Confidential/Registered

Municipality of Enschede

Board of Mayor and Aldermen

PO box 20

7500 AA ENSCHEDE

Date

March 11, 2021

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 Mayor and Aldermen of the Municipality of Enschede,

The Dutch Data Protection Authority (AP) has decided to inform the mayor and aldermen of

to impose an administrative fine of € 600,000 on the municipality of Enschede (the Municipal Executive of Enschede).

The Municipal Executive of B&W Enschede has processed personal data of owners/users without any basis

of mobile devices with Wi-Fi enabled in the city center of Enschede. With that has

the Municipal Executive Enschede article 5, first paragraph under a, jo. Article 6, paragraph 1 of the General

Data Protection Regulation (GDPR) violated.

The decision is explained in more detail below. Chapter 1 is an introduction and Chapter 2 describes it

legal framework. In chapter 3, the AP assesses whether personal data is involved, the

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

penalty worked out and chapter 5 contains the operative part and the remedy clause.

1

Our reference

[CONFIDENTIAL]

Date

March 11, 2021

1 Introduction

1.1 Concerned Government Agency

This decision concerns the Municipal Executive of the municipality of Enschede

(hereinafter: the B&W Enschede Board). On July 17, 2018, the AP received a complaint from a complainant with

in it the request to impose a corrective measure on the municipality of Enschede. The complainer

explained that there are sensors in the city center of Enschede that record data from people passing by

who have turned on the Wi-Fi on their phone. Collecting and processing this data

According to the complainant, this is done without a basis within the meaning of Article 6, paragraph 1, of the General

Regulation

data protection (hereinafter: AVG). The AP then started an investigation into compliance with the GDPR

by the B&W Enschede college. During the investigation, the AP received two similar complaints.

1.2 Process flow

During the investigation, the AP requested information from the Municipal Executive of B&W Enschede and from Retail

Management Center B.V. (hereinafter: Bureau RMC), the organization commissioned by the Municipal Executive

Enschede provides the WiFi measurements in the city center of Enschede. The AP also has information

requested from [CONFIDENTIAL] (hereinafter: [CONFIDENTIAL]), the organization that Bureau RMC

in turn hires for the management of the sensors and for processing all data associated with the

sensors are collected. In addition, on May 29, 2019, supervisors of the AP conducted an investigation

done on site at a number of shopkeepers in the city center of Enschede where a sensor was installed. The same one day other supervisors of the AP at the office of Bureau RMC in Amsterdam have a statement taken from the director of Bureau RMC and two employees of [CONFIDENTIAL] and documents copied and data requisitioned on the spot.

In a letter dated 8 May 2020, the AP has sent the Municipal Executive of Enschede an intention to enforce sent. Also given the opportunity to do so by the AP in this letter, the Board of B&W Enschede on July 14, 2020, issued a written opinion on this intention and the implications thereof basis report. The AP subsequently requested further information on 14 January 2021 this view.

2. Legal framework

2.1 Scope GDPR

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, for the purposes of this Regulation:

1. “Personal Data”: any information relating to an identified or identifiable natural person (“the data subject”); […].

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 natural or legal person, a public authority, a agency or other body which, alone or jointly with others, determines the purpose and means of the

determines the processing of personal data; when the objectives of and the means for this

processing are set out in Union or Member State law, they may specify who

the controller is or according to which criteria it is designated; […].

2.2 Lawfulness of the Processing

Article 5, first paragraph, preamble and under a of the GDPR stipulates, among other things, that personal data must be

processed in a manner that is lawful in relation to the data subject.

Article 6, first paragraph, of the GDPR then provides an exhaustive summary of the basis for a

lawful data processing. This article states that processing is lawful only if and for

insofar as at least one of the six principles referred to has been met. The for the college B&W Enschede

any eligible bases are: 1

c) the processing is necessary for compliance with a legal obligation to which the

controller rest;

e) the processing is necessary for the performance of a task carried out in the public interest or for a task in

in the exercise of public authority vested in the controller

instructed;

f) the processing is necessary for the purposes of the legitimate interests of the

controller or of a third party, except where the interests or fundamental rights and the

fundamental freedoms of the data subject that necessitate the protection of personal data

outweigh those interests, in particular where the data subject is a child.

3. Assessment

3.1 Processing of personal data

3.1.1 Introduction

The Municipal Executive of Enschede has had WiFi measurements carried out with the aim of measuring the effects of

investments by the municipality of Enschede in the city center with a view to responsible use of

public funds. The AP will first assess whether the data that is processed for these WiFi measurements

are personal data within the meaning of Article 4(1) of the GDPR.

1 In the present situation, no permission has been requested from the data subjects (ground a), the Wi-Fi measurements are not necessary
performance of a contract with the data subject (ground b) and they are also not necessary to protect certain vital interests protect (ground d).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

3.1.2 Facts

Given the extensive investigation into this case, the AP refers to the first chapter for the facts of Annex 1 to this Decision. Below is a brief summary of the facts, after which the AP comes to a judgment.

The Municipal Executive of Enschede has taken the decision to start 24/7 on September 6, 2017 measurements via sensors in the city center of Enschede. The Municipal Executive of Enschede has this assignment awarded to City Traffic B.V., now Bureau RMC. Bureau RMC subsequently [CONFIDENTIAL] hired for the installation and maintenance of the sensors in the city center of Enschede and for collecting and validating the data collected with the sensors.2

In the investigation, the AP has found that eleven sensors have been installed since at least May 25, 2018 various shopkeepers in the city center of Enschede. Each sensor has a range of up to 20 to 30 meters. The sensors have from this date of all mobile devices within range on the WiFi was enabled the MAC address, signal strength, date and time were captured and temporarily stored in the working memory of the sensor. This storage lasted as long as the device was within range of the sensor was plus two minutes. The AP also notes that the sensors scan continuously. Furthermore has the AP determined that each device detected upon entry and two minutes after leaving it range of the sensor in real time the following data has been sent to the server: status 1 or 2,

pseudonymised MAC address, signal strength, date and time, spoofed indicator and sensor ID.

One and the same pseudonymization method runs on all sensors and this method has been used since May 25, 2018 not changed. The pseudonymization results in one MAC address on each of the sensors one and the same pseudonymised MAC address.

The data measured in one day by the sensors in the city center of Enschede will be collected daily in a short-term table. The time of day when the device is through the sensor scanned is recorded accurately to the second. In the period up to January 1, 2019 it is pseudonymised MAC address not truncated upon entry to the server, in the period from January 1 2019 yes. Trimming involves removing [CONFIDENTIAL]. The other data that is sent to the server, namely sensor ID, date, time, signal strength, status and spoofed indicator have been adopted unprocessed in the short-term table.

Each night, two filters were applied to the short-term table, namely an opt-out filter and an opt-out filter resident filter. These filters have the effect that certain records from the short-term table are not end up in the long-term table. The AP has established that the residents filter does not include all residents filters out and that incorrect information is given about this on the municipality's website.

After applying the filters to the short-term table, two consecutive records of the same result (truncated) pseudonymised MAC address to one record in the long-term table. From May 25, 2018 to on January 1, 2019, the long-term table contained the following data: pseudonymised MAC address,

2 The AP will discuss the relationship between these parties in more detail in section 3.2.

date, TimeIn, TimeOut, Retention, SignalStrengthIn, SignalStrenghtOut. Transferred on January 1, 2019 on the clipping of the pseudonymised MAC address and the pseudonymised MAC address was

data replaced with the truncated pseudonymised MAC address. The AP also notes that in the long-term table as of May 25, 2018 contained data over a period of between six and seven months.

The Municipal Executive of B&W Enschede has received estimates of various variables about unique visitors to the city center of Enschede. For this purpose, the applicable data in the long-term table deduplicated based on the truncated pseudonymised MAC address and then certain statistical calculations are applied to it.

On April 30, 2020, the Municipal Executive of Enschede instructed Bureau RMC to 2020 to turn off the sensors. The sensors will no longer provide counting data from May 1, 2020.3

The AP has established that from at least May 25, 2018 to May 30, the Municipal Executive of Enschede April 20204 processed data from roughly 1.8 million unique mobile devices and that the number of detections will be significantly higher.

The AP subsequently established that the long-term table after 1 January 2019 clearly shows living patterns can be distilled. Given the regularity of the patterns it can be reasonable concluded that the records associated with the pattern belong to one mobile device. The lifestyle patterns can, for example, reveal a person's place of residence or place of work, but also more sensitive data such as visits to medical institutions.

The AP further notes that Bureau RMC in its privacy protocol, which specifically pertains to processing via the City Traffic method, has recorded that it and/or its partners as of at least May 25, 2018 process personal data within the meaning of the GDPR. Bureau RMC also has in its privacy protocol included that the reports that clients receive from Bureau RMC do not contain any personal data contain.

3.1.3 Assessment

During the processing process (from detection by a sensor to storage in the long-term table) there are different sets of data. These sets are shown in the table below, where a distinction is made between the period prior to the introduction of the pruning of

pseudonymised MAC addresses (May 25, 2019 – January 1, 2019) and the period after the implementation of this trim (January 1, 2019 – April 30, 2020).

3 Letter of 16 February 2021 from the Municipal Executive of B&W Enschede to the AP, page 3 and appendix 2.

4 In the period from 10 December 2018 to 3 January 2019, the Municipal Executive of B&W Enschede paused the Wi-Fi measurements. earlier
data collected during this period were stored in the long-term table, so data were transferred during this period processed by the B&W Enschede college. See also appendix 1, paragraphs 1.3 and 2.5.

May 25, 2018 - January 1, 2019

January 1, 2019 – April 30, 2020

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

Phase in
processing process

Temporary storage on
every sensor

Shipping to and
reception on the
server

Short-term table
the server

MAC address; signal strength; Date;
Time of day

Pseudonymized MAC address;

signal strength; Date; Time of day; Sensor-

ID; Status; Spoof indicator

Pseudonymized MAC address;

signal strength; Date; Time of day; Sensor-

ID; Status; Spoof indicator

long-term table

the server

ID; Pseudonymized MAC address;

Signal strengthIN; Signal strengthOFF,

Date; Time IN; Time OFF;

Dwell time; Sensor ID; BWCode

Same as prior to January 1

2019

Same as prior to January 1

2019

Clipped pseudonymized MAC

address; signal strength; Date;

Time of day; Sensor ID; Status; Spoofed

indicator

ID; Trimmed pseudonymised

MAC address; Signal strengthIN;

Signal strengthOFF, Date;

Time IN; Time OFF; Dwell time;

Sensor ID; BWCode

In the table above are the most valuable attributes in terms of being able to identify

natural persons in bold. On the one hand, it concerns the MAC address, first pseudonymised

and later trimmed, and on the other side the combination of Date, Time in seconds and Sensor ID.

This last combination very precisely represents when a mobile device was true; so this is one

location data. The AP therefore refers in this context to 'location data'.5

In addition, two shadings have been added to the above table, namely light gray for the

(pseudonymized) MAC address and dark gray for the truncated pseudonymized MAC address.

In the remainder of this section, the AP will demonstrate that all sets included in the table above

qualify data as personal data within the meaning of Article 4(1) of the GDPR.

Light gray areas: The MAC address or pseudonymised MAC address in combination with the location data

qualify as personal data within the meaning of the GDPR at every stage of the processing process

Article 4, preamble and part 1, of the GDPR stipulates that data qualifies as personal data if

it is information about “an identified or identifiable natural person”. From the first situation,

5 The European data protection supervisors already recognized in 2011 the location data of mobile devices

that these can reveal a lot about the owners of those devices. See also Pages 7 and 8 of WP185 Advice 13/2011 on

geolocation services on smart mobile devices: “Most people tend to keep their mobile devices close to them

such as in a trouser or jacket pocket, in a bag or on the bedside table next to the bed. (…) It rarely happens that someone like

this

loan the device to someone else. (…) For example, the place to sleep can be deduced from a pattern of inactivity at night and

from a

regular travel pattern in the morning the location of the employer.”

information about an 'identified person' is not the case in this situation because the identity

of the natural person does not follow directly from the MAC address or the pseudonymised MAC address

address and location information.

To be personal data, the data must therefore be information about an identifiable

natural person'. In this case, the natural person must be directly or indirectly identifiable

based on identifiers or characteristic elements. Possible identifiers in the present

situation may be: the MAC address, the pseudonymised MAC address and the location data.

A MAC address – if not spoofed6 – is a unique identification number of a mobile device.

Because mobile devices such as smartphones and tablets are very personal, the natural

person in question will be linked to the MAC address via his/her mobile device. This means that

a non-spoofed MAC address can be an identifier of a natural person.

The pseudonymised MAC address is, as explained in the facts, a translation of a MAC address

to another unique character string. As a result, the pseudonymised MAC address -

provided the underlying MAC address is not spoofed – an identifier of a natural person can

are.7

The location data is explicitly referred to as in Article 4, part 1, of the GDPR

possible identifier of a natural person since location data can reveal a lot about

the owner of the mobile device.

The question now is whether in each phase of the processing process on the basis of the aforementioned

identifiers a natural person can be identified. The AP describes each phase in the following

processing is an example of a way in which it was reasonably possible to process the

identify the natural person to whom the data relates.

Method 1: Identification of persons using the data stored on the sensor

During the investigation, the AP determined that the MAC address and location data become temporary

stored in the working memory of each sensor and that the pseudonymised MAC address and the

location data is sent to the server. [CONFIDENTIAL] is responsible for it

management of all sensors in the city center of Enschede and collecting the data. Bee

[CONFIDENTIAL] The exact location of the sensors is therefore known and people have access to it

working memory and the software that runs on each sensor.8 Simultaneously with a new detection of a mobile device through a sensor it is for example possible for someone from [CONFIDENTIAL] to be on site or to observe via a camera which person walks within the range of the sensor. Especially on

6 In this context, spoofing is an informal term for “MAC Address Randomization”, a technique by which part of the MAC address sometimes randomly changes for the purpose of reducing the ability to track a device through time and space.

7 See chapter 4 of WP 216 Advice 5/2014 on anonymization techniques.

8 For example, by logging directly into the sensor or by adding to their software code that it should become working memory written to another location where employees can access it.

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

quiet moments in the city center, this leads directly to the identification of the natural person. For control the person may be asked for his/her MAC address. The same way of identification is possible in the case of pseudonymised MAC addresses and the associated location data, because then too the moment of detection on the spot or via a camera the person in question can be observed.

Method 2: Identification of persons using the data in the short-term table (until January 1, 2019)

This way describes that, based on the data in the short-term table, it is also possible to calculate the identify natural persons. [CONFIDENTIAL] takes care of the collection and validation of the data. The short-term table is therefore held by [CONFIDENTIAL]. From mobile devices entering the range of a sensor, data with associated 'status 1' is recorded in the short-term table and if the same mobile device leaves the range of the sensor a little later, then data with status 2 is sent to the short-term table. However, if a mobile device stays within the range of a certain sensor, for example because that person lives within it or works, then the short-term table only contains a status 1 record with the

pseudonymised MAC address, Date and Time. If a status 2 record is not forthcoming for a longer period of time is it known to [CONFIDENTIAL] that the relevant resident or shop assistant is still within range of the sensor. Someone from [CONFIDENTIAL] can then be on site identify the person and identify the person.

Method 3: Identification of persons using the data in the long-term table (until 1 January 2019)

Finally, for [CONFIDENTIAL] it is also included in the historical data on the basis of the long-term table possible to identify natural persons. The AP has determined that in the long-term table after January 1, 2019, i.e. after the introduction of cutting, living and exercise pattern recognizable.9 This will also be the case in the long-term table before 1 January 2019, when there were still unique pseudonymised MAC addresses, because then also six months of data were kept. Using a pattern it is possible for [CONFIDENTIAL] to predict when the natural person in question is located somewhere, for example the person who every night between 04:00 and 05:00 moves between sensors in the city center of Enschede. During the night there are hardly any other people walking on the street and it is therefore possible for [CONFIDENTIAL] to ter identify this person locally or via a camera.

