

Police Netherlands

to the attention of the Chief of Police, Mr. H.P. from Essen

PO Box 17107

2502 CC THE HAGUE

Date

November 17, 2022

Our reference

z2021-17798

Contact

[CONFIDENTIAL]

Subject

mobile camera cars Rotterdam - decision to impose a fine

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Hoge Nieuwstraat 8, 2514 EL The Hague

T 070 8888 500 - F 070 8888 501

authoritypersonal data.nl

Dear Mr van Essen,

The Dutch Data Protection Authority (hereinafter: AP) has decided to impose an administrative fine on the Chief of Police

of € 50,000 for violation of Article 4c, first paragraph, of the Police Data Act (hereinafter:

Wpg). This is because the chief of police failed to inform prior to the intended processing of

police data – namely making camera images using two so-called mobile cameras

cars in Rotterdam – carry out a data protection impact assessment while processing

of police data was likely to pose a high risk to the rights and freedoms of individuals.

This decision explains the administrative fine. To this end, (1) the

reason and course of the proceedings, (2) the established facts, (3) the violation and (4) the amount of the

fine. Finally (under 5) the operative part and the legal remedies clause follow.

Public version

Date

November 17, 2022

Our reference

z2021-17798

1

2

3

4

1 Reason and course of the process

In the spring of 2020, the Netherlands was confronted with the COVID-19 pandemic. The cabinet announced then introduced measures to prevent the spread of the virus. These measures were applied locally level laid down in emergency regulations. An emergency ordinance was also introduced in the municipality of Rotterdam corona measures in force (hereinafter: “emergency regulation”)¹. These measures included, among others the ban on gatherings and the obligation for people to keep a distance of 1.5 meters (in public space). hold. To monitor and enforce compliance with the corona measures are in the municipality Rotterdam deployed two cars from April 10, 2020 with a camera mounted on the roof, also known as mobile camera cars (hereinafter referred to as: “MCAs”).

Following reports in the media, the AP has contacted the municipality of Rotterdam.

In the period from 10 April 2020 to 17 April 2020, it turned out that two MCAs had indeed been deployed, but this deployment was discontinued after a week at the request of the police.² When the AP received signals that the MCAs were deployed again from April 26, 2020, the AP decided to launch a start research. The AP investigated, among other things, whether the chief of police acted in violation with the obligation to carry out a data protection impact assessment in a timely manner (hereinafter also: “GEB”) as referred to in Article 4c of the Wpg. Since the AP has no authority to commit violations

of Article 3 of the Wpg with a fine, the AP does not comment on the

answer to the question whether the Chief of Police acted in accordance with Article 3 of the Wpg.

For this reason, this also means that the AP does not comment on the answer to the question whether in this decision

Article 3 of the Police Act 2012 (hereinafter: Police Act) can serve as a basis for the deployment of the MCAs.

The investigation has led to the AP's Customer Contact and Controlling Investigation Department op

has adopted a report of findings on 26 November 2021 (hereinafter: investigation report). In the

Insofar as relevant here, the investigation report concluded that the Chief of Police was obliged to provide a

GEB before processing the camera images using the MCAs and that

he failed to do so by only carrying out a GEB during the processing, with which the chief of police in

has acted contrary to Article 4c of the Wpg.

In a letter dated 16 December 2021, the AP sent the Chief of Police an intention to enforce.

On 21 January 2022, the Chief of Police submitted a written opinion on this intention and the

research report on which it is based. An opinion hearing will be held on 22 February 2022

took place during which the Chief of Police further explained his written opinion orally.

1 Gemeentebld 2020, 85971. Officially announced on March 30, 2020: <https://www.rijnmondveilig.nl/lichameijke-emergency/emergency-regulation-covid-19-30-march-2020/>

2 The police appeared not to have been formally involved in the decision to deploy the MCAs.

Public version

2/18

Date

November 17, 2022

Our reference

z2021-17798

2 Factual findings

5

6

7

8

9

10

The following is a summary of the relevant facts established in the investigation report. The

The Chief of Police has not contradicted the facts laid down in the investigation report.

2.1 The use of MCAs

In May 2020, the Eurovision Song Contest would have taken place in Rotterdam. In the context of the preparations for the safety measures surrounding this event, the desire has arisen to implement MCAs to make. Subsequently, the Supervision and Enforcement Department of City Management of the municipality of Rotterdam for the period 1 April to 1 June 2020, the rental of two MCAs has been realized. Day after the municipality Rotterdam had signed the rental offer became the Eurovision Song Contest because of the COVID-19 pandemic cancelled.

