Confidential/Registered

Municipality of Enschede

College of Mayor and Aldermen

PO Box 20

7500 AA SCALE

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

Contact

[CONFIDENTIAL]

Topic

Decision to impose an administrative fine

Authority for Personal Data

PO Box 93374, 2509 AJ The Hague

Bezuidenhoutseweg 30, 2594 AV The Hague

T 070 8888 500 - F 070 8888 501

authority data.nl

Dear Board of Mayor and Aldermen of the Municipality of Enschede,

The Dutch Data Protection Authority (AP) has decided to inform the Municipal Executive of

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

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

of mobile devices with Wi-Fi turned on in the city center of Enschede. With that,

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

Violated Data Protection Regulation (GDPR).

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

legal framework. In chapter 3, the DPA assesses whether personal data is involved, the processing responsibility and the violation. In chapter 4 the (height of the) administrative fine and Chapter 5 contains the operative part and the remedies clause.

1 Introduction

1.1 Relevant government agency

This decision relates to the college of mayor and aldermen of the municipality of Enschede (hereinafter: the B&W Enschede Board). On July 17, 2018, the AP received a complaint from a complainant with therein the request to impose a corrective measure on the municipality of Enschede. the complainant explained that there are sensors in the city center of Enschede that collect data from people walking by who have turned on the Wi-Fi on their phone. Collecting and processing this data according to the complainant, without justification within the meaning of Article 6, paragraph 1, of the General Regulation data protection (hereinafter: GDPR). The AP then started an investigation into compliance with the GDPR by the college B&W Enschede. During the investigation, the AP received two similar complaints.

1.2 Process

During the investigation, the AP requested information from the Municipal Executive of Enschede and 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 hires in turn to manage the sensors and to process all the data generated with the sensors are collected. In addition, regulators of the AP on May 29, 2019, investigated done on site at a number of shopkeepers in the city center of Enschede where a sensor was installed. the same

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 on the spot and data requisitioned.

In a letter of May 8, 2020, the AP has an intention to enforce to the college B & W Enschede

sent. The AP has also given the opportunity to do so by means of this letter, the Municipal Executive has

Enschede gave its opinion in writing on 14 July 2020 about this intention and the follow-up to it

underlying report. The AP subsequently requested further information on 14 January 2021 about

this view.

2. Legal framework

2.1 Scope GDPR

Pursuant to Article 2(1) of the GDPR, this Regulation applies to all or part of

automated processing, as well as to the processing of personal data that are in a file

included or intended to be included therein.

Pursuant to Article 4 of the GDPR, for the purposes of this Regulation:

1. “Personal data”: any information about 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” means 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

processing of personal data; when the objectives and resources for this

processing is established 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 provides, among other things, that personal data must be:

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

Article 6(1) of the GDPR then provides an exhaustive list of the grounds for a

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

insofar as at least one of the six principles mentioned is 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 of a task in

in the context of the exercise of official authority vested in the controller

dedicated;

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

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

fundamental freedoms of the data subject that require the protection of personal data, more important

outweigh those interests, especially when the data subject is a child.

3. Review

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 dealing responsibly with

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

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 WiFi measurements are

not necessary for

performance of an agreement 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

In view of the extensive investigation in this case, the AP refers to the first chapter for the facts

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

comes to a judgment.

The Municipal Executive of Enschede has made the decision to start with 24/7 as of September 6, 2017.

measurements via sensors in the city center of Enschede. The college B&W 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 at least since 25 May 2018.

various shopkeepers in the city center of Enschede. Each sensor has a range of up to 20 to 30 meters. The

As of this date, all mobile devices in range that have 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 was located plus two minutes. The AP also notes that the sensors are continuously scanning. Furthermore,

the AP determined that every device detected on entry and two minutes after exit 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.

One and the same pseudonymization method is running 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 leading to one and the same pseudonymised MAC address.

The data measured in one day by the sensors in the city center of Enschede are collected daily in a short-term table. The time of day when the device passed through the sensor scanned is hereby recorded accurately to the second. In the period up to January 1, 2019 it is pseudonymised MAC address not truncated when entering the server, in the period from January 1 2019 does. The clipping involves removing [CONFIDENTIAL]. The other data that is sent to the server, namely sensor ID, date, time, signal strength, status and spoofed indicator are taken over in the short-term table unedited.