The above three examples of ways of identifying natural persons by [CONFIDENTIAL] has been taken into account recital (26) of the GDPR stating that account should be taken into account by all means reasonably expected to be used used by the controller or by another person to the natural person directly or indirectly identify". The AP concludes that the above three ways of identifying natural persons in view of the time, costs and manpower required [CONFIDENTIAL] require. The criteria from the judgment in Breyer v Germany10 have also been met, because the methods are neither prohibited by law nor impracticable in practice. That employees of

9 See also appendix 1, section 1.2, page 46 et seq.

10 CJEU, 19 October 2016, ECLI:EU:C:2016:779, r.o. 46.

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

[CONFIDENTIAL] do not use these resources in practice to target persons in the inner city of Enschede does not detract from the fact that they could reasonably do so.

In addition to identification by [CONFIDENTIAL], the AP notes that the identification is also by employees of Bureau RMC can be done. The AP has determined that Bureau RMC based on the service level agreement with [CONFIDENTIAL] has access to all data [CONFIDENTIAL] collected. In addition, the AP notes that even the B&W Enschede Board can do the identification, because it also has access to all data on the basis of the processing agreement with Bureau RMC.

If necessary, identification of the natural persons could also take place by the to link personal data collected with the sensors to the data collected via the various smart-city projects in Enschede.11

With regard to the use of MAC addresses and location data, it is noted that the predecessor of the AP in 2015 in a study of a company that provided WiFi tracking, ruled12 that the recording MAC addresses and location data via sensors qualifies as processing personal data because identification of the natural persons was possible on the above described Way 1.13 In addition, the joint European data protection regulators in their opinion on apps on smart devices stated that location data and unique identifiers of mobile devices are personal data.14 In their opinion about the proposed e-Privacy Regulation, they stated: 'In this context, it should be noted that these MAC addresses are personal data, even after security measures such as hashing have been undertaken."15

Based on the foregoing, the AP concludes that the combination of MAC address and location data and the combination of pseudonymised MAC address and location data on the sensor from May 25, 2018 to with April 30, 2020 and in the short- and long-term table until January 1, 2019 qualify as

personal data within the meaning of the GDPR.

11 www.smartenschede.nl

12 The report has been tested against the definition of personal data in Article 1 under a of the Personal Data Protection Act: 'every information relating to an identified or identifiable natural person". The current definition of personal data in the AVG is identical.

13 Section 5.1 of the final findings report 'Wifi tracking of mobile devices in and around stores by Bluetrace' (z2014-00944) of 13 October 2015. Can be found at www.autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-wifi-tracking-rond-winkels-vlucht-met-the law. At the time, the AP also informed the VNG by letter about its views on WiFi tracking: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_ap_vng_wifi-tracking.pdf.

14 WP202 Opinion 02/2013 on apps on smart devices, page 8. Available from the AP's website: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/downloads/int/wp202_en_opinion_on_mobile_apps.pdf

15 WP247 Opinion 01/2017 on Proposed Regulation for the ePrivacy Regulation, page 11. See also WP223 Opinion 8/2014: Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed. For instance, wearable things kept in close proximity of data subjects result in the availability of a range of other identifiers, such as the MAC addresses of other devices which could be useful to generate a fingerprint allowing data subject location tracking. The collection of multiple MAC addresses of multiple sensor devices will help create unique fingerprints and more stable identifiers which IoT stakeholders will be able to attribute to specific individuals. These fingerprints and identifiers could be used for a range of purposes, including location analytics7 or the analysis of movement patterns of crowds and individuals.

Such a

trend must be combined with the fact that such data can later be combined with other data issued from other systems (e.g.

CCTV or

internet logs). In such circumstances, some sensor data are particularly vulnerable to re-identification attacks.

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

From the privacy protocol of Bureau RMC and the infographic with which Bureau RMC explains

the City Traffic method, the AP concludes that Bureau RMC also believes that it and/or its partners

processed personal data up to the time of cutting off the pseudonymised MAC

address.

Dark gray areas: Trimming the pseudonymised MAC address does not eliminate all three risks

traceability, linkability and deducibility from which it is still personal data

the meaning of the GDPR

Bureau RMC states that the short and long-term table after the introduction of 'anonymisation on the

server' no longer contain personal data within the meaning of the GDPR. The infographic about the City Traffic

method16 formulates this as follows: “The anonymized code is now no longer traceable, linkable and

identifiable to a unique device. Our data therefore does not contain any personal data.”

The AP then concludes that the chosen anonymization method of (only) cutting off a

small part of the pseudonymised MAC address insufficiently reduces the risks of traceability,

excludes linkability and deducibility and that the data qualifies as personal data. The

AP explains this below.

Linkability

The risk of linkability exists if there is the possibility to have at least two records left

linking the same data subject or group of data subjects (in the same database or in

two different databases).

The AP finds that linking records about the same data subject or group of data subjects

actually takes place. This is because two consecutive records with the same clipping

pseudonymised MAC address in the short-term table linked and included in the

long-term table. In addition, the data in the long-term table is deduplicated based on the

truncated pseudonymized MAC address to serve as the basis for the college B&W grades

Enschede about unique visitors to the city center of Enschede. The AP also refers to the statement here

of the employees of [CONFIDENTIAL]17 that the loss of detail due to cutting off part of

the symbols of the hashed Mac address is limited so linking is still possible.

It follows from the foregoing that the chosen anonymization technique does not exclude the risk of linkability.

Since all three risks are required to be excluded, the conclusion can already be drawn now

that the anonymization technique fails and that re-identification of natural persons is possible. For the

for completeness, the AP also deals with the two other risks.

16 See appendix 1, section 1.2, figure 2.

17 See appendix 1, section 1.2, page 44.

Traceability

The risk of traceability is present if it is possible to identify a person in a dataset

individualize by highlighting certain records.

The AP has been able to demonstrate that clear living patterns can be derived from the long-term table. This

patterns are linked to one truncated pseudonymised MAC address, which means it is possible

is that the patterns contain the location data of multiple mobile phones. However, given the regularity of the patterns it can be reasonably concluded that all registrations belong until the pattern originates from a single mobile device, and therefore one natural person. This makes it possible to individualize a person. The AP therefore concludes that the risk of traceability cannot be ruled out.

Deducibility

A risk of deducibility is present if there is the possibility to determine the value of a deduce a personal characteristic with a high degree of probability from the values of a series of others attributes. From the three visualizations of the long-term table18, it is very likely that one value of a personal characteristic can be derived, for example the place to sleep or the location of the employer. The AP therefore concludes that clipping the pseudonymised MAC address also removes the risk of deducibility.

Based on the foregoing, the AP concludes that the short and long-term table are insufficiently resistant to re-identification.

In addition, the AP concludes that the combination of the clipped pseudonymised MAC addresses and the detailed location data in these tables qualify as personal data within the meaning of Article 4 part 1 of the GDPR, because the previously described ways 2 and 3 of identification also apply case of truncated pseudonymised MAC addresses. Way 2 works because it also works in the short-term table is visible if there is only a status 1 record, and so that the person belongs to it truncated pseudonymised MAC address is still within range of the sensor.

Someone from [CONFIDENTIAL] can then determine on the spot which person it is and the identify person. For way 3, the AP had already based it on the long-term table with truncated pseudonymised MAC addresses.

3.1.4 View of the Executive Board of B&W Enschede and response by AP

The main point of the B&W Enschede Board is that the Board only collects anonymous, aggregated data from Bureau RMC receives. Below is a summary of the view of the Municipal Executive of B&W Enschede

with the response of the AP.

Operation and storage sensors

As the Board of B&W Enschede of Bureau RMC/[CONFIDENTIAL] understands, a sensor has a range of potentially up to 70 meters around the measuring point. The sensor captures the Wi-Fi signals that a

18 See appendix 1, section 1.2, page 46 et seq.

device emissions within the sensor area. The sensor receives a 'packet' of data including the MAC address of the device and WiFi strength. According to the Municipal Executive, no (other) until registered personally identifiable data. Also, no longitude, latitude, or address information is provided received by the sensor.

The status messages sent to the server are accompanied by the hashed MAC address.

This hashing19 takes place immediately upon forwarding. In its research, the AP indicates that there is unpseudonymized (i.e. original) MAC addresses are stored on the working memory of the sensor. According to the Board of B&W Enschede, that is correct, but that is only very temporary (a few milliseconds); after all, without that temporary storage in the working memory of the sensor there would be no hashing can take place. However, according to the Board of B&W Enschede, this is not possible identification take place. After all, one cannot gain access to the sensor, in such a way that one find out a MAC address. No MAC addresses are kept permanently and there are for example, no lists or databases with MAC addresses are available. Desk RMC/[CONFIDENTIAL] cannot access the MAC addresses on the sensors.

The AP does not follow the view of the Municipal Executive. That the sensors potentially have a range of up to 70 meters does not detract from the fact that in this case the sensors have been “calibrated” and adjusted to the

across the road.20 The sensors therefore do not have a range of 70 meters around the measuring point, but a reach across the street. The AP also notes that for the determination of the location no GPS data is required. After all, the location of the sensor is known to [CONFIDENTIAL] and the sensor ID is sent to the server. This means that this data is in a different database not that [CONFIDENTIAL] has no access to it.

The Board of B&W Enschede also states that access to the MAC addresses is not possible the sensor. In response, the AP would like to emphasize the following. There are two modules on the sensor active. The first [CONFIDENTIAL] is the receive module and keeps track of MAC addresses as they become received. The working memory of this module therefore contains all MAC addresses that are also within the last two minutes have been received by the sensor. The second module [CONFIDENTIAL] receives status-1 and status-2 messages from the first module. The first message means “there is a new phone detected” and the second means “the phone has not been seen for more than two minutes”. The two modules communicate through a so-called [CONFIDENTIAL]21 and unhashed MAC addresses sent. The hashing only takes place in the second module, just before the data be sent to the server. [CONFIDENTIAL]22. [CONFIDENTIAL].23 [CONFIDENTIAL].

19 Hashing is the conversion of a sequence of numbers and/or letters into another unique sequence by means of an algorithm.

20 Statement of statement by Bureau RMC and [CONFIDENTIAL] made on 29 May 2019, page 2 (document number 49).

21 [CONFIDENTIAL]

22 [CONFIDENTIAL]

23 [CONFIDENTIAL]

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

Identification of natural persons

Furthermore, the Municipal Executive of B&W Enschede takes the position that the MAC addresses used by the sensor collects, whether or not in combination with a location data, not directly or indirectly to identify an individual natural person can lead. The Board of B&W Enschede disputes the finding of the AP that a MAC address, for example in combination with a location data, in some situations could identify a natural person, not. However, the board of B&W Enschede wants emphasize that there can only be direct or indirect identifiability if there is is of (link to) additional data.

In its report, the AP assumes too quickly that there is of traceability. According to the Board of B&W Enschede, the publication of WP29 shows expressly that the single MAC address is not considered personal data. Is a MAC address according to WP29, only personal data if it is combined with other data. In this case however, there is no combination of the MAC addresses with other data. The only other data that could possibly play a role in this context is a (rough) location data. This location data is in this case too imprecise to identify an individual in conjunction with a MAC address can identify.

The Municipal Executive of B&W Enschede also takes the position that the criteria have not been met the judgment Breyer / Germany to speak of personal data. The MAC addresses are namely not stored, but hashed directly on the sensor, after which the original MAC address becomes deleted. It is therefore not possible to access the original MAC addresses. Future identification is impossible for that reason alone.

According to the B&W Enschede college, the data sent from the sensor has no direct information location data. The Sensor ID is no more or less than a designation of the sensor, it says not yet exactly where the sensor is located. In addition, the Sensor ID only appears for the first time sending the hashed MAC addresses from the sensor to the server. Due to the separate storage association of the Sensor ID with the MAC address only take place later in the counting process. From that however, the MAC address is no longer available at the moment. The MAC address is used when sending it

hashed to the server, and then truncated. Identification, also by means of a

so-called location data, can therefore not take place according to the Municipal Executive of B&W Enschede.

The AP does not follow the view of the Municipal Executive of B&W Enschede. The college B&W Enschede explains

false emphasis on the fact that MAC addresses are transformed and not independent

be kept for some time. However, it ignores the data seen by the AP

as personal data.

The combination (pseudonymous identifier + date time + location) is personal data. Here's that

combination of truncated hashed MAC address, date plus time in seconds and the ID of the sensor. The

any possibility to go from a hashed and truncated MAC addresses back to the original

MAC address is therefore irrelevant. The point here is that the pseudonymous identifier changes over time

little has changed.

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

The ability to trace back (and ultimately identify) is a result of design decisions in the

platform. Storing the unchanged identifiers for a long time makes it possible to

track individuals. At that time they are only displayed as a number. But this is

the same number for six months. One cannot speak of robust in this case

anonymization techniques. In any case, this was not the case during the AP's investigation.

Because the same identifier comes along time and time again, tracking people is therefore possible. With that

time and location becomes a factor. And as mentioned above by the AP, the exact location is included

of the sensors known to [CONFIDENTIAL] where the range of the sensors is set up to the

across the street and not 70 meters. Movement patterns are highly individual. The lecture

B&W Enschede underestimated the sensitive nature of location data that was always kept for half a year.

Living patterns

The AP concludes that living patterns can also be distilled from the hashed and truncated data
which in themselves can be traced back to an individual. However, the municipality of Enschede believes that
traceability to an individual on the basis of a lifestyle is not possible in this case.
In the eyes of the Municipal Executive of B&W Enschede, it can be assumed that a certain pattern develops
also in the future, occurrence will never be the basis of a real, indirect, identification. Profiling is
after all, this is only possible if several counts of a pseudonym are collected. To the
municipality understood, in this case most counts are made on the basis of one-off counts. like that
applies to approximately 70% of the censuses.
In addition, there may be theoretical overlap in the living patterns that the AP believes it can abstract
occur across multiple devices, due to the truncating of the hashed values. It's not over
rule out in advance that two or more hashed, and then truncated, data has the same value
to get. Furthermore, not only individuals carry devices with a MAC address, but themselves
various other devices such as pin devices, smart TVs and printers can also be located in the area.
This only possible method of identification outlined by the AP is identification by an employee of
Bureau RMC/ [CONFIDENTIAL] on site or via remote camera images. This one
According to the Municipal Executive of B&W Enschede, the possibility of identification is unworkable or, in fact, impossible.
The
Inappropriateness of a request, namely asking a person what MAC address he/she has, is no more
than a theoretical one. In addition, Office RMC/[CONFIDENTIAL] does not have a MAC address at all
at its disposal to verify that MAC address. After all, the MAC address is determined according to the
college B&W Enschede immediately hashed and later anonymized. In addition, the MAC address is not
recorded in a list or, for example, a database, so that subsequent identification and checks do not take place
can find.
Real-time identification, really necessary to identify a natural person and also
the only example of identification that the AP gives in its research report is possible, according to the Board

the search area is too large. The AP must also take into account that there is a lot of pressure

hundreds, if not thousands, of people can be in the sensor area at times.

Incidentally, contrary to what the AP believes, the municipality of Enschede has no possibility at all to acquire knowledge

of any data that can be traced back to individuals at Bureau RMC/[CONFIDENTIAL]. The

According to the Municipal Executive of B&W Enschede, a single contractual option is insufficient to assume that

the municipality actually had and has access to the said data.