Subsequently, a plan was devised to deploy the two leased MCAs in the context of enforcement of the corona measures. In a memo of April 1, 2020, the mayor of the municipality of Rotterdam notified in writing by the Safety Directorate of the intention to deploy the MCAs.

The memo in question explains that the corona measures require a lot of effort from enforcers and police would ask when capacity was scarce. The MCAs could support these parties in the performance of their duties. In addition, the memo explains that the authority to mobile using camera surveillance to maintain public order in the event of a (threatened) disruption of the public order is based on Article 3 of the Police Act and that the MCAs are based on this basis and for this purpose would be deployed temporarily, namely as long as the emergency ordinance was applicable in the Safety region Rotterdam-Rijnmond.

As of April 10, 2020, the two MCAs have actually been deployed. At the request of the police, the MCAs have run out. However, it was halted on April 17, 2020, because its deployment had taken place without the involvement of the Police.

Subsequently, the police and the municipality of Rotterdam jointly drew up a deployment framework for the deployment of the MCAs. The deployment box contains a description of the purpose for which the MCAs were created used, the legal framework and the practical procedure that had to be followed.

According to the deployment framework, the deployment of the MCAs served a multiple purpose. The MCAs became used to obtain an up-to-date picture of the situation on site and, on that basis, to deploy capacity of special investigating officers and police officers.

In addition, the MCAs would have a preventive effect and the presence of camera surveillance can have a de-escalating effect.³

³ According to the deployment framework, violent incidents in the enforcement of the rules from the emergency ordinance were one of the reasons for deployment of the two MCAs.

Public version

3/18

Date

November 17, 2022

Our reference

z2021-17798

11

12

13

14

15

It also follows from the deployment framework that the MCAs are deployed as flexible camera surveillance on the basis of Article 3 of the Police Act, that responsibility for deploying the two MCAs lay with the police and that the deployment of the MCAs would in any event last as long as the emergency ordinance was in effect.

In addition, it follows from the deployment framework that from 26 April 2020 the two MCAs were controlled by a

employee of Supervision and Enforcement of the municipality of Rotterdam with a boa certification. The driver was given a list of pre-designated areas and locations at the start of the shift.⁴ The camera could only be turned on at the designated location if there was group formation or any other observable violation of the emergency ordinance. The camera was allowed during the ride location A to location B cannot be turned on. In exceptional cases, the MCAs were allowed to use camera images continue to deploy units due to the de-escalating effect.

On April 25, 2020, the members of the Rotterdam triangle⁵ approved the deployment framework, subject to the condition that some adjustments were made. The two MCAs are the following day, so from 26 April 2020, deployed again between 12:00 and 23:00.⁶ The police evaluation, among other things, shows that the MCAs have driven daily up to and including 31 May 2020.

2.2 Collecting, receiving, viewing and forwarding camera images

The rental quote from the MCAs shows that both cars were equipped with a so-called 'Rooftop Unit' with which camera images could be made by means of a so-called 'Panorama Video Subsystem'. It follows from the system specifications that there was HD megapixel image format and that the panoramic cameras contain 2 megapixel color sensors and a good image with sufficient detail could give. It also follows from the rental offer that each of the MCAs could take camera images from one to ten meters around the vehicle. This is clear from the detailed explanation of the 'Panorama Video Subsystem' camera images could be taken on both sides of the vehicle with a large opening angle.

According to the rental offer, the MCAs could drive sharply at a speed of fifty kilometers per hour take camera pictures.

It follows from the camera images checked by AP supervisors that they show a lot of detail and the cameras have also made sharp camera images while driving. The cameras were used from four angles images made: left front, right front, left rear and right rear. This together gives a 360 degree overall picture of the situation around the vehicle. From the advanced and awaited camera footage It follows that CCTV footage was taken far beyond the vehicle. Let the camera images park,

⁴ These areas and locations were determined by the Large-Scale and Special Operations Corona Staff. The Chief Duty Officer

of the police, with the intervention of the Operations Center of the police, could provide additional information.

5 The triangle of a certain area is the consultative body between the mayor, the (chief) public prosecutor and the chief of police or

police team chief of the team that includes the municipality in question – in this case the municipality of Rotterdam.

6 City Management Supervision, Police and Security Directorate, Evaluation Pilot deployment mobile camera car dated 15 July 2020, p. 5 (file item 43).

