in which the supervisory authority became aware of the infringement, 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, paragraph 2, of the GDPR, insofar as they are previously with regard to the controller [...] in question with regard 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, arising directly or indirectly from the infringement result.

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

fine category does not allow an appropriate punishment in the specific case, when determining the amount of

the fine the fine bandwidth of the next higher category or the fine bandwidth of the next to lower category apply.

Pursuant to Article 9 of the Fine Policy Rules 2019, when determining the fine, the AP will, if necessary, taking into account the financial circumstances of the offender. In case of reduced or If the offender has insufficient financial capacity, the AP can further mitigate 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, in this case, the following factors mentioned in Article 7 are particularly relevant for the determining the amount of the fine:

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

4.3.1 Nature, seriousness and duration of the infringement

Pursuant to Article 7, opening words and under a, of the Fine 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.

Under Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16, paragraph 1 of the Treaty on the Functioning of the European Union (TFEU), everyone has the right to protection of his personal data. The principles and rules concerning the protection of

natural persons when processing their personal data must be in accordance with their fundamental rights and freedoms, in particular their right to protection of personal data. The GDPR aims to contribute to the creation of an area of freedom, security and justice and of 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 conform to the principle of proportionality against other fundamental rights are weighed up. Any processing of personal data must be fair and lawful to happen. The personal data must be sufficient, 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 use of personal data and the equipment used for processing. With the GDPR, effective protection of personal data intended.

Notification of breaches should be seen as a means of ensuring compliance with the related rules to improve the protection of personal data. If an infringement in connection with 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 for the person in question. Therefore, as soon as the controller becomes aware of a breach of personal data the supervisor without delay and if possible within 72 hours of the personal data breach. The supervisor is thus in able to properly perform its duties and powers, as laid down in the GDPR.

13/16

Date

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 containing information regarding the data subject is processed other than the email address.

The AP does not follow the PVV Overijssel in this. It should be assumed 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 AP considers that the infringement concerns 101 persons, which furthermore includes of a special category of personal data, namely those that reveal political opinions. The In view of this, the AP considers the violation serious, but sees no reason to pay the basic fine increase or decrease.

4.3.2 Intentional or negligent nature of the infringement (culpability)

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. Now that this is a violation, the imposition of an administrative fine in accordance with established case law²⁸ does not require that it is demonstrated that there is intent and the AP may presume culpability if it offense 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 discovery and has lawfully ruled that there is no obligation to report the infringement to the AP.

The AP notes that insofar as such a consideration has already taken place, the PVV Overijssel has not performed it correctly. As a ground for not reporting the infringement to the AP, she has indicated: "it concerns an invitation that has been sent to people who have previously registered with us and have expressed an interest in receiving our invitations." And we did not report this, because it concerned people who indicated periodically from to receive our email." In addition, the PVV Overijssel has indicated in that context that it is "not to

an involuntary group of people.”³⁰ However, this is not a criterion against which one could concluded that this would be a non-reportable infringement. At the time that the PVV Overijssel was aware of the incident, based on the nature of the wrongful personal data provided must make a risk assessment and subsequently report the breach at the AP. PVV Overijssel has nevertheless failed to report to the AP.

28 Cf. CBb 29 October 2014, ECLI:NL:CBB:2014:395, r.o. 3.5.4, CBb September 2, 2015, ECLI:NL:CBB:2015:312, r.o. 3.7 and CBb March 7, 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 investigation 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 on the basis of this established culpability, sees no reason to increase or decrease the basic fine.

4.3.3 Measures taken to limit the damage suffered by those involved

The PVV Overijssel has indicated that it has changed its working method and processes immediately after observation modified to prevent such a mistake from being made again and measures have been proven to be effective.

The AP considers that no measures have been found to mitigate the damage (possibly) suffered by those involved to limit. A political organization such as the PVV Overijssel can be expected to fully commit itself is aware of the sensitivity of the personal data it processes and has an appropriate

level of protection. Only after the incident did she indicate that someone internally would become proficient in the GDPR.

The AP therefore sees no reason in the circumstances invoked to increase the basic amount of the fine pursuant to Article 7, under c of the 2019 Policy Rules.

4.3.4 Proportionality

Finally, on the basis of Articles 3:4 and 5:46 of the Awb (principle of proportionality), the AP assesses whether the applying 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 According to the 2019 Fine Policy Rules, the AP entails that, if necessary, when determining 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 this as follows. Pursuant to Article 3 of the Foundation's Articles of Association Support Provincial Faction Overijssel Party for Freedom, it is the realization of the purpose of the foundation Capital intended for use formed by the financial contribution of the province Overijssel, and that which is obtained in other ways. According to the Regulation on official assistance and political group support in the province of Overijssel, the political groups receive an annual financial contribution as contribution to the costs of the functioning of the group. This allowance amounts to at least maximum of €3,570 for each member of Parliament belonging to that fraction, increased by €26,460 per fraction (per 1 January 2019).³¹

31 Ordinance on official assistance and faction support for the province of Overijssel 2016, Provincial Gazette no. 33, 2 January 2017 and no. 2734,

Apr 11, 2019.

15/16

Date

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 regard, 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 at € 7,500.

5. Operative part

fine

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

Yours faithfully,

Authority Personal Data,

mr. A. Wolfsen

Chair

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. Submit it of a notice of objection suspends the effect 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 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.

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