The AP largely does not follow the view of the municipal executive of B&W Enschede. As mentioned above

the AP considers the anonymization techniques used to be insufficient, so that it was possible to

to be able to track individuals when storing the unchanged identifiers for a long time. The

AP does agree with the fact that in 70% of the cases the counts are made on a one-off basis

counts. However, that does not detract from the fact that the Municipal Executive of Enschede of tens of thousands of citizens

does

processed multiple counts and that the one-time visitors could be identified on the basis of the

data on the sensors. And although there are of course also some devices such as printers in the city,

it seems to the AP inconceivable that these are visible in multiple locations as they extend throughout the city

to move. The resident filter makes an attempt to filter out these types of devices.

The AP continues to maintain its position that identification of natural persons is possible in three

ways described in section 3.1.3. The AP has taken into account all means of which

it is reasonable to expect that they will be used by the controller or by

another person to directly or indirectly identify the natural person, for example

selection techniques.24 The combination (pseudonym identifier + date time + location) makes it possible to identify someone. It is not for nothing that Article 4, part 1, of the GDPR considers location data as an identifier.25 After someone has been identified, they can be checked ask for its MAC address. The AP has cited this control question as an example. However, there are many ways to verify the identity of persons.

If Bureau RMC/[CONFIDENTIAL] had properly implemented all the technical measures referred to then there was no tracking. The step to actually identify therefore requires less others not a disproportionate amount of effort according to the AP. And in some cases – the nocturnal ones hiker for example – identification requires only a very limited effort. From the collected data trace his living patterns, so that you can find out someone's place of residence or place of work. The AP refers continue to page 12 of this decision for an explanation of why real-time identification is indeed possible used to be.

Finally, it is not required that all information from which the data subject can be identified must be rests with one and the same person.26 It is important here that the Municipal Executive B&W Enschede lawfully has access to all means that can be used to directly or indirectly harm a natural person

24 Recital 26 GDPR.

25 For a further in-depth look also see https://www.nature.com/articles/srep01376

26 CJEU, 19 October 2016, ECLI:EU:C:2016:779, r.o. 43.

identify. That the Municipal Executive of B&W Enschede has contractually agreed to be able to provide data upon request from Bureau RMC and [CONFIDENTIAL], the Commission pre-eminently gives lawful access to the personal data. It is legal that the Municipal Executive of B&W Enschede does not (want to) use it

irrelevant.

3.2 Controller

3.2.1 Introduction

In the context of the question whether the Municipal Executive B&W Enschede processes the personal data in line with Article 5,

first paragraph, preamble and under a jo. Article 6(1) of the GDPR is also important to determine who to contact marks is as a controller as referred to in Article 4, part 7, of the GDPR. Thereby

determining who determines the purposes and means of the processing of personal data.

3.2.2 Facts

Given the extensive investigation into this case, the AP refers to the second chapter for the facts

of Annex 1 to this Decision. Below is a brief summary of the facts, after which the AP concludes

judgment is coming.

The Municipal Executive of Enschede has decided to start on 6 September 2017 with 24/7 measurements via

sensors in the city center of Enschede. The contract for this has been awarded to City Traffic B.V., currently

RMC office. In addition, the municipality of Enschede has both a press release and a number on its website

Posted Q&As about the WiFi measurements.

The WiFi measurements were carried out with the aim of measuring the effects of municipal investments in

the city center of Enschede with a view to responsible use of public funds. In addition

points out that the measurements can provide insight into subjects that are important

for the fulfillment of its public task, such as the effects of roadworks, keeping

shopping Sundays and market days, inner city promotion, the attractiveness of events, the acquisition

of shops and catering establishments and determining whether and when intervention is necessary in the context of order and security

safety.

On September 26, 2017, the Executive Board of B&W Enschede and the predecessor of Bureau RMC issued a

processor agreement concluded in the context of the WiFi measurements in the city center of Enschede. In

this agreement stipulates that the Municipal Executive of B&W Enschede is responsible for the processing

processing of personal data. It is also stipulated that the processor, Bureau RMC, processes the data

for the benefit of the Municipal Executive of B&W Enschede. Bureau RMC only processes the data on behalf of

the Municipal Executive of B&W Enschede and will also follow all reasonable instructions in this regard. At all times

At the request of the Municipal Executive of Enschede, all data originating from the municipality of Enschede will be processed

with regard to the processor's agreement has been handed over to the B&W Enschede college. Desk

RMC may only outsource the work to third parties after prior written permission

of the college B&W Enschede. And the parties agree that Bureau RMC will have the data processed

by [CONFIDENTIAL], with whom Bureau RMC has concluded a level service agreement.

16/58

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

The Municipal Executive of Enschede B&W has had a steering role in the number and locations of the sensors that

used for the Wi-Fi measurements. In addition, in response to the

publication of the AP on November 30, 2018 about WiFi tracking to Bureau RMC

temporarily pause wifi measurements in the city center of Enschede. As of 1 January 2019, Bureau RMC op

at the request of the B&W Enschede Board, the so-called “anonymisation on the server” has been introduced, whereby

the last three characters of the pseudonymised MAC addresses are truncated. B&W College

Finally, on April 30, 2020, Enschede instructed Bureau RMC to complete the

turn off sensors.

3.2.3 Assessment

Article 4, preamble and part 7, of the GDPR defines a controller as a

natural or legal person, public authority, agency or other body that, alone

or jointly with others, determines the purposes and means of the processing of personal data. In

this case is that the processing of the MAC address of the mobile device, the time (in seconds) and the date of the detection by the sensor and the sensor ID. It is not required that the controller has the personal data in his possession.27

The AP is of the opinion that the Municipal Executive of B&W Enschede is responsible for the processing of personal data by means of the Wi-Fi counts in the city center of Enschede, because they are the who has determined both the purpose and partly the means of the processing. She justifies this as follows.

The person who determines the purpose of the processing of the personal data is the one who determines why the processing takes place. As discussed in section 3.2.2, the Municipal Executive of B&W Enschede was the one who decided to carry out Wi-Fi measurements. In addition, the data is processed for a by the Municipal Executive of Enschede determined the purpose, namely measuring the effects of municipal investments in the city center of Enschede. The other purposes that the college B&W Enschede in cites her point of view for the Wi-Fi measurements (e.g. measuring the effects of road works, inner city promotion and shopping Sunday) are also determined by the council and are moreover based on the Municipalities Act.28 Furthermore, on 30 November 2018, the Municipal Executive of Enschede Have Bureau RMC temporarily pause the processing and have the sensors switched off on May 1, 2020. It college B&W Enschede was also the one who determined with her college decision that there personal data are being processed, and the person who can therefore decide to stop doing so. With that the Municipal Executive of B&W Enschede has control over whether or not the personal data is processed. The AP concludes that the Municipal Executive B&W Enschede defines the purposes for the processing of personal data has decided.

27 CJEU, 5 June 2018, ECLI:EU:C:2018:388 (Wirtschaftsakademie) and CJEU, 29 July 2019, ECLI:EU:C:2019:269 (Fashion ID).

28 In its opinion, the Municipal Executive of B&W Enschede argues that the measurements also provide insight into the effects of roadworks, holding shopping Sundays and market days, inner city promotion, the attractiveness of events, the acquisition of shops and catering establishments and determining whether and when intervention is necessary in the context of order and

The person who decides how the processing takes place should be regarded as the one who uses the means determines. As discussed in section 3.2.2, the Municipal Executive of Enschede has decided for the to use a service provider, namely Bureau RMC, for the processing of personal data. The technical elaboration of the processing of personal data is delegated to Bureau RMC, whereby the Municipal Executive of B&W Enschede did have the option, on the basis of the processing agreement, to to give instructions. The Municipal Executive of Enschede B&W has also influenced the resources for the processing by co-determining how many sensors would be placed and where they would be placed would become. The AP concludes that the Board of B&W Enschede will determine by whom the processing would be carried out and also the way in which the processing takes place, for example by the number sensors and their locations, has partly determined how the processing of personal data took place.

Based on the above, the AP concludes that the B&W Enschede Board has achieved both the goal and the partial has determined the means for the processing and therefore qualifies as controller within the meaning of Article 4, opening words and part 7, of the GDPR for the processing of personal data via sensors in the city center of Enschede.

3.2.4 Opinion of the Board of B&W Enschede and response by AP

In its view, the Municipal Executive argues that it is not a controller within the meaning of the AVG is. In doing so, she distinguishes between her responsibility as a client, which she is not disputed, and the concept of controller as defined in the GDPR. Although the college B&W Enschede designates itself as controller in the processing agreement

according to her factual circumstances which indicate that she has none or only jointly

is the controller. For example, the operation of the WiFi counting technique, the way in which the

data is collected, which data exactly is collected for the desired output, the

choice for hashing and truncating, the storage and the (whether or not in consultation) retention period determined by

Office RMC. The Municipal Executive of B&W Enschede also has no access to the data and no control

about the fact that Bureau RMC provides or even sells data to third parties. The college also conducts B&W

Enschede that it does not prescribe the frameworks and/or conditions within which the data will be processed

incorporated. Furthermore, Bureau RMC states in Article 1.1 of its Privacy Protocol CityTraffic that it itself

is the controller.

The AP has taken note of the argument of the B&W Enschede Board, but does not follow it.

Below it will first be explained why the AP is of the opinion that the B&W Enschede Board should have the

is the controller. Subsequently, the AP will discuss why this is not the case

joint controller.

Processing responsibility

The factual circumstances to which the Commission refers all relate to the resources for the

processing. After all, what matters is how the processing takes place. Although Bureau RMC influence

has on the method of processing, College B&W Enschede is the one who has chosen to make use of the

use services offered by Bureau RMC, the person who has determined how many sensors there are

would be placed and where they would be placed. The municipality has (also) determined this

what means are used for the processing.

The fact that the municipality would not have access to the data processed by Bureau RMC means, according to the

AP does not mean that it cannot be a controller within the meaning of the GDPR. The Court of Justice of the European Union (CJEU) has determined that it does not require all information based on which the data subject can be identified, is associated with one and the same person.29

The Municipal Executive of B&W Enschede further points out that Bureau RMC can determine the data to be passed on to a third party lot to sell. The AP distinguishes between different processing operations. First of all there is the processing of personal data by Bureau RMC for the purpose of the Municipal Executive Enschede, namely measuring the effects of municipal investment in the city centre. This is the processing that is the subject of the investigation and for which the AP charges the Board as controller qualifies. This responsibility is limited to the processing for which the College B&W Enschede determines the goal and partly the means. In addition, there is the possible processing in which Bureau RMC can give other parties access to the information that it also uses for the delivery of the information to the College of B&W Enschede. Bureau RMC may have these because in the Processing agreement stipulates that Bureau RMC is entitled to an assessment file (removed from personal data), a copy of the data that can be used for anyone who makes an application about, for example, crowds at a certain place in the city center of Enschede. In that second situation there is there is a processing that falls outside the purposes of the Municipal Executive B&W Enschede, and therefore also beyond its responsibility as controller. That the college B&W Enschede for this other, second processing is not a controller does not affect the conclusion that the Municipal Executive of B&W Enschede is still the one who determines the purpose and partly the resources and therefore qualifies as a controller.

The Municipal Executive of B&W Enschede further argues that it does not prescribe the frameworks and/or conditions within which the data is processed. The AP does not follow this argument. In the processing agreement certain Bureau RMC will follow all reasonable instructions of the B&W Enschede Board. Desk RMC has already done this by suspending processing twice at the request of the Municipal Executive. The AP concludes from this that the Commission, if desired, will define the frameworks and/or conditions within which the

data can be processed. That the municipality has not always used this

possibility, or not intending to do so, does not detract from its existence.

Finally, the Commission argues that CityTraffic's Privacy Protocol stipulates that Bureau RMC

is the controller. The AP does not follow this argument either. First of all, paragraph 1.1 of the

Privacy Protocol that CityTraffic is responsible, insofar as they (alone or jointly with others)

determines the purposes and means of processing MAC addresses. That means according to the AP

not that Bureau RMC is in any case the controller. Furthermore, Bureau RMC and the

college B&W Enschede stipulates in the processing agreement concluded between them that precisely the college

B&W Enschede is the controller. Now the processing agreement between the parties

29 CJEU, 19 October 2016, ECLI:EU:C:2016:779, r.o. 43.

agreement is, in contrast to the privacy protocol of Bureau RMC, must be connected

searched for in this processor agreement. In addition, the B&W Enschede college is the one that

actually determines the purposes and partly the means of the processing. In such a situation, where

the actual situation deviates from a “paper” reality, such as the privacy protocol, is the actual one

leading situation.

Joint Controllership

The Board of B&W argues that if the AP is of the opinion that the Board

is responsible for the processing, that there is then only joint

controller. The AP does not follow this argument and motivates it as follows.

Article 26 of the GDPR stipulates that when two or more controllers jointly manage the

determine the purposes and means of the processing, they are joint controllers.

Article 4, preamble and part 7 of the GDPR also stipulates that the controller
is the one who, alone or jointly with others, determines the purposes and means of the processing. In both
Articles stipulates that the (joint) controller determines the purpose and means for the
processing determines. It appears from the factual circumstances cited by the B&W Enschede Board
that Bureau RMC has a degree of influence over the means of processing. However, it has not turned out
that Bureau RMC determines the purposes for the processing of personal data for the Municipal Executive
Enschede. Since Bureau RMC does not determine the purposes for the processing, it cannot do so
being a controller. As a result, there can be no question of joint
controller. That Bureau RMC partly influences the determination of resources
this does not change for the processing, because the (joint) controller has purpose and
means of processing.

3.3 Lawfulness of the Processing

3.3.1 Introduction

In section 3.2, the AP noted that the Municipal Executive B&W Enschede de
is the controller for the processing in the context of the WiFi measurements. The AP will be in it
assess whether the Municipal Executive of B&W Enschede can successfully appeal for this processing
on one of the bases from Article 6 of the GDPR.

3.3.2 Assessment and response to opinion

Article 5, first paragraph, preamble and under a, of the AVG stipulates, among other things, that personal data must be
processed in a manner that is lawful in relation to the data subject. It is traded in
accordance with this principle of legality, if there is a sound legal basis for the
processing is available.

Article 6, first paragraph, of the GDPR then provides an exhaustive summary of the basis for a
lawful data processing. This article states that processing is lawful only if and for
insofar as at least one of the six principles referred to has been met. The for the college B&W Enschede

any eligible bases are:30 c) necessary to comply with a legal

obligation; e) necessary for the performance of a task in the public interest or of a task in the

framework of the exercise of public authority; f) legitimate interest.

3.3.2.1 Statutory duty or duty of public interest

Article 6, third paragraph, of the GDPR stipulates that the processing of personal data that takes place on the

legal bases c) and e) must be established by Union or Member State law applicable to the

controller applies. The purpose of the processing must be set out in Union law or

Member State law, or is in terms of legal basis e) necessary for the fulfillment of

a task in the public interest or for the exercise of official authority vested in the

controller has been granted.

Recital 45 of the GDPR reads: “This regulation does not prescribe that for each individual processing

specific legislation is required. Legislation that serves as a basis for several will suffice

processing based on a legal obligation to which the controller is subject, or for processing that

is necessary for the performance of a task of general interest or for a task in the context of the performance

of public authority. (…)”

Recital 41 of the GDPR does state that the legislation on the basis of which the processing takes place

must be sufficiently clear, precise and predictable: “This legal basis or legislative measure must

however, be clear and precise and its application predictable to those to whom it applies

applies, as required by the case law of the Court of Justice of the European Union (“Court of Justice”) and the

European Court of Human Rights.”