Two filters were applied to the short-term table each night, namely an opt-out filter and a resident filter. These filters result in certain records from the short-term table not being appear in the long-term table. The AP has found that the resident filter does not include all residents filters out and that incorrect information is provided on the municipality's website.

After applying the filters to the short-term table, two consecutive records of the same (truncated) pseudonymised MAC address to one record in the long-term table. From May 25, 2018 to as of 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, SignalStrengthOut. Has passed on January 1, 2019 on the clipping of the pseudonymised MAC address and the pseudonymised MAC address became data 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 B&W Enschede college 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 college B&W Enschede has instructed Bureau RMC to transfer data as of May 1. 2020 to turn off the sensors. The sensors will no longer provide counting data from 1 May 2020.3

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

The AP has subsequently established that from the long-term table after January 1, 2019 it is clear: living patterns can be distilled. Given the regularity of the patterns, it is reasonable to concluded that the records associated with the pattern belong to one mobile device. The living patterns can, for example, reveal someone's home or workplace, but also more sensitive data such as visits to medical institutions.

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

3.1.3 Assessment

During the processing (from detection by a sensor to storage in the long-term table) there are distinguish 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 truncation of pseudonymised MAC addresses (May 25, 2019 – January 1, 2019) and the period after the implementation of this

cut (January 1, 2019 – April 30, 2020).

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

4 In the period from December 10, 2018 to January 3, 2019, the Municipal Executive of Enschede paused the WiFi measurements. earlier

collected data during this period was stored in the long-term table, so data was passed through 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

any sensor

Shipping to en

reception on the

server

Short-term table on

the server

MAC address; signal strength; Date;

Time of day

Pseudonymized MAC address;

signal strength; Date; Time of day; Sensor-

ID; status; Spoofed indicator

Pseudonymized MAC address;

signal strength; Date; Time of day; Sensor-

ID; status; Spoofed indicator

Long-term table on

the server

ID; Pseudonymized MAC address;

signal strengthIN; Signal strengthOFF,

Date; timeIN; timeOFF;

residence time; Sensor ID; BWCode

Same as prior to January 1

2019

Same as prior to January 1

2019

Clipped pseudonymised MAC

address; signal strength; Date;

Time of day; Sensor ID; status; Spoofed

indicator

ID; Clipped pseudonymized

MAC address; signal strengthIN;

Signal strengthOFF, Date;

timeIN; timeOFF; residence time;

Sensor ID; BWCode

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

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

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

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

location data. In this context, the AP therefore refers to 'location data'.5

Two hatches have also been applied in the table above, 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

data qualify 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 provides that data qualify as personal data if

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

5 On location data from mobile devices, European data protection supervisors have already identified in 2011

that they 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 have their mobile devices close to them

such as in a trouser or jacket pocket, in a bag or on the nightstand next to the bed. (…) It is rare that someone has such a

lend the device to someone else. (…) Thus, from a pattern of inactivity at night, the sleeping place can be inferred and from a

regular morning travel pattern the employer's location.”

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

information about an 'identified person' is not possible in the present situation because the identity

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

address and location information.

In order 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

by means of identifiers or characteristic elements. Possible identifiers in present

situation: 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 highly 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 conversion of a MAC address

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

provided that the underlying MAC address has not been spoofed – an identifier of a natural person can

be.7

With regard to the location data, it is explicitly mentioned in Article 4, part 1, of the GDPR as:

possible identifier of a natural person as 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. Hereafter the AP describes per phase in the

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

natural person to whom the data relates.

Way 1: Identification of persons from the data stored on the sensor

During the investigation, the AP determined that the MAC address and location data are temporarily stored

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

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

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

[CONFIDENTIAL] So the exact location of the sensors is known and access to the

working memory and the software running 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 on-site

or detect via a camera which person comes within range of the sensor. especially on

6 Spoofing in this context is an informal term for “MAC Address Randomization”, a technique by which part of the MAC address

address sometimes changes randomly for the purpose of tracking a device by reducing time and space.

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

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

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

quiet moments in the inner city, this leads directly to identification of the natural person. To check 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 also on the moment of detection on site 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 1 January 2019)

This way describes that on the basis of the data in the short-term table it is also possible to identify natural persons. [CONFIDENTIAL] takes care of the collection and validation of the data. The short-term table therefore rests with [CONFIDENTIAL]. From mobile devices that use the range of a sensor, data associated with '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 within range of a particular 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 available for a longer period of time, then is it known to [CONFIDENTIAL] that the relevant resident or shop employee is still

within range of the sensor. Someone from [CONFIDENTIAL] can then be on site
identify the person and identify the person.