Public version

4/18

Date

November 17, 2022

Our reference

z2021-17798

see public roads, residential areas, shopping areas, beaches, boulevards and parking lots, where adults and children are recognizable.

16 An image processing system, the so-called ScanGenius, was mounted on each of the two MCAs SMART system. The research report established that as of April 26, 2020 – the start date of the deployment of MCAs – the camera images taken by the two MCAs were made live sent to the so-called 'Control Room Enforcement': the central control room of the Enforcement Service of the municipality of Rotterdam, which is located at Kleinpolderplein⁷.

17

18

19

20

These camera images received in the Enforcement control room were then sent via a data line forwarded to the so-called 'camera surveillance viewing room', which is located at the same location. The camera images came in here in the program 'Genetec' and then with the program

'Coppweb' watched live by authorized operators of the municipality of Rotterdam under supervision from the police.⁸

The camera images could - also with the help of the program 'Coppweb' - be further forwarded to several other police departments.⁹ The investigation report established that the camera images were actually forwarded to other police locations on a number of occasions.¹⁰

2.3 Keeping and destroying camera images

The camera images of the MCAs that did not contain any incidents were kept for seven days and subsequently destroyed. In the event of incidents, the camera images were recorded at the viewing area in accordance with the Wpg

camera surveillance. The GEB adopted on May 26, 2020 recommends that the retention period for reduce camera footage from the MCAs from seven days to zero without incident. In the evaluation, this recommendation has been repeated and it has also been noted that the camera images are unnecessary preserved.

It is also stated in the GEB that the stored camera images, in line with Article 14 of the Wpg, are via a automated provisioned process were destroyed, including backups.

⁷ A 4G SIM card in the processing unit of the image processing system provided the link.

⁸ At the camera surveillance viewing centre, camera images are automatically included in the Genetec basic program. It program Coppweb makes it possible to view live images from Genetec.

⁹ The supervisor could possibly decide to forward the camera images to the Police Operations Centre.

The camera images from the Operations Center could then be forwarded to the Police if necessary Coordination Center at a police station or to the appropriate screens in the area of the District Approach Team from the police.

¹⁰ The research report established that findings made using the MCAs – after an assessment by a supervisor in the Kleinpolderplein viewing area and the Police Operations Center – several times led to the deployment of the police.

Public version

Date

November 17, 2022

Our reference

z2021-17798

2.4 Carrying out a data protection impact assessment

21

22

23

The investigation report establishes that [CONFIDENTIAL] the police have a so-called pre-GEB established on May 10, 2020. According to the pre-GEB, this document is intended to assess whether performing a GEB is required. It was concluded in the pre-GEB that this is not the case was necessary for the deployment of MCAs.

According to the pre-GEB, the use of MCAs would, among other things, not involve systematic and large-scale monitoring in public space, because it concerned a limited number of locations where camera images could be made and the camera would only turn on if required was the cause. Also, according to the pre-GEB, there was no large-scale processing, because there no camera images of large groups of people would be made. The size of the group according to the pre-GEB depended on the extent to which the permitted number of persons was based of the emergency ordinance was exceeded. Moreover, according to the pre-GEB there was no question of a new technology, because cameras that have been installed pursuant to Article 151c of the Municipal Act be able to record camera images from multiple angles.

This follows from the evaluation in response to questions from the Rotterdam city council and questions from the AP the police and the municipality of Rotterdam have jointly drawn up a GEB. This follows from the GEB the GEB has been finalized and approved on May 26, 2020 by [CONFIDENTIAL] the municipality Rotterdam and the police [CONFIDENTIAL].

2.5 Conclusion

It follows from the foregoing that the MCAs have been deployed from 26 April 2020, and that the police and the municipality Rotterdam have established a final GEB on May 26, 2020.

3 Assessment

3.1 Applicability of the Police Data Act and competence of the Dutch Data Protection Authority

3.1.1 Legal framework

25 The General Data Protection Regulation (hereinafter: AVG) contains a general regulation for the protection of personal data that is directly applicable in all EU Member States. For the protection of personal data processed by the police and judiciary in the context of their

task performance, Directive 2016/680 has been established (hereinafter: the Directive¹¹). Member States serve this

11 Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection and prosecution of criminal offenses or the enforcement of sentences, and on the free movement of such data and repealing Framework Decision 2008/977/JHA.