Bases c) and e) both require that the processing is necessary. This

necessity requirement means that the principles of proportionality and

subsidiarity. The principle of proportionality means that the infringement of the interests of the
processing of the personal data of persons concerned must not be disproportionate in relation to it
purpose to be served with the processing. Under the subsidiarity principle, the purpose for which the
personal data are provided in reasonableness not in any other way, for the processing of
personal data of the person concerned, can be achieved in a less disadvantageous way.
In its view, the Municipal Executive of B&W Enschede states that the processing in the context of Wi-Fi counts
can be based on Article 6(1)(e) of the GDPR. According to the Board, the AP misunderstands that the
The municipality of Enschede has a very broad task. It follows from the Municipalities Act that the municipality 'daily
administration of the municipality. According to the Commission, this task is not simply formulated broadly,
but precisely for a well-thought-out reason. In the eyes of the municipality, its responsibilities, and
in line with this, the need to carry out the wifi counts in order to meet those different
responsibilities, from various (formal and material) laws and regulations and documents.
30 In the present situation, no permission has been requested from the parties involved (ground a), the Wi-Fi measurements
are not necessary
performance of a contract with the data subject (ground b) and they are also not necessary to protect certain vital interests
protect (ground d).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

The Municipal Executive of Enschede refers to article 160 paragraph 1 sub a and h, article 212 paragraph 1, article 213
paragraph 1, article 172 paragraph 1 of the Municipalities Act. And to the retail agenda of the national government, Visie
bustling city center and the mobility vision, the APV of Enschede, the testing framework
event permits, the further rules for terraces, the municipal budget and the
subsidy regulation.

According to the Municipal Executive of Enschede, passerby counts can provide insight into various aspects that are important for municipalities to be able to base their policy on various areas and therefore to give substance to the 'public task' that it has as a municipality towards its inhabitants. This According to the Commission, information is only really valuable if it is 'continuous' information, ie not only information based on incidental events. In the eyes of the community, the chosen method of counting is actually more privacy-friendly than, for example, manual counts. Manual counting has many disadvantages: double counting cannot be prevented, and thus give manual counts are not a reliable picture. Moreover, this is very labour-intensive and therefore expensive. In the latter In this case, the counter sees by definition which person is where. Other alternatives to counts than via WiFi are actually not available. There are infrared counts, but also this one method does not remove double counting from the counts.

The AP has asked the Municipal Executive of Enschede whether it is necessary for municipal tasks to know visitor flows or the number of visitors per (measurement) point. The college B&W Enschede has stated the following. At the start of the passerby counts, the B&W Enschede college was alive still assuming – based on information that the Commission obtained from the Bureau at that time RMC – that Bureau RMC would provide anonymous information about visitor flows. The term "visitor flows" was also mentioned in the Executive Board decision to switch to visitor counts over Wi-Fi. According to the Board of B&W Enschede, this explains why in the opinion of the Board there are sometimes visitor flows are discussed. After the start of the visitor counts and the first results of the census data (around the beginning of 2018), however, showed that the Board could not see any flows, but it did print per sensor tip. The Municipal Executive of Enschede has therefore stated only the number of passers-by at a certain time point and moment.31

The AP does not follow the view of the Municipal Executive of B&W Enschede and arrives at the following assessment.

The AP first of all notes that there is no legal obligation on the Municipal Executive of B&W Enschede, laid down in Union law or national law, to have the Wi-Fi measurements carried out in the city centre. Also the processing of personal data is not based on a more broadly formulated duty of care or legal

obligation. The AP therefore firstly concludes that the B&W Enschede Board cannot successfully appeal
do so on the basis of Article 6(1)(c) of the GDPR.
The AP then investigates whether the Wi-Fi measurements could be processing operations that are necessary for
a task of public interest. The AP has already concluded that the Wi-Fi measurements are processing in
within the framework of municipal government tasks. Government tasks are tasks of public interest. That's how it is
board B&W Enschede is authorized, pursuant to Article 160 of the Municipal Act, to 'manage the day-to-day management of
the
31 Letter of 16 February 2021 from the Municipal Executive of B&W Enschede to the AP, page 2.

municipality". This concerns a task of general interest, such as keeping things in order
the finances of the municipality, spatial planning and urban development
scissored.
The AP notes that recital 45 of the GDPR does not state this for every individual processing
specific legislation is required. In the present case, this means that the various processing operations are those
can be determined based on one legal provision. Recital 41 of the GDPR required
however, a certain degree of concreteness of the legislation. This recital states that the
legislation, in this case the task of public interest, must be clear, precise and predictable.32
This foreseeability requirement means, among other things, that the (legal) consequences of certain actions
must be foreseeable to a certain extent by the public.
From the requirement that an interference with the exercise of the right to respect for private life as referred to in
Article 8 of the ECHR must be provided for by law ("in accordance with the law"), it follows that that
interference must be based on a duly published legal regulation from which the citizen

can determine with sufficient precision which data relating to his private life with an eye
can be collected and recorded for the fulfillment of a certain government task, and under what conditions
conditions that data can be processed, stored and used for that purpose. So one is required
sufficiently precise legal basis. This means that, for example, the general task of a
government service cannot in all cases serve as a legal basis for data processing.33 It means
also that an obligation for a government agency to provide data while that
government agency has a statutory duty of confidentiality, expressly and clearly in a
statutory regulation must be laid down, and that it is not permissible for such an obligation
is exclusively deduced from the development history of or the coherence between legal
provisions or is assumed because of the effectiveness of a legal regulation.34

The AP is of the opinion that the statutory task of 'carrying out the day-to-day management of the municipality' is not
appropriate
meets the above requirements, because this task is formulated too broadly, is not concrete and therefore not
is sufficiently predictable.35 A citizen cannot sufficiently deduce from Article 160 of the Municipal Act which on
data relating to his private life with a view to the fulfillment of this government task
can be collected and recorded, and under what conditions that data can be used for that purpose
edited, stored and used. The AP is aware of the fact that the legislator has enforced Article 160
Municipal Act has deliberately formulated it broadly. Only this has the effect of making it spacious
formulated job description (for the sake of the effectiveness of a legal regulation) not without
can serve as a legal basis for this data processing.

32 See also ECLI:NL:RBROT:2020:2257 in this context.

33 See also HR 24 February 2017, ECLI:NL:HR:2017:288 (Belastingdienst ANPR case)

34 ABRvS 3 February 2016, ECLI:NL:RVS:2016:253

35 The legislator has explicitly opted for the broadly formulated concept of ‘day-to-day management’ and not for more detailed
tasks
because "such an enumeration is almost by definition doomed to be inconclusive." Parliamentary Papers II 2000/01, 27 751,

The Board of B&W Enschede also refers in its opinion to various articles in the
Municipal Act, the APV and several documents. The AP notes that only Article 160 of the Municipalities Act de
competence of the Municipal Executive of B&W Enschede. The other articles pertain to powers of others
organs of the municipality. The Municipal Executive has been designated by the AP as
controller, which means that the other articles of the law do not apply for that reason
may be as Member State law in which the task of public interest is assigned to the controller
assigned is arranged.

The AP also went through the entire APV of Enschede, but the AP did not find any articles here
against which a citizen can deduce that the personal data referred to in paragraph 3.1 can be used
are processed for government tasks and under what conditions that data can be used for that purpose
edited, stored and used. The other documents cited by the Municipal Executive
Finally, Enschede cannot be a basis for the processing of personal data because this
are not legal requirements.

The AP therefore concludes that the Municipal Executive of B&W Enschede cannot successfully invoke the
basis in Article 6, first paragraph under e, of the GDPR. With this, the AP does not mean that a municipality
can never have a legal basis for counting visitors. The legal regulation serves
however, formulated more concretely for this situation and thus be sufficiently predictable.

Needless to say, the AP also maintains its position that the requirements have not been met in the present situation
requirement of necessity because the principles of proportionality and subsidiarity are not met.

The invasion of the privacy of hundreds of thousands of citizens whose MAC addresses and location data through the

sensors have been collected and processed disproportionately in relation to the processing to serve goal, namely testing the effectiveness of investments in the city center of Enschede. In this assessment, the AP takes into account that the right to protection of privacy of citizens in public space weighs heavily, given the reasonable expectation of the public to act as passers-by cannot be followed unnoticed and the fact that data is systematically and for were recorded for a longer period of time. Especially for residents and frequent visitors to the municipality Enschede, the current processing of personal data is an extra major breach of protection of personal life. That the Municipal Executive of B&W Enschede did not aim to collect personal data processing does not detract from the fact that personal data is the responsibility of the college were processed. This undermines the citizens' sense of being unobserved in public delusions and to have faith in the government.

In addition, the subsidiarity principle has also not been met because the objectives pursued by the college B&W Enschede can be served in a different, less far-reaching way. Even on ways in which no personal data is processed. The college B&W Enschede has, whether it was intended or unintentional, have personal data processed under its responsibility with which it was possible to track civilians. However, the Municipal Executive of Enschede B&W has stated that it does not needs visitor flows but only the crowds per sensor point. This resulted in the processing of personal data under the responsibility of the Municipal Executive of B&W Enschede between May 25, 2018 to

and with April 30, 2020 not necessary and also excessive. In addition to the fact that in the used database insufficient technical measures were taken, the personal data also unnecessarily (apart from the raw data) always kept for half a year.

There are sufficient methods to measure the crowds in a certain place where the protection of
personal data is better protected. For example, one can gain insight into crowds by
market surveys. But people also count via an automatic visitor counter that emits an infrared beam
broadcasting is an eminently effective technique. This technique is also affordable and gives the opportunity to
to provide the continuous information that the Municipal Executive of B&W Enschede needs. Double counting is possible
can be filtered out with statistical calculations. Knows almost every method or technique used
measurement errors and requires calibration, often also at the level of individual sensors. This allows the
correct any measurement errors in the counts. In addition, a small measurement error, as far as this after
calibration would still exist, given that one ultimately totals and groups numbers, not
insurmountable.

3.3.2.2. Legitimate interest

The first paragraph of Article 6 of the GDPR stipulates that basis f) legitimate interest does not apply to the
processing by public authorities in the exercise of their duties. Recital (47) of
the GDPR provides the following explanation: “(…) Since it is up to the legislator to determine the legal basis for
personal data processing by public authorities, that legal basis should not apply to the
processing by public authorities in the performance of their tasks.”

Government bodies will not be able to use the basis in the performance of their duties
'legitimate interest', but will have to use other grounds. This does not apply to
insofar as the government agency carries out 'typical business activities' involving personal data
are processed, such as, for example, the processing of personal data that is necessary for the
security of government buildings. For actions that fall outside the performance of the task, there may be
a basis must be assumed in the legitimate interest of the organization. Government
does not differ essentially from a private party in this respect.

Article 6, first paragraph, of the GDPR therefore stipulates that basis f) does not apply to 'processing by
public authorities in the exercise of their duties”. This does not apply insofar as the
government agency performs 'typical commercial activities'. The AP has already established that

the aim of the wifi measurements is to test the effectiveness of municipal investments in the city center of Enschede, with a view to responsible use of public funds. The AP concludes from this that the Wi-Fi measurements are processing in the context of the municipal government tasks. The AP therefore concludes that the Municipal Executive of B&W Enschede cannot invoke the basis of legitimate interest within the meaning of Article 6(1)(f) of the GDPR. It's on the legislator to determine the legal basis for personal data processing in such cases create government agencies.

In its view, however, the Municipal Executive of B&W Enschede is of the opinion that collecting information about visitor numbers and visitor flows in the context of WiFi counts is a legitimate interest for the Municipal Executive of B&W Enschede, the entrepreneurs, investors, visitors and residents. The AP has recognized in the Bluetrace case, according to the B&W Enschede Board, that there may be a legitimate interest in collecting such information.36

The Municipal Executive of B&W Enschede also states that the processing in the context of Wi-Fi counts is correct met the necessity requirement. The wifi counts are necessary for this described interests that are pursued. It is not possible to retrieve this information a less intrusive way. With WiFi counting, according to the B&W Enschede much more sustainable, efficient and reliable results are collected. Here comes according to the B&W Enschede Board, that Bureau RMC has taken all kinds of measures that entail entail compliance with the requirement of proportionality and subsidiarity. As before in described in this view, the Municipal Executive of B& W Enschede has always relied on the expertise of Bureau RMC as a professional contractor. Furthermore, the municipality of Enschede informs everyone who uses the

enters the city center of Enschede, actively through warning signs about the Wi-Fi counts. The
those involved are also informed about this via the website of the municipality of Enschede.
Finally, the Municipal Executive of Enschede states that Bureau RMC has already corresponded around 2016
with the AP about its working method in the context of WiFi counts. In that context, Bureau RMC has adopted the
AP followed directions provided. Bureau RMC was able in that regard – partly because the AP subsequently
has not been heard from again - assume that its working method is in accordance with the
privacy laws and regulations and has also been approved by the AP.
The AP does not follow the view of the Municipal Executive of B&W Enschede and maintains its position that it
college B&W Enschede cannot successfully invoke the basis of legitimate interest. It
After all, college B&W Enschede has itself explained in detail that the processing in the context of
Wi-Fi counts are necessary for municipal government tasks and not for 'typically commercial
actions'. The fact that the Municipal Executive of B&W Enschede has its own legal duties above
referred underlines this assessment all the more. As a result, the AP does not get to one
weighing of interests under Article 6(1)(f) of the GDPR. And as for the Bluetrace case,
in that case it concerns a company and not a government agency that makes the comparison by it
college B&W Enschede does not apply.
Finally, the AP notes that it did indeed conclude the investigation into Bureau RMC with a
formal letter. In this letter, the AP explicitly stated that the AP does not express an opinion on the
data processing to which the investigation related. The statement of the B&W Enschede Board that
Bureau RMC could therefore assume that its working method is in accordance with the privacy legislation.
and regulations and, moreover, has been approved by the AP, so the AP deems it incorrect.
36 CBP, Wifi tracking of mobile devices in and around shops by Bluetrace, z2014-00944, October 13, 2015,
https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapport_db_bluetrace.pdf, p. 40.

Date

March 11, 2021

4. Fine

4.1 Introduction

From 25 May 2018 to 30 April 2020, the Municipal Executive of Enschede acted in violation of article 5, first paragraph, under a, jo. Article 6, first paragraph, of the GDPR by personal data of owners/users of mobile devices on which the WiFi is switched on in the city center of Enschede unlawfully process.

The AP makes use of its authority to inform the Municipal Executive for the established violation to impose a fine on Enschede. The AP applies the Penalty Policy Rules 2019 for this. 37 After this, the AP first briefly explain the fine system, followed by the motivation of the fine (amount) in the present case.

4.2 Penalty Policy Rules of the Dutch Data Protection Authority 2019

Pursuant to Article 58, second paragraph, opening lines and under i and Article 83, fifth paragraph, of the GDPR, read in coherence with Article 14, third paragraph, in conjunction. 18 of the UAVG, the AP is authorized to the B&W Enschede college to impose an administrative fine in the event of a violation of Articles 5 and 6 of the GDPR up to €20,000,000. The fine for this violation of Article 5, first paragraph, under a of the GDPR is made dependent on the underlying provision, being Article 6(1) of the GDPR. This applies a category III fine, with a fine range between €300,000 and €750,000 and a basic fine of € 525,000. […].38

Pursuant to Article 7, without prejudice to Articles 3:4 and 5:46 of the General Administrative Law Act, the AP (Awb) take into account the factors derived from Article 83, second paragraph, of the GDPR and in the Policy rules referred to under a to k.

4.3 Fine amount

4.3.1. Review conditions

The AP takes into account the question whether an administrative fine will be imposed and the amount thereof

various factors. In this assessment, the AP takes into account, among other things, the nature, the size and the number of affected people.