Way 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
long-term table possible to identify natural persons. The AP has established that in the
long-term table from after 1 January 2019, i.e. after the introduction of cutting, lifestyle and exercise pattern
can be recognized.9 This will also be the case in the long-term table from before January 1, 2019, when there was 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 relevant natural person is located somewhere, for example the person who
moves between sensors in the city center of Enschede every night between 04:00 and 05:00. During the night
there are hardly any other people on the street and it is therefore possible for [CONFIDENTIAL] to
to identify this person on site or via a camera.

In the above three examples of ways of identifying natural persons by
[CONFIDENTIAL] takes into account recital (26) of the GDPR which states that taking into account
should be taken by "all means reasonably foreseeable"
used by the controller or by another person to identify the natural person
directly or indirectly identified. The AP concludes that the above three ways of identifying
natural persons, in view of the time, costs and manpower required, no excessive effort of
[CONFIDENTIAL] require. The criteria in Breyer v Germany10 are also met, because the
manners are neither prohibited by law nor impracticable in practice. That employees of

9 See also appendix 1, paragraph 1.2, page 46 and further.

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

Date

March 11, 2021

[CONFIDENTIAL] do not use these resources in practice to target people in the inner city of

Identifying Enschede does not alter the fact that they could reasonably do so.

In addition to identification by [CONFIDENTIAL], the AP notes that the identification is also made by employees

can be done by Bureau RMC. The AP has established that Bureau RMC on the basis of the

service level agreement with [CONFIDENTIAL] has access to all data that [CONFIDENTIAL]

collected. In addition, the AP notes that even the Municipal Executive of Enschede can do the identification,

because it also has access to all data on the basis of the processing agreement with Bureau RMC.

Possibly, 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 an investigation of a company that provided Wi-Fi tracking found12 that it

registering 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 supervisors stated in their opinion on apps on smart devices that

location data and unique identifiers of mobile devices are personal data.14 In their opinion

They stated about the proposed e-Privacy Regulation: '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-term 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 tested against the definition of personal data in Article 1 under a of the Personal Data Protection Act: ‘every data concerning an identified or identifiable natural person”. The current definition of personal data in the AVG is identical.

13 Section 5.1 of the report final findings 'Wi-Fi tracking of mobile devices in and around stores by Bluetrace' (z2014-00944) dated 13 October 2015. Can be found at www.autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-wifi-tracking-rond-winkels-schijn-met-the law. At the time, the AP also informed the VNG by letter about its positions 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 through the AP 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 log). 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 provides an explanation of 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 the pseudonymised MAC address.

Dark gray areas: Clipping the pseudonymised MAC address does not eliminate all three risks traceability, linkability and deducibility, so that it is still personal data in 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 City Traffic infographic 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 does not adequately address the risks of traceability, linkability and deducibility and that the data qualify as personal data. The AP explains this below.

Linkability

The risk of linkability is present if there is the possibility to have at least two records relating the same data subject or group of data subjects (in the same database or in two different databases).

The AP notes 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 truncated
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 pseudonymised MAC address to serve as the basis for grades for college B&W
Enschede about unique visitors to the city center of Enschede. The AP also points 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 that pairing is still possible.
It follows from the foregoing that the chosen anonymization technique does not exclude the risk of linkability.
Since it is required that all three risks are excluded, the conclusion can already be drawn
that the anonymization technique fails and that re-identification of natural persons is possible. For the
For completeness, the AP also covers the other two risks.
16 See appendix 1, paragraph 1.2, figure 2.
17 See Appendix 1, Section 1.2, page 44.

Date
March 11, 2021
Our reference
[CONFIDENTIAL]
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 one
patterns are associated with one truncated pseudonymised MAC address, meaning it is possible
is that the patterns contain the location data of multiple mobile phones. However, given the
regularity of the patterns it can reasonably be concluded that all records belonging to
to the pattern come from a single mobile device, and thus one natural person.