Public version

6/18

Date

November 17, 2022

Our reference

z2021-17798

Directive into their national law. The Netherlands has implemented the Directive in the

Wpg.¹²

It follows from Article 2, second paragraph, opening words and under d, of the GDPR that the GDPR does not apply to the processing operations that fall within the scope of the Directive. The AVG and the Directive - as in the Netherlands implemented in the Wpg – are therefore mutually exclusive.

Article 2(1) of the Wpg stipulates that the Wpg applies to the processing of police data by a competent authority that are included in a file or are intended to be therein

to be included.

Article 1, preamble and under I of the Wpg defines a competent authority as any government agency which is competent for the tasks referred to in part a, or any other body or entity that is authorized to exercise public authority and public powers in view of the tasks referred to in part a.

26

27

28

29 Pursuant to Article 1, preamble and under a, of the Wpg, police data is “any personal data that is processed in the context of the performance of the police task, referred to in Articles 3 and 4 of the Police Act 2012”.

30

31

32

Pursuant to Article 3 of the Police Act, the police are responsible for ensuring effective enforcement of the rule of law and the provision of aid to those in need. The actual enforcement of the legal order is divided into criminal enforcement of the legal order and enforcement of the public order.¹³

It follows from Article 35 of the Wpg that the AP is authorized to supervise the processing of personal data in accordance with the provisions of and pursuant to the Wpg.

3.1.2 Assessment

It follows from the established facts that the camera surveillance with the use of MCAs during the research period has been carried out by a competent authority, namely the police. The deployment framework stipulates that the police was responsible for deploying the MCAs. Furthermore, established facts show that the police was in charge of looking out and possibly transmitting the camera images. In addition, the MCAs are deployed for the purpose of maintaining public order, as part of the police task. As

has been explained above, the deployment framework stipulates that the deployment of the MCAs took place on the basis of 12 Stb. 2018, 401.

13 Articles 11 and 12 of the Police Act.

Public version

7/18

Date

November 17, 2022

Our reference

z2021-17798

33

34

Article 3 of the Police Act, namely to make the corona measures more efficient and targeted to enforce.

It also follows from the established facts that the camera images were recorded in a file. The camera images entered the program 'Genetec' and could be viewed and possibly forwarded using the program 'Coppweb'. This is also evident from the established facts CCTV footage was kept for seven days.

3.1.3 Conclusion

The AP concludes that camera surveillance with the use of MCAs in the research period has taken place by a competent authority in the context of the performance of the police task and that the camera images were recorded in a file. Insofar as this involved the processing of police data (see section 3.2 of this decision), this processing falls within the scope of the Wpg and the AP is authorized to supervise this and to take enforcement action.

3.2 Processing of police data and responsibility for processing

3.2.1 Legal framework

35 Pursuant to Article 1, preamble and under a, of the Wpg, police data is "any personal data that

36

37

38

is processed in the context of the performance of the police task, referred to in Articles 3 and 4 of the Police Act 2012”.

Article 1, preamble and under b, of the Wpg defines personal data as “all information about a identified or identifiable natural person”.

Article 1, preamble and under c of the Wpg stipulates that the processing of police data is means “any operation or set of operations relating to police data or any set of police data, whether or not performed by automated means, such as collecting, recording, organize, structure, store, update or change, retrieve, consult, use, provide by by means of forwarding, distributing or otherwise making available, bringing together, with each other linking, blocking or destroying police data.

Article 1, preamble and under f, part 1, of the Wpg stipulates that the controller for the processing of personal data by the police is the chief of police, as referred to in Article 27 of the Police Act 2012.

Public version

8/18

Date

November 17, 2022

Our reference

z2021-17798

39

40

41

3.2.2 Assessment

Personal data

It follows from the established facts that camera images were made with the MCAs on which identified or identifiable natural persons were observable. From the technical specifications show that camera images could be made with a 'Rooftop Unit'. In addition, it turns out from the facts established in the investigation report, camera images were made with the two MCAs on which people were recognizable in the image that it was also the intention to be able to do people identify. For this reason, for example, no 'blurring' was applied.

Police data

The established facts show that these personal data are processed in the context of the implementation of the police task. As explained above, maintaining public order is part of the police task as referred to in Article 3 of the Police Act. The camera images that were taken with the MCAs made were used for maintaining public order, more specifically for maintaining the corona measures.

Processing

It has been explained above how the camera images were collected, sent, received, looked for, forwarded, stored and destroyed. It has also been established that the two MCAs actually do CCTV footage was collected during the deployment. The camera images were taken from the MCAs forwarded directly to the Enforcement control room. The received camera images were then forwarded via a data line to the camera surveillance viewing room and there under the direction of the police watched. In addition, it was established that the camera images could be forwarded further to other police locations, which also happened a few times. Furthermore, it is established that the CCTV footage was retained and destroyed after seven days.