Lawfulness is one of the basic principles of data protection. A processing of personal data is lawful if it takes place on the basis of a legal basis. In the event of interference private life of the citizen as in the present case, is particularly important that a

37 Stct. 2019, 14586, March 14, 2019.

38 Article 2, under 2.2 and 2.3 of the Fining Policy Rules jo. appendix 2 of the Fining Policy Rules 2019.

public authority can base its actions on a sufficiently accessible, accurate and foreseeable legal requirement. With the collection of personal data without a basis, the Municipal Executive of B&W Enschede has violated the principle of legality. This hits the core of the right to respect for private life and the protection of personal data. It detracts from citizens' sense of being unobserved in public delusions and trust in government.

From May 25, 2018 to April 30, 2020, the Municipal Executive of Enschede has without basis processes personal data of hundreds of thousands of citizens. This violation ended structurally and lasted for a long period of time. From the data collected under responsibility of the Board of B&W Enschede has been processed, a detailed picture can be obtained of the behavior of (individual) citizens. For example, the living patterns can or workplace, but also more sensitive data such as visits to medical institutions or locations that can provide data about someone's sex life.39 The mere fact that this is possible can lead to citizens no longer feeling unobserved by the government. In view of this, according to the

AP talks about a serious situation.

In addition to the fact that the B&W Enschede Board is not based on a foreseeable legal regulation processed personal data, the AP also deems it amiss that the Municipal Executive of B&W Enschede de has processed personal data excessively and for longer than was necessary for the intended purpose purposes. If a controller processes location data or has it processed, then the greatest possible care must be taken to prevent these data from being (indirectly) become identifiable.

In view of the above circumstances, the AP sees reason to submit a to impose a fine and the basic amount of the fine pursuant to Article 7, preamble and under a, of the Fining policy rules 2019 to be increased by € 75,000 to € 600,000.

View of the Board of B&W Enschede and response AP

In its view, the Municipal Executive of B&W Enschede states that there has never been any special and criminal personal data has been processed. Given the very limited nature and seriousness of the alleged infringement of the AVG, the Municipal Executive of B&W Enschede therefore believes that there is a fine-reducing circumstance. In addition, according to the college, the parties involved did not suffer any damage. Next is the municipality Enschede has never been reprimanded by the AP for a violation of privacy law- and regulations and the municipality of Enschede has always fully cooperated with the investigation by the AP. The Municipal Executive of B&W Enschede therefore considers these circumstances to be mitigating factors.

The AP does not follow the view of the Municipal Executive of B&W Enschede and motivates this as follows. As mentioned above, sensitive data can be derived from the collected data. A government agency that processes personal data without having a legal basis for doing so

39 See also WP202 Opinion 02/2013 on apps on smart devices.

Date

March 11, 2021

certainly harmful to civilians. In addition, the Municipal Executive of Enschede has not substantiated why those involved have suffered no harm. Despite the AP not having the same breach before determined by the Municipal Executive of B&W Enschede and according to the Municipal Executive of B&W Enschede, there is no such thing damage, the AP sees due to the seriousness of the violation and the culpability of the B&W Enschede college no reason to refrain from imposing an administrative fine or to reduce the amount of the fine to lower. Finally, the AP is of the opinion that the cooperation of the Municipal Executive of B&W Enschede has not progressed gone beyond its legal obligation to comply with Article 31 of the GDPR. The college B&W Enschede did not cooperate with the AP in a special way.

4.3.2 Culpability and negligent nature of the breach

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.

Pursuant to Article 6, paragraph 1, of the GDPR, processing of personal data is only lawful if it takes place on the basis of a basis. This is a continuation of what already applied under the Directive 95/46/EC and the Personal Data Protection Act. The starting point is that the College B&W Enschede has its own responsibility to comply with the GDPR since the entry into force to comply with the rules laid down therein. That the processing of data in the context of WiFi counts took place at Bureau RMC and [CONFIDENTIAL] does not detract from this. The college B&W Enschede has the legal duty to assume responsibility for determining the processing purposes responsible for the data processing regarding the Wi-Fi counts. The college B&W Enschede failed to conduct careful research into the collected data or to obtain legal advice about it. Also the fact that Bureau RMC had stated in the quotation that they convert and validate data to flows of visitors and footfall of the shopping public, the Board of B&W Enschede had alert must ensure that visitor flows from the collected data could also be displayed. In

instead, the B&W Enschede Board assumed that a third party, with a commercial interest,

took responsibility. The AP considers this culpable.

The Municipal Executive of B&W Enschede has argued that they have always focused on guaranteeing

privacy with regard to the Wi-Fi counts performed by Bureau RMC. That is according to the college

marks as a mitigating circumstance, since they are not intentionally or knowingly on an unlawful basis

how personal data is processed. Furthermore, the Municipal Executive of B&W Enschede believes that they have not been

negligent,

given that the measures taken were intended to process purely anonymous data that is not

traceable to individuals.

The AP sees, partly with reference to section 3.1.3, no reason to refrain from the

imposing an administrative fine or reducing the amount of the fine. The AP believes that

the aforementioned circumstances are not exculpated by the Municipal Executive of B&W Enschede. Of a

government agency, partly in view of the large volume of data processing, may be expected that

it is thoroughly aware of the standards that apply to it and complies with them. Especially in a society

making it increasingly difficult to anonymize data. The college B&W Enschede had more research

to the data processed under its responsibility. Or Bureau RMC de

whether or not agreements with the Municipal Executive of B&W Enschede have been fulfilled is a civil matter between the

Bureau

RMC and the college. The AP also notes that the violated provision of Article 6, first paragraph, of the AVG

no intent required as an ingredient. Since this is a violation, for the imposition of a

administrative penalty, in accordance with established case law, does not require proof of intent.40

The AP may assume culpability if the perpetrator has been established.41

4.3.3 Proportionality and financial circumstances

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. Application of the proportionality principle is possible

among other things play a role in the capacity of the controller.

The Municipal Executive of Enschede has asked the AP to take the financial circumstances into account

of the municipality, without expressly stating that there is a limited financial

carrying capacity. According to the Municipal Executive of Enschede, it is generally known that almost all municipalities in

The Netherlands, due to Corona, among other things, finances are under pressure.42

From what the AP understands, the B&W Enschede Board does not want to expressly state that there is a

limited financial capacity, but that the AP must take into account the financial

conditions of the municipality. Regardless of this conflicting signal, the AP has the public financial

consulted figures from the municipality of Enschede. The AP states on the basis of the (by the municipality of Enschede

self-published) figures, that the municipality of Enschede had general reserves of almost 60 at the end of 2020

million euros and receivables of 40 million euros.43 Given these general reserves and liquidity, the

AP it is unlikely that the present fine will cause continuity problems at the municipality of Enschede

yield.

In conclusion, the AP sees no reason to refrain from imposing an administrative fine or to

reduce the fine amount. The AP considers the fine amount of € 600,000 to be proportionate and there are no others

facts and circumstances that necessitate moderation of the aforementioned amount.

4.4 Conclusion

The AP sets the total fine amount at € 600,000.

40 cf. Trade and Industry Appeals Tribunal 29 October 2014, ECLI:NL:CBB:2014:395, par. 3.5.4, Sept. 2, 2015,

ECLI:NL:CBB:2015:312, par. 3.7 and 7 March 2016, ECLI:NL:CBB:2016:54, par. 8.3; Administrative Jurisdiction Division of the

Council of State 29

August 2018, ECLI:NL:RVS:2018:2879, para. 3.2 and 5 December 2018, ECLI:NL:RVS:2018:3969, par. 5.1.

41 Parliamentary Papers II 2003/04, 29 702, no. 3, p. 134.

42 Letter of 16 February 2021 from the Municipal Executive of B&W Enschede to the AP, page 3.

43 Municipal budget 2021-2024, section 5.3. See: https://documenten.enschede.nl/gb2021.

Our reference

[CONFIDENTIAL]

Date

March 11, 2021

5. Operative part

The AP explains to the mayor and aldermen of the municipality of Enschede, due to

violation of article 5, first paragraph, under a, jo. Article 6, first paragraph, of the AVG, an administrative fine

amounting to € 600,000 (in words six hundred thousand euros).44

Yours faithfully,

Authority for Personal Data,

e.g.

drs. C.E. Mur

Board member

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.

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

Date

March 11, 2021

Attachment 1

Our reference

[CONFIDENTIAL]

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

1. Facts about the concept of personal data

1.1 The sensors installed in the city center of Enschede

If Wi-Fi is turned on on a mobile device, the device sends at regular intervals

intermittently signals that it is looking for a network to connect to. The sensors that are

hung in the city center of Enschede, these signals are picked up. An employee of

[CONFIDENTIAL] has stated that consumer routers are used as sensors in Enschede

used.45

The Municipal Executive of B&W Enschede has stated that the Wi-Fi measurements are carried out using elf

sensors. These eleven sensors were installed on May 25, 2018 and this number has not changed since then.46 Bureau RMC has confirmed this.47 Finally, it also follows from the data collected with the sensors that the AP received in the context of the investigation48 and from the information on the website www.binnenstadsmonitorenschede.nl where use is made of the data collected with the sensors

facts.

It follows from the information provided by Bureau RMC that the sensors have been installed at eleven different locations shopkeepers located in the city center of Enschede.49 AP supervisors have 29 visited a number of these retailers in May 2019 and have the boxes below containing the routers found.50

Figure 1: Two sensors found at two different retailers

45 Page 2 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

46 Responses to the 'Questions about the sensors', letter of 24 May 2019 from the Municipal Executive of B&W Enschede to the AP (file document 26).

47 Page 1 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

48 Citytraffic_number_telpunt 4 Excel sheets and Citytraffic_week overview 4 Excel sheets, appendices 14 and 15 to a letter dated 24 May 2019 from college B&W Enschede at the AP (file document 26). Export Enschede Sep-Dec long term table.zip, received from [CONFIDENTIAL] op 12 December 2019 (file document 69) and Export Enschede Jun - Aug 2019 long term table.zip, received from [CONFIDENTIAL] on 16 December 2019 (file document 72).

49 Excel list location sensors, appendix to e-mail of 23 May 2019 from Bureau RMC to the AP (file item 25).

50 Statements of Official Acts on-site investigation at eight shopkeepers in the city center of Enschede according to Bureau RMC

hang a sensor like this (file documents 30-38).

The director of Bureau RMC has stated that the range of each sensor is basically across the street is.51 On the website www.citytraffic.nl Bureau RMC states that this range is 20 to 30 meters is.52

Based on the foregoing, the AP concludes that eleven sensors have been installed since at least May 25, 2018 at various retailers in the city center of Enschede. Each sensor has a range of 20 to 30 meters.

1.2 The processing of data using the City Traffic method

Bureau RMC calls the method data from mobile devices on which Wi-Fi is located via sensors enabled to collect and process into reports the 'City Traffic method'. This City Traffic method is applied in the city center of Enschede. The website of Bureau RMC contains a infographic that visualizes this method (as of January 1, 2019).53 In this section, the AP discusses the different phases of data collection and processing through the City Traffic method.

Figure 2: Infographic City Traffic method after January 1, 2019

51 Page 2 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

52 www.citytraffic.nl/hoe-we-tellen.

53 Screenshots of web pages on www.rmc.nl recorded on 26 April 2019 (file document 10).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

The collection of data by the sensors and transmission to the server

The first phase involves the capture by the sensors of certain data from mobile devices

on which the Wi-Fi is enabled. Each sensor has a certain range and in this section

demonstrated that data from the

mobile device are collected and then partially pseudonymized and sent to the

central server.

During the on-site investigation on May 29, 2019, an employee of [CONFIDENTIAL] stated

that the same software runs on every sensor in the city center of Enschede and that therefore every sensor

has the same effect.54 The employee further stated that the sensors do not work

changed since May 25, 2018.55

When asked by the AP which data from mobile devices is collected by the sensors,

an employee of [CONFIDENTIAL] replied as follows: “The MAC address, the location ID of

the sensor, the date and time of reception of the Wi-Fi signal on the sensor and the signal strength. Also on the

sensor keeps track of when you are first seen by the sensor and when you were last seen.” 56

The aforementioned MAC address of a device is a factory-built globally unique

number.57 It is a sequence of 12 hexadecimal characters (0-9, A-F) in the form 00:0C:6E:D2:11:E6. As

previously indicated, a device with Wi-Fi on sends the signal at regular intervals

that it is looking for a network to connect to. Via this signal, the MAC address of the

device captured by a sensor.

Later in the statement, an employee of [CONFIDENTIAL] indicated that on the sensors

it is also determined whether a captured MAC address is a so-called 'spoofed MAC address': “It concerns

broadcasting a fake MAC address, to prevent tracking of phones (e.g. by Apple). Spoofed

we do not include addresses in our counts (…).”58

The software code provided by [CONFIDENTIAL] to the AP that runs on the sensors shows that the

following the sensor occurs as soon as a WiFi-enabled device is within range of the sensor

comes:59

1. The device's MAC address and signal strength are captured.

2. The date and exact time of receipt are determined.

54 Page 2 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

55 Page 2 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

56 Page 1 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

57 Page 6 of WP185 Opinion 13/2011 on geolocation services on smart mobile devices.

58 Page 10 of the report of the statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49

and 55).

59 [CONFIDENTIAL] and Declaration of Official Acts analysis source code of 18 February 2020 (file document 78).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

3. The MAC address, signal strength, date and time are stored in the working memory of the

sensor (as long as the device is within range of the sensor).60

4. It is determined whether the MAC address is a spoofed MAC address or not.61

5. The MAC address is pseudonymised (see next section 0).

6. The following data is sent to the server: Pseudonymized MAC address,

signal strength, date, time, spoofed indicator and sensor ID62, with associated 'status 1' to

to indicate that the relevant data relates to the moment the mobile device entered the

reach came.63

The director of Bureau RMC

stated: “It is immediately replaced on the sensor, so the MAC address is immediately hashed on the sensor.”64 Also

the website www.citytraffic.nl states that the MAC address is immediately pseudonymised.65 The AP

notes, however, that this is not confirmed by the software code of the sensors. It shows

namely, as explained in the previous marginal, that there are unpseudonymized MAC addresses

are stored in the working memory of the sensors.

An employee of [CONFIDENTIAL] has stated the following about what happens as long as a

device with the WiFi enabled is within range of a sensor: “The MAC address becomes the whole

time captured, the sensor checks if the MAC address has been seen before, if yes, it increments the last seen time and this

process repeats itself until the MAC address has not been seen for two minutes.”66 The software code and its own analysis

of this software code by a supervisor of the AP confirms this operation.67

An employee of [CONFIDENTIAL] has stated the following about when the data will be

forwarded to a server: “The status 1 message is forwarded directly to the server, the status 2 message as

the MAC address is out of sight for two minutes. It is forwarded live, not every minute, for example. So from each

passant, data is forwarded twice.”68 The software code and our own analysis of this

software code by a supervisor of the AP confirms this operation.69 The collection of both the

time when the MAC address first comes into range (State 1) as the last seen time

(state 2) is used to determine the residence time of the MAC address within the range of the sensor,

see appendix 1, page 42 et seq. (long-term table).

60 This has been confirmed by the employees of [CONFIDENTIAL], page 3 of the report of statement by Bureau RMC and

employees

[CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

61 The indicator is 1 if there is a spoofed MAC address and 0 if the MAC address is not spoofed.

62 This is a unique number linked to each sensor.

63 In addition to 'status 1', a 'status 2' is also used, which refers to the moment the range of the sensor is left.

64 Page 3 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55). Bureau RMC and the employees of [CONFIDENTIAL] sometimes use the term 'hashing' in their statements to pseudonymize.