This makes it possible to individualize a person. The AP therefore concludes that the risk of traceability is not excluded.

deducibility

A risk of inducibility is present if there is a possibility to measure the value of a personal characteristic is most likely to be derived from the values of a series of other attributes. From the three visualizations of the long-term table18, it is likely that a value of a personal characteristic can be derived, for example the sleeping place or the location of the employer. The AP therefore concludes that clipping the pseudonymised MAC address also does not exclude the risk of inducibility.

On the basis of the foregoing, the AP concludes that the short-term and long-term table are insufficiently resistant to re-identification.

In addition, the AP concludes that the combination of the truncated 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 in case of truncated pseudonymised MAC addresses. Method 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 belonging to the truncated pseudonymised MAC address is still within range of the sensor.

Someone from [CONFIDENTIAL] can then determine on the spot who 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 Municipal Executive of Enschede and response from the AP

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

Operation and storage sensors

According to the board of B&W Enschede of Bureau RMC/[CONFIDENTIAL], 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, paragraph 1.2, page 46 and further.

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

device emissions within the sensor area. The sensor receives a 'packet' of data including the
MAC address of the device and the WiFi strength. According to the Municipal Executive, no (other) to
the personally identifiable information is registered. Also no longitude, latitude or address data are sent
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. The AP indicates in its investigation that there are
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 this 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
could find out a MAC address. No MAC addresses are stored 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 alter the fact that in this case the sensors are “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 range right across the street. The AP also notes that for the determination of the location
no GPS data is needed. After all, the location of the sensor is known to [CONFIDENTIAL] and the

sensor ID is sent to the server. That this data is in another database means

not that [CONFIDENTIAL] doesn't have access to it.

The Board of B&W Enschede also states that access is not possible to the MAC addresses on

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 receiving module and keeps track of MAC addresses as they become

receive. The working memory of this module therefore contains all MAC addresses that are also within the

have been received by the sensor in the past two minutes. 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 Hashen is the conversion of a series of numbers and/or letters into another unique series by means of an algorithm.

20 Report of statement of 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 natural persons

Furthermore, the Board 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 Municipal Executive of 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 college of B&W Enschede wants emphasize that there could only be direct or indirect identifiability if there is is of (link with) additional data.

In its report, the AP assumes too quickly in the eyes of the Board of B&W Enschede that this is the case 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. A MAC address is according to WP29, personal data is only considered 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 The fact that could possibly play a role in this regard is (rough) location data. This location data is, however, in this case too imprecise to identify an individual in conjunction with a MAC address can identify.

In addition, the Municipal Executive of Enschede takes the position that the criteria from have not been met the Breyer v Germany judgment in order to be able to speak of personal data. The MAC addresses are namely not saved, but hashed directly on the sensor after which the original MAC address is deleted. It is therefore not possible to get to 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 effect location information. The Sensor ID is nothing 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 comes into view for the first time when sending the hashed MAC addresses from the sensor to the server. Due to the separate storage, linking of the Sensor ID with the MAC address only takes place later in the counting process. From that at the moment, however, the MAC address is no longer available. The MAC address is sent when it is sent after all, hashed to the server, and then truncate. Identification, also on the basis of a so-called location data, can therefore not take place according to the Municipal Executive of Enschede.

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

wrong emphasis on the fact that the MAC addresses are transformed and not standalone for

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

as personal data.

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

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

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

MAC address is therefore irrelevant. The point here for the AP is that the pseudonymous identifier can be traced over time

little has changed.

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

The possibility of deduction (and ultimately identification) is a result of design decisions in the

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

to track individuals. At that time they are only displayed as numbers. But this is

same number for six months. In this case one cannot speak of robust

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

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

time and location become a factor. And as has already been mentioned by the AP, the exact location is

of the sensors known to [CONFIDENTIAL] where the range of the sensors is adjusted to the

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

B&W Enschede underestimates the sensitive nature of location data, which were always kept for six months.

Lifestyles

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 is of the opinion that

traceability to an individual on the basis of a lifestyle is not possible in this case.

In the eyes of the B&W Enschede Board, it can be assumed that a certain pattern develops

also in the future will never be the basis of a real, indirect, identification. Profiling is

after all, only possible if several counts of a pseudonym are collected. To the

municipality understood, in this case most counts are done on the basis of one-off counts. Such

applies to approximately 70% of the counts.