Controller

42 It has been explained above that the members of the Rotterdam triangle on 25 April 2020 under the condition of some adjustments have been agreed to the deployment framework, after which the MCAs were approved on 26 April 2020 on the basis of

of Article 3 of the Police Act have been deployed under the responsibility of the police. From the legal framework follows that the Chief of Police is designated by law as the controller for the processing of police data with the police. The AP therefore concludes that the chief of police qualifies as controller for processing camera images using the MCAs.

Chief of Police's views

The Chief of Police notes that the implementation of both the GEB and the pre-GEB is a joint process from the municipality and the police. After all, decision-making about the use of the MCAs lay with the Rotterdam triangle and around camera surveillance – both on the basis of Article 151c of the Municipalities Act and on pursuant to Article 3 of the Police Act – the municipality had the impression that there was joint

43

Public version

9/18

Date

November 17, 2022

Our reference

z2021-17798

controller. This was partly prompted by the text on the AP's website on that moment.

Reply AP

44 The AP sees the administrative context within the Rotterdam triangle and the situation in which the police act as the

45

municipality of Rotterdam were located, as well as the circumstance that at the time of the proposed processing at the municipality of Rotterdam there could be uncertainty about the question of who if controller had to apply to the processing of camera images on the basis of Article 151c of the Municipal Act. In that context, it is conceivable that both the police and the municipality of Rotterdam should take action

felt responsible to strive for a jointly supported analysis of the possible effects of the (intended) processing of the camera images on the protection of personal data.

From, among other things, the memo of April 1, 2020 from the Directorate of Security to the mayor and the

However, the deployment framework established by the Rotterdam triangle on 25 April 2020 shows that the MCAs are flexible camera surveillance were not deployed on the basis of Article 151c of the Municipalities Act, but on the basis of Article 3 of the Police Act. The deployment framework also shows that responsibility for the deployment of the MCAs lay with the police. The basis for and responsibility for the use of this resource existed therefore no ambiguity at the municipality of Rotterdam. From the legal framework set out above it follows conclusively that the police data was processed for the purpose of the chief of police is the controller. The fact that the municipality may have doubts about this cannot change this. In in any case, the text of the AP's website that reads at that time cannot provide a concrete reason have formed for this purpose, since that text only related to Article 151c of the Municipalities Act and not Article 3 of the Police Act.

3.2.3 Conclusion

46 Based on the foregoing, the AP concludes that the camera images contain information about identified or identifiable natural persons and that this was the case personal data within the meaning of Article 1, preamble and under b, of the Wpg. These personal data were processed in the context of the performance of the police task and therefore constituted police data such as referred to in Article 1, preamble and under a, of the Wpg. Collecting, sending, receiving, looking, forwarding, storing and destroying police data were processing of police data as referred to in Article 1, preamble and under c, of the Wpg. The Chief of Police qualifies as controller for processing camera images with the MCAs, as referred to in Article 1, preamble and under f, part 1, of the Wpg.

Public version

Date

November 17, 2022

Our reference

z2021-17798

3.3 Carrying out a data protection impact assessment

47

48

49

50

51

3.3.1 Legal framework

Article 4c, first paragraph, of the Wpg stipulates that in the case of a type of processing, in particular a processing involving the use of new technologies, having regard to the nature, scale, context or its purposes is likely to pose a high risk to the rights and freedoms of individuals, the controller carries out an assessment of the effect prior to processing of the intended processing activities on the protection of personal data.

3.3.2 Assessment

Article 4c of the Wpg provides for the obligation to monitor the processing of police data are likely to pose a high risk to the rights and freedoms of individuals to carry out a GEP.

This applies in particular to processing operations involving the use of new technologies.

Article 35, first paragraph, first sentence of the GDPR contains an identically formulated obligation processing of personal data that falls within the scope of the GDPR.

Probably high risk

The established facts show that there is an innovative application of new technology or organizational solutions. Having regard to the nature, scope, context and purposes of the processing of camera images using the two MCAs, the processing likely posed a high risk

for the rights and freedoms of individuals. The AP explains this below.