65 Screenshots of web pages www.citytraffic.nl recorded on 31 July 2019 (file document 54).

66 Page 3 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

67 [CONFIDENTIAL] and Declaration of Official Acts analysis source code of 18 February 2020 (file document 78).

68 Page 2 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

69 [CONFIDENTIAL] and Declaration of Official Acts analysis source code of 18 February 2020 (file document 78).

The software code shows that as soon as a detected mobile device is out of range of the sensor the following data is sent to the server: Status '2', pseudonymised MAC address, last measured signal strength in range, last determined date and time in range (this refers to the time of day minus the two minutes), spoofed indicator and sensor ID.70

When asked how long the MAC addresses remain in the working memory of each sensor, a employee of [CONFIDENTIAL] replied: “The data will be sent to the server as soon as it is detected that the device has been out of range of the sensor for 2 minutes. Then the data from the sensor disappears. So how long the data is kept depends on how long someone is in the area/range of the sensor plus 2 minutes.”71 The software code and a proprietary analysis of this software code by a supervisor of the AP confirms this effect.72

Based on the foregoing, the AP concludes that at least from May 25, 2018 to the present, each sensor

had the same effect in the city center of Enschede. The sensors have during this period of
all mobile devices within range on which the Wi-Fi was enabled, the MAC address,
signal strength, date and time captured and temporarily stored in the working memory of the sensor.
This storage lasted as long as the device was within range of the sensor plus two minutes.
The AP also notes that the sensors scan continuously. Finally, the AP notes that each
detected device upon entry and two minutes after departure from the range of the sensor in real time
the following data has been sent to the server: status 1 or 2, pseudonymised MAC address,
signal strength, date and time, spoofed indicator and sensor ID.
Pseudonymizing the MAC address on the sensors
An employee of [CONFIDENTIAL] has stated that on every sensor in Enschede the same
pseudonymization method is applied and that this method has not been changed since 25 May 2018.73
When asked by the AP which method is used, an employee of [CONFIDENTIAL]
answered: “[CONFIDENTIAL]”74 This is also apparent from the software code75 and a [CONFIDENTIAL]
drafted document on the pseudonymization method.76
During the on-site investigation on May 29, 2019, an employee of [CONFIDENTIAL]
stated: “One MAC address practically yields one hashed number, there is minimal chance of collision, namely two
MAC addresses the same

70 [CONFIDENTIAL] and Declaration of Official Acts analysis source code of 18 February 2020 (file document 78).

71 Page 2 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

72 [CONFIDENTIAL] and Declaration of Official Acts analysis source code of 18 February 2020 (file document 78).

73 Pages 2 and 4 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55). The employee of [CONFIDENTIAL] also stated that the same method on all their sensors running in the Netherlands.

74 Page 4 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

75 [CONFIDENTIAL] and Declaration of Official Acts analysis source code of 18 February 2020 (file document 78).

76 MAC hashing analysis prepared by [CONFIDENTIAL] (no date), received from [CONFIDENTIAL] on 3 June 2019 (file document

43).

yield hashed value."77 This is apparent from the document on the pseudonymisation method [CONFIDENTIAL] chose this method precisely because there is only a negligible chance on equal results.78

Based on the foregoing, the AP concludes that one and the same pseudonymization method is running on all sensors in the city center of Enschede and that this method has not changed since 25 May 2018.

In addition, the AP notes that the pseudonymization results in one MAC address on each of the sensors leads to one and the same pseudonymised MAC address.

The short-term table on the server

For this purpose, the AP has established that at least from 25 May 2018 in the city center of Enschede van any mobile device that had its Wi-Fi turned on and passed through the range of a sensor there data from the mobile device twice, namely when entering the range and two minutes after out of range, are sent to the server in real time. In addition, the AP has concluded that per January 1, 2019 All pseudonymised MAC addresses incoming to the server will be truncated.

Regarding this, an employee of [CONFIDENTIAL] has stated: "If the hashed79 MAC address arrives it is clipped in memory (real time) and then written into a raw table, (…)."80

An employee of [CONFIDENTIAL] also stated: "We use two tables on the server. A short-term table containing today's data and a long-term table containing 6-month data."81 The AP

will deal with the short-term table first.

About what will be cut off from the pseudonymised MAC address as of January 1, 2019, a

employee of [CONFIDENTIAL] stated: “[CONFIDENTIAL], omitting the colon.”82

And: “Only the hashed MAC address is truncated and the rest of the data does not change that.”83 The

software code confirms the foregoing, with the addition that also removes the colons from the truncated

pseudonymised MAC address will be removed.84 The result after truncation is a string of

[CONFIDENTIAL] consisting of 0-9 or a-z without colons (see MACNUMBER column in

Figure 3).

77 Page 5 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

78 Page 3 last paragraph and page 4 third paragraph MAC hashing analysis prepared by [CONFIDENTIAL] (no date), received

of [CONFIDENTIAL] on 3 June 2019 (file document 43).

79 [CONFIDENTIAL] uses the term 'hashed' here as an alternative to 'pseudonymised'.

80 Page 6 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

81 Page 7 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

82 Page 6 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

83 Page 6 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

84 [CONFIDENTIAL] and Declaration of Official Acts analysis source code of 18 February 2020 (file document 78).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

During the on-site investigation, an employee of [CONFIDENTIAL] asked the supervisors of

allowed the AP to inspect the short-term table.85 These employees also received a

part of the short-term table with the data collected in Enschede on 29 May 2019

to the AP.86 A screenshot of the first few records of this short-term table filtered by the

sensor [CONFIDENTIAL] concerns:

Figure 3: Screenshot of the first part of the short-term table for May 29, 2019 for a sensor

An employee of [CONFIDENTIAL] has provided the following explanation of the columns:

“-

-

-

-

-

-

-

"HOSTNAME" is the unique identifier of the sensor, the location ID of a sensor.

"MACNUMBER" is the pseudonymized and truncated MAC address.

'DATE' is the day-week-year.

"TIME" is the time on that day when the device was scanned. (…).

"SIGNAL" is the signal strength at which the device has been detected.

'STATUS' 1 is when he was first sighted and status 2 is when he is outside

the range of the sensor.

"SPOOFED" is 1 if it was a spoofed MAC address (and 0 if not). (…).”87

85 Statement of official acts on site investigation Bureau RMC and [CONFIDENTIAL] on 29 May 2019 (file document 39).

86 Export Enschede 29-5-2019.zip, received from [CONFIDENTIAL] on 3 June 2019 (file document 42). The first detection

(record in the

table) was at time 00:00:00 and the last at time 20:20:37.

87 Pages 9 and 10 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019

(files 49 and 55).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

The AP notes that DATE is recorded at the day level and the TIME is accurate to the second. The

HOSTNAME is the unique sensor ID, each of the eleven sensors in the city center of Enschede has one

unique [CONFIDENTIAL] code.88

In the screenshot above, blue and red are two consecutive state 1 and state 2 records

boxed from the same truncated pseudonymized MAC address ([CONFIDENTIAL]). later shows

indicates to the AP that each of these two records will be merged into one record in the long-term table.

Based on the foregoing, the AP concludes that since at least May 25, 2018, the data stored on one

day are measured by the sensors in the city center of Enschede are collected daily in the

short-term table.89 The time of day at which the device was scanned by the sensor is calculated on

recorded accurately to the second. In the period up to January 1, 2019, the pseudonymised MAC

address not cut off when entering the server, but in the period from 1 January 2019. Cut it off

involves removing the last three characters of the pseudonymised MAC address (without

colon). The other data sent to the server i.e. sensor ID, date, time,

signal strength, status and spoofed indicator are taken raw in the short-term table.

The application of filters

During the on-site investigation at Bureau RMC on 29 May 2019, an employee of

[CONFIDENTIAL] stated that on the short-term table, covered in the previous paragraph, every night

certain filters are applied after which the remaining records are added to the long-term table

added.90 This [CONFIDENTIAL] employee explained this in a document: “The

code for the filters (…) run in the morning at 00:15:00 in timezone Europe/Amsterdam on the detections of the previous

day. We use two types of filters when processing the data from the RAWRESULTS_HTTP_WIFI table to

tables where the data is for a longer period. These are the opt-out filter and the resident filter.”91

[CONFIDENTIAL]'s explanation of the opt-out filter states: “The opt-out filter removes detections from the

(…) table when the detections contain a hashed and truncated mac address that is also in the opt-out list.”92

The Municipal Executive of B&W Enschede has been providing information about this opt-out list since the start of the Wi-Fi measurements on the website

from the municipality the following explanation: “Everyone has the ability to change his MAC addresses from mobile

register devices on the City Traffic website for an opt-out register. After this, these MAC addresses are not

longer counted and included in our investigations. The opt-out register can be found at http://citytraffic.nl/site/page/opt-

88 During the on-site investigation at Bureau RMC on 29 May 2019, the AP was provided with a list of the sensor IDs and the corresponding street

in the city center of Enschede.

89 With the exception of the period from December 10, 2018 to January 3, 2019, because the sensors were switched off at that time, see

appendix 1, section 2.5.

90 Page 7 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

91 Page 3 of source code, clipping and filters.pdf, received from [CONFIDENTIAL] on 20 June 2019 (file document 46).

92 Page 3 of source code, clipping and filters.pdf, received from [CONFIDENTIAL] on June 20, 2019 (file document 46).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

out.”93 On the aforementioned web page at www.citytraffic.nl there is an input field that allows someone to enter the MAC address of his/her mobile device can be placed on the opt-out list.

The AP notes that because the opt-out filter is only applied to the short-term table, it is not the case MAC addresses that have been specified are no longer captured by the sensors.

[CONFIDENTIAL]'s explanation of the resident filter concerns: “The resident filter removes the detections from the (…) table for a mac address when the mac address at the same scanner on a day is both between 05:00 and 07:00 seen as between 10:00 PM and 11:59:59 PM.” 94

The software code shows that the resident filter works as follows: 95 all records of a clipped pseudonymised MAC address in the short-term table will be removed if truncated pseudonymised MAC address both between 5 and 7 am and between 10 and 12 pm in or outside the range of same sensor. This is because there must be a detection in both time periods. This effect has as a result if, for example, a person with a mobile device on which the Wi-Fi is switched on lives within range of a sensor and is home all day, records from his/her mobile device cannot be filtered out. The same applies, for example, to residents who live alone between 5 and 7 or leave the house or come home between 22 and 24 hours.

With regard to the resident filter, the AP notes that it collected every night on the daily data is applied, which means that each day it is determined anew whether someone qualifies as resident or not.96 It follows from Figure 7 on page 48 that the qualification can differ on a daily basis.

Since the start of the Wi-Fi measurements in September 2017, the Municipal Executive of B&W Enschede has published on the website of the municipality the following Q&A stand for residents of the city center of Enschede:97

“I live in the city centre, what will be done with my data?

City Traffic counts the number of passers-by in the shopping street. The sensors therefore have an automatic filter around residents not included in the counts. City Traffic knows that signals from residents mainly before and after

store opening hours are measured. That is why City Traffic assumes that when the same signal is sent twice per day, once in the morning and once in the evening, this is a signal from a resident. These signals are from that moment on every day automatically filtered out. Therefore, if you live near a counting point, you will not be included in the counts."

The AP notes that this text contains several inaccuracies. First, it says that the sensors are the filter apply, while this is only done on the server. Second, it is suggested that one-off becomes determines whether someone lives near a sensor and then automatically gets out every day filtered out, when in reality the filter determines every night whether someone is a resident or not.

93 www.enschede.nl/sites/default/files/QandAokt2017.pdf, last visited by the AP on 6 January 2020.

94 Page 3 of source code, clipping and filters.pdf, received from [CONFIDENTIAL] on June 20, 2019 (file document 46).

95 ConvertWifi.php, received from [CONFIDENTIAL] on 20 June 2019 (file document 46). Declaration of Official Acts analysis source code of February 18, 2020 (file document 78).

96 Declaration of Official Acts analysis source code of 18 February 2020 (file document 78).

97 Q&As, appendices 5 and 6 to the letter of 24 May 2019 from the Municipal Executive of B&W Enschede to the AP (file document 26).

Finally, the statement that residents are not included in the counts is not correct in all cases, as follows from the analysis of the resident filter above.

Based on the foregoing, the AP concludes that there are two filters on the short-term table every night are applied, namely an opt-out filter and a resident filter. These filters do that certain records from the short-term table do not end up in the long-term table. In addition the AP notes that the residents filter does not filter out all residents and that the website of the

municipality is given incorrect information about this.

The long-term table on the server

Because the clipping of the pseudonymised MAC address was introduced on January 1, 2019, the long-term table pseudonymised MAC addresses until January 1, 2019 and after January 1, 2019 only truncated pseudonymised MAC addresses. An employee of [CONFIDENTIAL] has stated: “The hashed mac addresses that were in the database around that period are retroactive cut off. 98

At the request of the AP, [CONFIDENTIAL] released the long-term table with the data on Enschede provided for 29 May 2019 only.99 A screenshot of the first few records of this long-term table, filtered by the two truncated pseudonymised MAC addresses boxed in the short-term table in Figure 3 concerns:

Figure 4: Long-Term Table Section Screenshot

From a comparison between the blue and red boxed records in the short-term table and the long-term table (Figure 3 and Figure 4) shows that two consecutive records (with status 1 and 2) of the same truncated pseudonymised MAC address in the short-term table results in one record in the long-term table. The timeIn (state 1) and TimeOut (state 2) are set one after the other and the Retention is set

98 Page 3 of source code, clipping and filters.pdf, received from [CONFIDENTIAL] on June 20, 2019 (file document 46) and page 6 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

99 Export Enschede 5/29/2019 long term table.zip, received from [CONFIDENTIAL] on 6 September 2019 (file item 60).

seconds (the time in between) is calculated. It also appears from the comparison of both tables that spoofed

MAC addresses in the short-term table are not included in the long-term table.100

[CONFIDENTIAL] has provided the following explanation of the columns in the

long-term table:101

“ID = ID of record

Mac = truncated hash value of a mac address

Date = Date of sighting

TimeIn= observation start time

TimeOut = observation end time

Retention = TimeOut – TimeIn

BWCode = detection type (B = bluetooth, W = wifi),

nowadays we only have W detections

SignalStrengthIn = signal strength start time

observation

SignalStrengthOut = signal strength end time

observation

LocationId = always 0, no longer in use”

The DPA notes that in the above list by [CONFIDENTIAL] the column "[CONFIDENTIAL]" per

is not included by mistake, this column refers to the aforementioned sensor ID. In addition, the AP notes

that the TimeIn and TimeOut are in seconds, so that the Retention (the residence time) is also in seconds.

Bureau RMC has stated about the retention period of the data in the long-term table: “At the

municipality of Enschede, it was a retention period of six months from the start of the counts, but this has not been the case

since then

changed.”102 The director of Bureau RMC later explained that on the first of the month the

data from the month of six months ago are deleted.103

Based on the foregoing, the AP concludes that, after applying the filters to the short-term table,

two consecutive records of the same (truncated) pseudonymised MAC address resulted in one

record in the long-term table. From May 25, 2018 to January 1, 2019, the long-term table contained the following data: pseudonymised MAC address, date, TimeIn, TimeOut, Retention, SignalStrengthIn, SignalStrengthOut. As of January 1, 2019, the pseudonymised MAC address and the pseudonymised MAC address given was replaced by the truncated one pseudonymised MAC address. The AP also notes that in the long-term table from 25 May 2018 data covered a period of between six and seven months.

The processing of the raw data and the figures that the B&W Enschede Board receives from Bureau RMC

The data in the long-term table form the basis for the figures that the Municipal Executive of B&W Enschede van Bureau RMC receives. It follows from the following statements by the director of Bureau RMC that the data in the long-term table are first deduplicated and then subjected to statistical operations are applied.

100 See also appendix 1, paragraph 1.2, page 35, which contains the statement of employees [CONFIDENTIAL] that spoofed MAC addresses are not included in the counts.

101 Kolomen.doc, received from [CONFIDENTIAL] on September 6, 2019 (file document 60).

102 Page 7 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

103 Emails of 20 December 2019 and 15 January 2020 from Bureau RMC to the AP (file documents 76 and 77).

During the investigation, an employee of [CONFIDENTIAL] was on site on May 29, 2019 stated: “Yes, within a zone we deduplicate.” The director of Bureau RMC added: “We want this

deduplication because we are looking for unique visitors to the city center. The customer is looking for wallets and not to passers-by. Someone who has been counted 10x is not a buyer 10x, but is 1x a buyer who has been seen 10x. The customers want

know the number of unique visitors within a zone. (…). So if the two of you walk into the city center of Enschede and there is no one else there, so in the aggregated half-hour image you will only return to the first sensor where you were seen. This does not apply to measuring, if you walk through the city center of Enschede you will be seen at every sensor and this is because

right into the raw data." 104

An employee of [CONFIDENTIAL] then stated: "We have it to deduplicate

pseudonymised MAC address. We count unique numbers, so if a MAC address is caught by the

sensor and that MAC address comes back there an hour later then we see it's the same phone because it's the same hash. The pseudonymization method is the same on all sensors and we anonymize on the server by clipping so we

can see across the set of sensors if the same MAC address has been true (not just on the sensor). We do have

loss of detail because we are truncating on the server, but with some certainty we can say that the same

phone has been at sensor A and later at sensor B."

The director is responsible for the statistical processing that is then applied to the deduplicated data

of Bureau RMC stated: "Every sensor was 'hand-calibrated' once during the installation. Then the conversion

determined from the number of signals to the number of passers-by, because not everyone also has their WiFi switched on. This is what we do

once and we also carry out market research into any increase or decrease in Wi-Fi use." 105

And: "The hand calibration determines what percentage of passers-by are cyclists, for example. This

percentage is later deducted from the collected data so that we only have the passers-by. This is a

probability calculation. This makes our counts slightly less reliable because of how many cyclists and cars pass by on the

We apply the time of calibration as an average for the whole day. We also tell this very emphatically to customers." 106

At the request of the AP, the Municipal Executive of B&W Enschede has some reports it has from Bureau RMC

received and submitted to the AP.107 It follows from this that the Municipal Executive of Enschede B&W first of all submits

estimates

receives figures and graphs from various variables about the unique visitors to downtown

Enschede. Below is a screenshot showing the figures for the week from April 1, 2019 to April 7

2019.108 The names of the eleven sensors are also included here.

104 Page 9 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents

49

and 55).

105 Page 8 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents

49

and 55).

106 Page 8 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents

49

and 55).

107 Printout report week 37 2018 from City Traffic Tool, appendix 2 to the letter of 20 September 2018 from the Municipal

Executive of B&W Enschede to the

AP (file item 3). Citytraffic_number_counter point 4 Excel sheets and Citytraffic_week overview 4 Excel sheets, appendices 14

and 15 to the letter from

24 May 2019 from the Municipal Executive of B&W Enschede to the AP (file document 26).

108 enschede_Whole_export_2019w14.xls in Citytraffic_weekly overview 4 Excel sheets, appendix 15 to the letter dated 24

May 2019 from the

college B&W Enschede at the AP (file document 26).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

Figure 5: Weekly report from Bureau RMC to Board B&W Enschede week 1 to 7 April 2019

Secondly, the Municipal Executive of B&W Enschede receives estimates of the number of unique visitors per hour per sensor.109

Based on the foregoing, the AP notes that the Municipal Executive of B&W Enschede receives estimates of different variables about unique visitors to the city center of Enschede. For this purpose the applicable data in the long-term table are deduplicated based on the clipped pseudonymised MAC address and then perform certain statistical calculations on it applied.

Bureau RMC's City Traffic method privacy protocol

Specifically about the processing of personal data in the context of the City Traffic method Bureau RMC has drawn up a privacy protocol. During the period from May 25, 2018 to April 21 By 2020, there will be two consecutive versions of this privacy protocol on the Bureau RMC website the following passages were included in both versions:110

“1.1 In order to make our services possible, we process various passerby data. The passerby data include data from passers-by that can be directly or indirectly traced back to an individual passer-by. The passerby data can therefore be regarded as personal data within the meaning of the General Data Protection Regulation (GDPR). (…).

3.1 (…) The analysis results are only reported to our clients on an aggregated basis. This means that the data in these reports can no longer be traced back to the encrypted number (from the MAC address of the device) of a passer-by, nor to the data of a device that a passer-by carries with him. We therefore do not provide any personal data to our clients.”

109 Reply to 'Questions about the information that the municipality of Enschede receives from the RMC bureau' and Citytraffic_number_telpunt 4 Excel sheets, appendix 14 to a letter dated 24 May 2019 from the Municipal Executive of B&W Enschede to the AP (file document 26).

110 Privacy protocol passerby counts Bureau RMC latest update 10 April 2018 (file document 8) and Privacy protocol

In the first passage, Bureau RMC states that it is within the framework of the City Traffic method processes personal data within the meaning of the GDPR. The privacy protocol does not specify until what time the stage of the processing process this is the case. From the text at step 4 'Anonymize' in the infographic about the City Traffic method (see Figure 2), the AP deduces that Bureau RMC is of the opinion that it processes personal data up to the moment of anonymization. The text reads: “On the server the pseudonymised data is cut off so that it cannot be traced in any way to a unique device or individual. The data we have is therefore anonymous.”

Based on the foregoing, the AP concludes that Bureau RMC sees this specifically in its privacy protocol on processing via the City Traffic method, has included that it and/or its partners from any case 25 May 2018 process personal data within the meaning of the GDPR. The AP also concludes that Bureau RMC has included in its privacy protocol that the reports that clients of Bureau RMC received do not contain any personal data.

Deduce living patterns from the long-term table

As determined by the AP in appendix 1 paragraph 2.5, Bureau RMC has adopted the 'anonymize on the server' introduced. This means that of any pseudonymised MAC address at reception on the server the last three characters (without a colon) are removed.

The AP notes that, unlike about pseudonymizing the MAC address, the AP's of [CONFIDENTIAL] whether Bureau RMC has not received a document with a detailed explanation the clipping and why this method of anonymisation was chosen.111 In general, this applies

clipping an attribute is an anonymization technique that makes an attribute

generalized. For example, times in minutes can be generalized to one

time interval (hour, day, month).

The clipping results in not one but several pseudonymised MAC addresses

one and the same truncated pseudonymised MAC address.112. Shearing looks on worldwide

issued MAC addresses; MAC addresses are not issued by country or location.

To test whether cutting off at a local level, namely in the city center of Enschede, has led to

enough mobile devices with the same truncated pseudonymised MAC address to access the data

to make it anonymous, a supervisor of the AP has the long-term table with data from a number

common truncated pseudonymized MAC addresses over weeks 23 through 34 of

2019 analysed.113 If there are enough devices locally with the same clipped pseudonymised

MAC address should move in the inner city then no living patterns should be visible in

the data. This is because it concerns living patterns of multiple devices (and therefore people).

111 The document on the pseudonymization method concerns the document MAC hashing analysis prepared by

[CONFIDENTIAL],

received from [CONFIDENTIAL] on 3 June 2019 (file document 43).

112 See page 19 of WP 216 Advice 5/2014 on anonymisation techniques.

113 Export Enschede Sep-Dec long term table.zip and Export Enschede Jun - Aug 2019 long term table.zip, provided by

[CONFIDENTIAL] on 12 and 16 December 2019 (files 69 and 72).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

After its own investigation, the AP has found that the data of certain truncated

pseudonymised MAC address, clear living patterns of individuals can be derived. This follows from

the Figure 6, Figure 7, Figure 8 and Figure 9 included below, containing visualizations of the data pseudonymised MAC addresses cut off from four.114 The days are shown horizontally in each visualization of the week and vertically the week number in 2019. Each gray square represents a whole day, from 0:00 night until 23:59:59. The hours 8:00 and 18:00 are marked. A colored stripe or area means that the truncated pseudonymized MAC address in question from the start moment to the end moment within range of the relevant sensor.

The first visualization below shows a consistent presence within range of the sensor [CONFIDENTIAL] (red), namely every Monday afternoon, Wednesday and Saturday from approximately 10:00 to 6:00 PM and Thursday from about 10:00 AM to 9:00 PM. The pattern is very similar to the shopping hours that apply in the city center of Enschede, with late shopping on Thursday.115 Also follows from the pattern that precedes the truncated pseudonymized MAC address every last Sunday of the month was within the red sensor for a few hours. Given this pattern, the AP considers it not inconceivable that the belongs to an employee or manager of one of the shops in the Langestraat in Enschede, where the sensor [CONFIDENTIAL] hangs.116

Figure 6: Initial visualization of truncated pseudonymised MAC address

114 Declaration of Official Acts analysis long-term table of 18 February 2020 (file document 79).

115 https://www.enschede.nl/vrijetijd/openingstijden-winkels-en-koopzondagen

116 Excel list location of sensors, appendix to e-mail of 23 May 2019 from Bureau RMC to the AP (file item 25).

As with the visualization above, there are also several hours in one day in the visualization below presence within range of one sensor (pink). It is noticeable here that on one day there are either none registration is visible (no dashes) or registrations spread over the day. This is the result of the on

The fact described on pages 40 and 41 is that the resident filter is applied daily and therefore a different one every day outcome (whether or not a resident). In addition, you can see in, for example, the Tuesday in week 23 that if there are registrations between 5 a.m. and 7 a.m. but not between 10 p.m. and 12 a.m., then the resident filter is not is activated (after all, there are dashes in this day). The AP does not consider it inconceivable, given the nocturnal registrations, that the above pattern belongs to a resident.

Figure 7: Second visualization of truncated pseudonymised MAC address

The third visualization below shows a truncated pseudonymized MAC address that is stored on Tuesday through with Friday every day between about 8:00 AM and 11:00 AM is signaled by many of the sensors in the city center of Enschede. It shows a regular movement pattern across multiple sensors. It pattern could be, for example, of a parcel deliverer.

Figure 8: Third visualization of truncated pseudonymised MAC address

The fourth visualization below shows a truncated pseudonymised MAC address that is used on Tuesdays through with Saturday between 04:00 and 05:00 at night by some of the sensors in the city center of Enschede has been taken care of. Perhaps this refers to a person who likes to take a walk at night.

Figure 9: Fourth visualization of truncated pseudonymised MAC address

Based on the foregoing, the AP concludes that the long-term table after January 1, 2019

clear living patterns can be distilled. Given the regularity of the patterns it is reasonable

can be concluded that the registrations belonging to the pattern belong to one mobile device.117

1.3 Duration of processing and number of data subjects

The AP has established above that since at least May 25, 2018, in the city center of Enschede

data from mobile devices with Wi-Fi enabled are collected and processed. The AP

has determined that the sensors in the period from 10 December 2018 to 3 January 2019

have been standing, so no new data were collected during this period.118 However, previously collected

data were stored in the long-term table during this period, so there were no changes in this

period of data processing.

Until the end of the investigation (April 21, 2020), the AP had several indications that the

Wi-Fi measurements are still being performed. This is what the website of the municipality of Enschede stated

that Wi-Fi measurements were carried out in the city center119 and the website also reported

www.binnenstadsmonitorenschede.nl still weekly about the number of unique visitors in the

inner city of Enschede.120 In addition, the AP neither of the B&W Enschede nor of

Bureau RMC received a message during the investigation that the WiFi measurements have stopped. During the day

the enforcement procedure of the AP, the Municipal Executive of B&W Enschede stated in its opinion that the

college has discontinued the wifi counts. On April 30, 2020, the Municipal Executive of Enschede B&W Enschede

RMC has been given the order to switch off the sensors as of 1 May 2020. The sensors do not deliver

counting data more from 1 May 2020.121 The AP therefore notes that the duration of the processing operations exceeds the

period

from May 25, 2018 to April 30, 2020.

The exact number of data subjects of whom, in the period from 25 May 2018 to April 2020, via his or her mobile

device data processed cannot be determined because by [CONFIDENTIAL] and Office

RMC does not store the data longer than between six and seven months. On the basis of the

Long-term table provided by [CONFIDENTIAL] to the AP with data for the period from 1 June

However, an estimate can be made of the number of mobile devices from 2019 to 6 December 2019

of data subjects whose data were processed in the period from 25 May 2018 to 4 April 2020.122

The chart below shows the number of unique truncated pseudonymised MAC addresses in the 27 weeks

in the period from June 1, 2019 to December 6, 2019. Any clipped pseudonymised

MAC address therefore appears in the chart once, namely in the week in which it appears for the first time

detected by a sensor in the city center of Enschede.

117 Registrations that fall outside this pattern may originate from other mobile devices.

118 See also appendix 1, section 2.5.

119 https://www.enschede.nl/bestuur/privacy/wifi-tellingen-binnenstad (last visited on 26 February 2020).

120 https://www.binnenstadsmonitorenschede.nl/visitors-week figures (last visited on 26 February 2020).

121 Letter of 16 February 2021 from the Municipal Executive of B&W Enschede to the AP, page 3 and appendix 2.

122 The unique number of truncated pseudonymised MAC addresses is used as an estimator for the number of unique

Mobile Devices.

Figure 10: Weekly number of detections from June 1 to December 6, 2019

The graph shows that there are many new detected mobile devices in the first weeks. In the weeks

after that, the number of new detections levels off. In the last week it was about 16,000 mobile

devices. In total, there were data from 671,701 unique mobiles during this 27-week period

devices in the long-term table.

If previous figures for the period 1 June - 6 December 2019 are applied to the period of 25

May 2018 to April 4, 2020, leading to an estimate of roughly 1.8 million unique mobile devices

of which data has been processed via the sensors in Enschede since 25 May 2018. It is assumed that

the first 27 weeks after May 25, 2018 are the same as the graph above. It is also assumed that after

the 27 weeks up to April 4, 2020, the number of new detections is 16,000 every week.123 This number keeps

incidentally, do not take into account the fact that for residents and persons who work in the downtown area

Enschede and who have enabled WiFi on their mobile device, they do not once, but (many)

detected by the sensors more often.

On the basis of the foregoing, the AP concludes that the Municipal Executive of B&W Enschede will in any case from 25 May 2018 to date has processed data from roughly 1.8 million unique mobile devices and that

the number of detections will be significantly higher.

123 From May 25, 2018 to April 4, 2020, this concerns 31 weeks in 2018, 52 weeks in 2019 and 14 weeks in 2020. The calculation is therefore as follows:

671,701 (for the first 27 weeks from May 25, 2018) + ((31-27)+52+14) x 16,000 = 1,791,701.

2. Facts about the concept of controller

2.1 Decision to start Wi-Fi measurements

The decision to collect data about visitors to the city center of Enschede via sensors

(hereinafter also: carrying out WiFi measurements) was taken by the B&W Enschede college. This follows from it

Commission decision, the first page of which is reproduced below.124

Figure 11: First page of the Executive Board decision, dated September 5, 2017, start WiFi measurements.

124 Board decision of 5 September 2017, appendix to e-mail of 23 September 2019 from the Board of B&W Enschede to the AP (file document

62).