It follows from marginals 47 and 48 of this Decree that the obligation to carry out a GEB is particularly becomes apparent in processing operations involving the use of new technologies. The use of such after all, technologies may involve new forms of data collection and use, possibly with a high risk to the rights and freedoms of natural persons.¹⁴

It was determined for this that cameras were mounted on the roof of the two MCAs with which 360 degree camera images could be made. These cameras were intended to provide a good image with sufficient detail up to ten meters around the vehicle. Even at a speed of fifty kilometers per hour, these cameras make sharp images. It has also been established that people, including children, were portrayed recognisably. Although the technique of making 360 degree camera images is not new in itself, the use of such cameras on (fast) driving cars do. Under these circumstances, making sharp images of people with these cameras is very important in the opinion of the AP an innovative use of this technology. Unlike, for example, the

14 Compare recitals 89 and 90 of the GDPR, as well as Guidance on data protection impact assessments and determining whether

processing is “likely to involve a high risk” within the meaning of Regulation 2016/679 (WP 248 rev.01), p. 12.

Public version

11/18

Date

November 17, 2022

Our reference

z2021-17798

use of 360-degree cameras with fixed camera surveillance or on a mobile mast, it uses such cameras on a moving car, for example, make it possible to follow people and of them camera images.

52 There was also monitoring of publicly accessible space, where personal data are processed

collected from both adults and children, in circumstances where they may not know that data is collected nor how it is used. Moreover, it can be done for people impossible to prevent them from meeting a public (or publicly accessible) space are subject to such processing.¹⁵ The MCAs actually have during the deployment period camera images made in, among other things, residential areas, shopping areas, parks, recreational areas and at beaches.

53

54

55

In addition, one of the purposes of using the mobile cameras was during the emergency ordinance to get an up-to-date picture in areas “where [were] known to have more during certain periods per day persons came together than [was] permitted”¹⁶. In view of this, the police had – unlike in the pre-GEB happened – have to take into account the possibility that (also) of large groups of camera images would be made and that this could transcend the character of incidental monitoring.

In view of the foregoing and the sensitive nature of the monitoring of public space, the processing of the camera images using the MCAs is likely to pose a high risk to the rights and freedoms of individuals.

Furthermore, the context in which and the purpose for which the camera images were made contribute to a increased risk to the rights and freedoms of individuals. The purpose of making the camera images was, after all, due to the more efficient and targeted enforcement of the corona measures in the emergency ordinance by enforcers and police. It is certain that the aim was also to identify persons and that a violation of the emergency ordinance could lead to the imposition of a fine. In addition the camera images were not only watched live but also processed further, now the camera images could and, where appropriate, were actually forwarded to other police locations.

Furthermore, the intention was to keep the camera images made with the MCAs for seven days as standard - a period to which attention has also been drawn in the finally drawn up GEB. In the case of one

incident, the camera images could be kept and used by the police (even) longer.

Conclusion

56 Based on the above, the AP concludes that the intended processing of the camera images

using the MCAs is likely to pose a high risk to the rights and freedoms of individuals

15 Compare Article 35(3) of the GDPR and Guidance on data protection impact assessments and determining whether a processing “is likely to involve a high risk” within the meaning of Regulation 2016/679 (WP 248 rev.01), p. 11.

16 See file document 42, 'Deployment frame Mobile Camera Vehicles (MCAs)', p. 1.

Public version

12/18

Date

November 17, 2022

Our reference

z2021-17798

57

58

yielded. The foregoing means that the chief of police was obliged to precede the intended processing of camera images to carry out an assessment of the effect on the protection of personal data.

Superfluously, the AP notes that this conclusion of the AP is in line with the decision of the AP in which the AP has established a list of processing operations for which a GEB is required under the GDPR. Also it follows from that decision that a GEB is required for fixed and flexible camera surveillance.¹⁷

Prior to processing

It follows from the foregoing that the chief of police was obliged to inform prior to the intended processing of camera images to carry out an assessment of the effect on the protection of personal data.

The AP has determined that the police and the municipality of Rotterdam have decided to jointly to carry out a GEB and that the municipality of Rotterdam and the police make this assessment on 26 May 2020

have completed. However, the processing has already started on April 26, 2020. With that, the chief of police failed to perform a GEB prior to processing camera images using the MCAs feed.

Chief of Police's views

59 The Chief of Police wishes to emphasize that at no point was any aspect ignored regarding compliance with the Wpg. According to the chief of police, this is also apparent from the fact that the pre-GEB has been carried out and with the outcome of that pre-GEB it was assumed that processing could be started become.