March 11, 2021

Our reference

[CONFIDENTIAL]

It follows from this page that the Municipal Executive of Enschede B&W agreed to the proposal on 5 September 2017

of the alderman to switch from 1-yearly manual counts to

24/7 Wi-Fi measurements.

After the municipal council decision of September 5, 2017, the Municipal Executive of B&W Enschede has replaced the

municipal council of

Enschede was informed by letter.125 In addition, there is a press release on the municipality's website

as a number of Q&As about the Wi-Fi measurements.126 In this communication it is stated that City

Traffic B.V. would perform the Wi-Fi measurements.

City Traffic B.V. was at the time a company owned by Bureau RMC and [CONFIDENTIAL]. On

This company was disbanded on 24 May 2018.127 Since then, Bureau RMC has been conducting this on behalf of the Board

B&W Enschede performs the WiFi measurements, whereby Bureau RMC purchases certain services from

[CONFIDENTIAL]. Bureau RMC now uses the term 'City Traffic' for its service via WiFi measurements

to count unique visitors in cities, among others.128

The director of Bureau RMC talks about the tender process that preceded the Board decision

stated: “City Traffic has existed since 2010 and has positioned itself as an alternative to Locatus

pass-through counts. Locatus was the party that did hand counts once a year. I then founded CityTraffic

to generate more dynamic data. Both Locatus and CityTraffic have been asked by the Municipality of Enschede for a

propose to do Wi-Fi counts there. (…) The reason for the municipality's request was the fact that via

wanted to roll out a certain subsidy free Wi-Fi network with NDIX129 and then the RMC agency was asked whether we

network to count passers-by. Part of the competition was also that we had to have a correlation

show between the counts of NDIX. It was later decided not to use the NDIX counts.”130

The quotation issued by Bureau RMC confirms that the Board had requested B&W Enschede

connection to the network of NDIX.131

In response to questions from the AP about the municipality's influence on the location of the sensors, the director of Bureau RMC replied: “The locations of the sensors for the NDIX network had already been determined. The municipality Enschede then indicated which areas/streets it missed and therefore where sensors should be placed. The

125 Letter of 5 September 2017 from the Municipal Executive of Enschede to the municipal council, appendix 3 to the letter of 24 May 2019 from the

college B&W Enschede at the AP (file document 26).

126 Press release of 6 Sept 2017 about measuring crowds with sensors and Q&A further information 24/7 counts in the city centre, appendix 4 and

5 with the letter of 24 May 2019 from the Municipal Executive of B&W Enschede to the AP (file document 26).

127 Excerpt Chamber of Commerce City Traffic B.V. of 9 August 2019 (file document 81).

128 Page 10 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55). See also www.citytraffic.nl (file document 54).

129 NDIX B.V. is an organization based in Enschede that works on managing and further developing a digital marketplace and making maximum bandwidth available to companies to stimulate innovation. See www.ndix.net.

130 Page 10 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

131 Page 2 of the proposal for Monitoring Visitor Flows in the Inner City of Enschede from Bureau RMC, appendix 1 to a letter dated 24 May 2019 from the

college B&W Enschede at the AP (file document 26).

The municipality has therefore determined the locations of the sensors. (…) the municipality had the coordinating role in the assignment. For

in terms of the number of sensors, I would have preferred many more. 132

On the basis of the foregoing, the AP concludes that the B&W Enschede Board took the initiative and the

made the final decision to start 24/7 measurements via sensors in September 6, 2017

the city center of Enschede. The Municipal Executive of B&W Enschede has sent two companies a tender for this

bring out. The contract has been awarded to City Traffic B.V., now Bureau RMC. Finally, the AP notes that

the Municipal Executive of B&W Enschede had a guiding role in the number and locations of the sensors.

2.2 Purpose of the Wi-Fi measurements for the Municipal Executive of B&W Enschede

In the Executive Board decision of 5 September 2017, the Executive Board of B&W Enschede has set the goal of the Wi-Fi

measurements

in the city center formulated as follows: “We would like to know how this location is developing: how many passers-by

walk through the streets, how many visitors do the city center have, how long do people stay in the city center and where do

they walk

by? To get a better picture of this, we will switch from 1-yearly manual counts to

24/7 counts via sensors.”133

Since December 2017, the Q&A on the website of the municipality of Enschede has stated the following about the goal

of the WiFi measurements: “The municipality of Enschede invests a lot in the city center and wants to be able to measure the

effects.

We do this through the passerby counts via sensors that give us daily insight into the number of visitors and the

visitor flows in the city centre. This gives us an idea of the attractiveness of our city centre, of the

influence of spatial changes in the city center and of effects of events, for example,

promotional campaigns and shopping times. The counts via sensors are also interesting for entrepreneurs who are established

or

who want to settle in the city center and for investors.”134

After the start of the Wi-Fi measurements, the complainant submitted a complaint to the Municipal Executive of Enschede.135

In

In response to the complaint, the Municipal Executive of Enschede writes in a letter to the complainant:

“- There is a clear goal (we invest a lot in the city center and want to measure the effects);

- The basis for the counts is “legitimate interest” (responsible use of public funds);” 136

Based on the foregoing, the AP concludes that the Wi-Fi measurements are carried out with the aim of measuring the effects of investments by the municipality of Enschede in the city center with a view to a responsible use of public funds. The Municipal Executive of Enschede considers the Wi-Fi measurements to be lawful because, according to her, they take place on the basis of 'legitimate interest'.

132 Page 11 of report of statement from Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 and e-mail dated 19

August 2019 from Bureau RMC to the AP (file documents 49 and 55).

133 See Figure 1 in this report.

134 Q&A modified December 2017, appendix 6 to the letter of 24 May 2019 from the Municipal Executive of B&W Enschede to the AP (file document 26). A

a similar text was published on the municipality's website from the Municipal Executive decision of 5 September 2017.

135 Letter of 10 November 2017 from the complainant to the municipality of Enschede, annex to the letter of 16 July 2018 from the complainant to the AP (file document 1).

136 Letter of 21 December 2017 from the Municipal Executive of B&W Enschede to the complainant, appendix to letter of 16 July 2018 from the complainant to the AP

(file item 1).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

2.3 Processor Agreement between College B&W Enschede and Bureau RMC

On September 26, 2017, the Board of B&W Enschede and the predecessor of Bureau RMC specifically with regard to the processing of personal data in the context of the WiFi measurements in the

inner city of Enschede a processing agreement as referred to in Article 14 of the then applicable Act protection of personal data (hereinafter: Wbp) closed.137

The preamble names the two parties between whom the agreement has been concluded: “The Municipality of Enschede, further

to be called the responsible party, legally represented in this matter by: [CONFIDENTIAL] and City Traffic, established in Amsterdam, hereinafter referred to as the processor, legally represented by [CONFIDENTIAL], declare to have agreed (…)”

The first, third and fifth paragraph of Article 4 of the processor agreement stipulates the following about the rights and obligations of the two parties:

“1. The Board of Mayor and Aldermen of the Municipality of Enschede is responsible within the meaning of the Wbp.

3. The processor processes data for the controller in accordance with his instructions.

5. When processing personal data in the context of the activities referred to in Article 3, the processor will act in accordance with applicable laws and regulations regarding the protection of personal data. The processor only processes personal data on behalf of the Strategy and Policy Department will follow all reasonable instructions in this regard, subject to deviating legal obligations.

6. The processor will at all times, at the first request of the controller, immediately provide all of the Municipal Enschede personal data with regard to this processing agreement to the responsible ter hand.”

Article 7, on the involvement of third parties, provides:

“1. The processor is only entitled to outsource the performance of the work in whole or in part to third parties with the prior written consent of the responsible person.

2. We agree that the processor has the data processed by [CONFIDENTIAL]. Editor has with this one party entered into a processing agreement.

(…)”

Based on the foregoing, the AP concludes that the B&W Enschede college sees itself as

controller within the meaning of the Wbp (currently the AVG) for the execution of

wifi measurements. In addition, the AP has established that City Traffic B.V., now Bureau RMC, uses personal data processed on behalf of the Municipal Executive of B&W Enschede, must follow its instructions and at the request of the Municipal Executive of B&W Enschede must submit the personal data. Finally, it follows from the foregoing that the Municipal Executive of Enschede has agreed that Bureau RMC has hired [CONFIDENTIAL]

for processing the personal data.

137 Processor agreement to monitor visitor flows in the city center of Enschede dated 26 September 2017, appendix 2 to the letter of 29 October

2018 from the Municipal Executive of B&W Enschede to the AP (file document 6).

2.4 The services that [CONFIDENTIAL] provides to Bureau RMC

Bureau RMC rents for the installation and maintenance of the sensors in the city center of Enschede [CONFIDENTIAL]. This is apparent from the following statements by the director of Bureau RMC:

“RMC purchases a subscription from [CONFIDENTIAL] for the sensors and that includes everything: the hardware, software, firmware, installation, service, maintenance, etc. This is arranged in a service level agreement between RMC and [CONFIDENTIAL]. The physical management of the sensors lies with [CONFIDENTIAL]. Then the council takes over Enschede subscribes to RMC for these sensors.”138

And, when asked who calibrates the sensor during installation: “The installer of the sensor, so someone from [CONFIDENTIAL].”139

The aforementioned service level agreement has been submitted to the AP by the director of Bureau RMC.

The service level agreement of October 31, 2016 confirms that [CONFIDENTIAL] the installation and performs maintenance of the sensors for Bureau RMC.140

The service level agreement also shows that Bureau RMC hires [CONFIDENTIAL] for the
collecting data with the sensors and validating that data.141 This is confirmed by
the fact that during the investigation the employees of [CONFIDENTIAL] generally used the
have answered detailed questions from the AP about the collection and processing of the data142 and the
submitted the necessary documentation. It also follows from the submitted invoice that [CONFIDENTIAL]
pays for the rented server space at Amazon AWS.143
Article 7 of the service level agreement states the following about the data collected with the sensors
agreement between [CONFIDENTIAL] (the 'contractor') and Bureau RMC (the 'customer'):
“The contractor is in no way entitled to process data from the customer in any way for a purpose
otherwise than primarily applicable to the customer. (…) The customer can at any time demand the data as well as the
require the contractor to delete data.”
Based on the foregoing, the AP finds that Bureau RMC hires [CONFIDENTIAL] for the
installation and maintenance of the sensors in the city center of Enschede and for the collection and
validating the data collected with the sensors. The AP also notes that Bureau RMC
on the basis of the service level agreement at any time the data that [CONFIDENTIAL] collects
and processed can claim.
138 Page 1 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents
49
and 55).
139 Page 8 of report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents
49
and 55).
140 Article 1 of the Service Level Agreement [CONFIDENTIAL]-Bureau RMC, appendix 1 part 4 to the Report of Official Acts
on-site investigation at Bureau RMC on 29 May 2019 (file document 39).
141 The introduction to the Service Level Agreement [CONFIDENTIAL]-Bureau RMC (file document 39).
142 Report of statement by Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

143 Invoice Aws June 2019, received from [CONFIDENTIAL] on 29 July 2019 (file document 50).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

2.5 Decision to pause WiFi measurements and switch to 'anonymize on the server'

On November 30, 2018, the AP released a news item stating that on the basis of

the AVG companies are only allowed to track people with WiFi tracking in very exceptional cases.144 In response

[CONFIDENTIAL] has sent an e-mail to the director of this within the municipality of Enschede

from Bureau RMC with the following questions:145

“Hai Huib, I called after the message below. Questions to you:

- How do you interpret this statement?

- Do the measurements of CT (red: City Traffic) fall below this?

- If so, is anonymization still an option?

- (…)”

In response to the AP news report, the Municipal Executive of B&W Enschede contacted

Bureau RMC and instructed her to pause the WiFi measurements. This follows from the

letter of 6 December 2018 sent to the municipal council by B&W Enschede:

“(…) the Dutch Data Protection Authority (AP) [has] published an article about WiFi tracking. (…) In the context of

Due to due care, we have chosen to instruct City Traffic to pause the WiFi counts for the time being. In

in the meantime, we are in talks with City Traffic to resolve this in the light of the publication.”146

On December 14, 2018, [CONFIDENTIAL] sent the following email to the director of Bureau RMC

sent: “We are working on a letter to the council that the counts can be resumed from January 1, 2019

because from that moment on, counting is done anonymously. (…) Can you confirm by email that you are

counting anonymously as of 1 January 2019?”147

The director of Bureau RMC replied on December 16, 2018: “(…) We can hereby confirm that we

from January 1, 2019 in addition to pseudonymizing on the sensor, will anonymize on the server. (…)”

As evidence for the actual implementation of this "anonymization on the server" [CONFIDENTIAL] a

screenshot of the change in the server's software code submitted to regulators of the

AP.148 It follows that 'anonymization on the server' was implemented at the end of December 2018, at least

dat [CONFIDENTIAL] of the pseudonymised MAC address (without the colons).

cut off. Appendix 1, pages 38 to 40 describes trimming in more detail.

On December 18, 2018, the municipal council was informed by letter from the Municipal Executive of B&W Enschede

of the fact that the WiFi measurements would be resumed.149 This letter states:

144 www.autoriteitpersoonsgegevens.nl/nl/nieuws/bedrijven-mogen-mensen-only-at-high-exception-with-wifitracking-following.

145 E-mail of 3 December 2018 from [CONFIDENTIAL] to [CONFIDENTIAL] from Bureau RMC, appendix 7 to the letter of 24 May 2019 from

the Municipal Executive of B&W Enschede to the AP (file document 26).

146 Letter of 6 December 2018 to the Council of Enschede pausing wifi counts, appendix 8 to the letter of 24 May 2019 from the Municipal Executive

Enschede to the AP (file document 26).

147 E-mail of 16 December 2018 from RMC anonymize confirmation, appendix 10 to the letter of 24 May 2019 from the Municipal Executive

Enschede to the AP (file document 26).

148 Page 3 of source code, clipping and filters.pdf, attachment 2 of documents received from [CONFIDENTIAL] on 20 June 2019

(file item 46).

149 Letter of 18 December 2018 to Council restarting WiFi counts, appendix 11 to the letter of 24 May 2019 from the Municipal Executive of B&W Enschede to

the AP (file document 26).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

“Until recently, City Traffic worked with pseudonymization of data on the sensor (MAC addresses that are encrypted on the sensor). This is regarded by the AP as personal data and must therefore comply with the General Regulation Data Protection (GDPR). (…) Anonymised data does not constitute personal data. In that case the General Data Protection Regulation not applicable. This is confirmed in the AP's publication of 30 November last in the further explanation of the standards. (…) We can inform you that City Traffic has confirmed to us that they switch to anonymous counting from 1 January 2019. In this way we maintain the privacy of our visitors secure downtown. From January 1, 2019, the sensors will be activated again and we will be able to return monthly report on the counts.”

From the information from the Municipal Executive of B&W Enschede, it follows that Bureau RMC for the period from 10 December 2018 up to and including 3 January 2019 has not reported any figures to the Municipal Executive of B&W Enschede.150

Based on the foregoing, the AP concludes that the Municipal Executive of B&W Enschede, in response to the publication of the AP of 30 November 2018 Bureau RMC has commissioned the WiFi measurements in the city center of Enschede to pause and that over the period from December 10, 2018 to January 3 2019 no figures have been reported by Bureau RMC to the B&W Enschede Board. The AP concludes on this basis that the sensors in the city center of Enschede in the period mentioned have stood. The AP also notes that Bureau RMC (at the request of the Municipal Executive of B&W Enschede) has introduced so-called 'anonymization on the server' as of January 1, 2019, with the last three characters of the pseudonymised MAC addresses are truncated.

150 share peringang.xls in folder 20190212, appendix 14 to a letter dated 24 May 2019 from the Municipal Executive of B&W Enschede to the AP (file document 26).