Reply AP

60 The DPA has established that the processing started on April 26, 2020, while the pre-GEB only received fourteen days later, namely on May 10, 2020. For that reason, there can be no question of outcomes that already in the pre-GEB. Moreover, in that pre-GEB, the police have the information referred to in paragraph 3.3.2. of this decision factors set out have not been sufficiently recognised, with the result that it has refrained from it at that time perform a GEB. The AP therefore concludes that attention has indeed been paid to aspects related to compliance with the Wpg in the sense that the police has drawn up a pre-GEB, but that attention was substandard.

61

3.3.3 Conclusion

The processing of camera images made using the MCAs involved processing of police data likely to pose a high risk to the rights and freedoms of individuals. For those this is why the chief of police had a GEB prior to the intended processing of those camera images

17 Decree on the list of processing operations of personal data subject to a data protection impact assessment (DPIA). is, stcrt. 2019, 64418, points 9 and 10.

Public version

Date

November 17, 2022

Our reference

z2021-17798

have to perform. Processing started on April 26, 2020, while there was no GEB at that time executed. Consequently, the Chief of Police acted in violation of Section 4c(1) of the Wpg.

4 Fine

4.1 Introduction

62 Prior to the intended processing of police data, the Chief of Police failed to – namely creating camera images using two MCAs – one GEB to run while that processing was likely to pose a high risk to the rights and freedoms of individuals. With this the Chief of Police has violated Article 4c(1) of the Wpg. The AP sees this as a reason to comply with the to impose an administrative fine on the chief of police. The AP motivates this in the following.

4.2 Penalty Policy Rules of the Dutch Data Protection Authority 2019

63 Pursuant to Article 35c, preamble and under c, of the Wpg, read in conjunction with Article 23, fourth paragraph, of the Criminal Code, the AP is authorized in the event of a violation of Article 4c, paragraph 1, of the Wpg to impose an administrative fine not exceeding the amount of the fine of the fifth category, which at the time of the observed violation amounts to an administrative fine of ten highest € 87,000.¹⁸

The AP has established fining policy rules to implement the aforementioned power of fining under the Wbp19 (hereinafter: the Penalty Policy Rules). In those Fining Policy Rules, a categorization has been chosen and bandwidth system. Violation of Article 4c of the Wpg is classified in category III. Category III has a fine range between €30,000 and €83,000 and a basic fine of €56,500. This follows from Article 5, under 5.1 and 5.2 of the Fining Policy Rules.

65 The AP adjusts the amount of the fine to the factors referred to in Article 7 of the
Penalty policies, by lowering or increasing the base amount. It is an assessment of the
seriousness of the offense in the specific case, the extent to which the offense can be imposed on the offender
and, if there is reason to do so, other circumstances.

18 See Article I of the Decree of 31 October 2019 amending the amounts of the categories, referred to in Article 23, paragraph
4, of
the Criminal Code (Stb 2019, no. 399).

19 Fining 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), Stcrt. 2019, 14586, March 14, 2019.

Public version

14/18

Date

November 17, 2022

Our reference

z2021-17798

4.3 Fine amount

66

67

A DIA is a process that is intended to describe the processing of personal data, the necessity
and proportionality and the related risks to the rights and freedoms of
help individuals manage by assessing these risks and determining measures to mitigate them
to deal with. It is an important accountability tool because it is a
not only helps the controller to meet the requirements of – in this case – the Wpg,
but also to demonstrate that appropriate measures have been taken to ensure that the
Wpg regulations regarding data protection are complied with. The police have –
in violation of the statutory provision – only decided during the processing to carry out a GEB, and

not prior to the intended processing. And also while executing that GEB are the processing continued. In view of this, the AP considers the violation serious so that the imposition of a fine is appropriate.

As explained above, violation of Article 4c of the Wpg is classified in the Fining Policy Rules category III, with a range of fines between a minimum of €30,000 and a maximum of €83,000 and a basic fine of €56,500.

68 The AP sees no reason to increase the basic amount of the fine on the basis of the provisions of Article 7 of the Reducing or increasing the penalty policy rules in the circumstances mentioned.

4.3.1 cooperation with AP investigation

Chief of Police's views

69 The chief of police requests the AP to take into account in its assessment that both the municipality and the police have all
70

71

cooperated with the AP's investigation.

Reply AP

It has been established that both the municipality of Rotterdam and the police have fully cooperated in the investigation by the AP. However, the AP is of the opinion that this cooperation has not gone beyond the statutory obligation pursuant to Section 5:20 of the General Administrative Law Act (hereinafter: Awb). For a
There is therefore no reason to reduce the fine.

4.4 Blame and Proportionality

It follows from the foregoing that the AP sets the fine amount at the basic fine of € 56,500. Finally
Pursuant to Articles 3:4 and 5:46 of the Awb, the AP assesses whether the application of its policy for
determine the amount of the fine given the circumstances of the specific case, not to one
disproportionate outcome.

Public version

Date

November 17, 2022

Our reference

z2021-17798

4.4.1 Culpability

Chief of Police's views

72 The Chief of Police argues, insofar as relevant here, that it must be recognized that a pre-GEB has been which concluded that a GEB was not necessary. In response to questions then performed a GEB. In this respect, therefore, there is no question of fault or negligence chief of police.

Reply AP

73 Since this concerns a violation, the imposition of an administrative fine is in accordance with fixed rules

74

case law does not require the AP to demonstrate that there is intent and the AP may be culpable assume if the perpetrator is established.

As explained above, the chief of police was legally obliged to enter prior to processing carry out a GEB within the framework of the deployment of the MCAs. In the opinion of the AP, in the implementation of the pre-GEB wrongly failed to recognize by the police that there was indeed a high risk for the rights and freedoms of individuals. This should have been expected of the police. It is therefore to reproach the Chief of Police – as controller – for not complying with the provisions referred to in Article 4c of the Wpg has fulfilled the obligation laid down.

75 It is not in dispute that the police (together with the municipality of Rotterdam) drew up a pre-GEB with the purpose of determining whether a GEB must be executed. However, this pre-GEB was not established until May 10, 2020, therefore fourteen days after the start of the deployment of the MCAs and (i.e. after the start of) the processing of the personal data. It would have been the police's way to wait with the deployment of the MCAs until

at least the moment when the pre-GEB would have been established. The circumstance that the police and the municipality of Rotterdam were already working on the implementation of the pre-GEB before May 10, 2020 - such as the Chief of Police stated during the opinion hearing – this does not change this. In addition, the police have processing also continued during the preparation of the GEB, with which the chief of police essentially meets the meaning of a GEB passes.

4.4.2 Proportionality

76 The AP is of the opinion that (the amount of) the total fine amount is not disproportionate in itself.²⁰

In this opinion, the AP has taken into account the seriousness of the infringement and the extent to which it is attributable to the chief of police

can be blamed. The fine is also in line with the meaning and role of a GEB in the processing of personal data, namely improving data protection in processing operations likely involve high risks related to the rights and freedoms of natural persons.

²⁰ See also marginals 66 to 75 for the justification.

Public version

16/18

Date

November 17, 2022

Our reference

z2021-17798

77

In this specific case, however, the AP takes into account that the deployment of the MCAs took place at the beginning of the COVID-19 outbreak in the Netherlands, namely in April and May 2020. At that time there was a national crisis situation with many uncertainties, in which the authorities were faced with the task of to quickly record and immediately implement measures to combat the COVID-19 outbreak. In Rotterdam, where the infections rose quickly, this led, among other things, to the proclamation of the so-called GRIP 4 situation.²¹ In view of this and in view of the impact that the (combating the) pandemic will have on

At the time, maintaining public order in a city like Rotterdam, the municipality stood Rotterdam and the police together for the task of immediately proceeding to active monitoring of the in measures included in the emergency ordinance, and where necessary direct enforcement thereof. That special circumstance makes it explicable for the AP that the chief of police has ordered the execution of a (complete) GEB less prominent on the retina prior to the processing of the camera images at least that the chief of police could have felt compelled to do so in view of those circumstances to make a decision.

78 Based on these circumstances, the AP sees reason to reduce the fine. The AP considers this case a fine of € 50,000 is appropriate and required.

4.5 Conclusion

79 The AP sets the total fine amount at €50,000.

21 GRIP stands for Coordinated Regional Incident Response Procedure. GRIP relates to the organization of the disaster and crisis management by the emergency services of the security region. The GRIP structure is in life called to organize the upscaling of the emergency services in an orderly manner. There are five scale-up levels, with GRIP I is the lowest level and GRIP V is the highest level.

Public version

17/18

Date

November 17, 2022

Our reference

z2021-17798

5 Operative part

The AP will issue an administrative order to the chief of police for violation of Article 4c, first paragraph, of the Wpg. fine in the amount of: € 50,000 (in words: fifty thousand euros).²²

Yours faithfully,

Authority for Personal Data,

e.g.

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. 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.

22 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, of the 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.

Public version