In addition, there may theoretically be overlap in the living patterns that the AP believes it can abstract

of multiple devices, due to the truncation of the hashed values. It's not on

pre-exclude that two or more hashed, and then truncate, data has the same value

to get. Furthermore, it is not only individuals who have devices with a MAC address with them, but that

various other devices such as pin machines, smart TVs and printers may also be located in the area.

This only possible method of identification that the AP outlines is identification by an employee of

Bureau RMC/ [CONFIDENTIAL] on site or via remote camera images. This one

The possibility of identification is, according to the B&W Enschede Commission, unworkable or, even worse: impossible. The

inappropriateness of a request, i.e. asking a person what MAC address he/she has, is no more

than a theoretical one. In addition, Bureau RMC/[CONFIDENTIAL] does not have a MAC address at all

has at its disposal to verify that MAC address. After all, the MAC address is

college B&W Enschede was immediately hashed and later anonymized. In addition, the MAC address is not

recorded in a list or, for example, a database, so that identification and control afterwards does 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 investigation report, according to the college

B&W Enschede will not take place due to the delay that occurs in the counting system and because

Date

March 11, 2021

the search area is too large. The AP must also be aware that there is a lot of pressure on
moments hundreds, if not thousands, of people can be in the sensor area.
Incidentally, the municipality of Enschede, contrary to the opinion of the AP, has no possibility at all to
to collect any data that can be traced back to individuals at Bureau RMC/[CONFIDENTIAL]. The
any contractual possibility, according to the B&W Enschede Commission, is insufficient to assume that
the municipality actually had and has access to the data referred to.
The AP largely does not follow the view of the Municipal Executive of Enschede. As mentioned before
the AP considers the applied anonymization techniques insufficient, so that it was possible to
to be able to track individuals when storing the unchanged identifiers for a long time. The
AP agrees with the fact that in 70% of the cases the counts are done on the basis of one-off
counts. However, that does not detract from the fact that the B&W Enschede council 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 some devices such as printers in the city,
it seems unimaginable to the AP that these are visible in multiple locations because they are located throughout the city
to move. The resident filter makes an attempt to filter out these types of devices.
The AP also maintains its position that identification of natural persons is possible on the three
ways described in section 3.1.3. In doing so, the AP has taken into account all means of which
can reasonably be expected to be used by the controller or by
another person to directly or indirectly identify the natural person, for example
selection techniques.24 The combination (pseudonymous identifier + datetime + location) makes it possible
to identify someone. It is not without reason that Article 4, part 1, of the GDPR
location data as an identifier.25 After someone has been identified, one can check that person
ask for his MAC address. The AP has mentioned this control question as an example. However, there are many
ways to verify the identity of persons.

If Bureau RMC/[CONFIDENTIAL] had properly carried out all the technical measures referred to

then there would be no tracking. The step to actually identify therefore requires

other disproportionate effort according to the AP. And in some cases – the nocturnal

walker for example - identification requires only a very limited effort. From the collected data

to trace his living patterns, so that you can find out someone's place of residence or workplace. 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 enabling the data subject to be identified is

rests with one and the same person.26 It is important here that the Enschede Municipal Executive is lawful

has access to all means that can be used to contact a natural person directly or indirectly

24 Recital 26 GDPR.

25 For more in-depth information, see https://www.nature.com/articles/srep01376

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

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

identify. That the Municipal Executive of Enschede has contractually agreed to be able to collect data

request from Bureau RMC and [CONFIDENTIAL], gives the Board pre-eminently lawful access to

the personal data. The fact that the B&W Enschede college does not (want to) make use of this is legal

irrelevant.

3.2 Controller

3.2.1 Introduction

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

first paragraph, opening words and under a jo. Article 6(1) of the GDPR is also important to determine who to

trademarks is the controller as referred to in Article 4(7) of the GDPR. In addition,

determines who determines the purpose and means of the processing of personal data.

3.2.2 Facts

In view of the extensive investigation in this case, the AP refers to the second chapter for the facts

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

judgment comes.

The B&W Enschede college has decided to start 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

office RMC. In addition, the municipality of Enschede has both a press release and a number of information 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 inner city of Enschede with a view to dealing responsibly with public funds. In addition

the municipality points out that the measurements can provide insight into topics that are important

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

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

of shops and catering establishments and determining whether and when action must be taken in the context of order and

safety.

On September 26, 2017, the Municipal Executive of Enschede and the predecessor of Bureau RMC

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

this agreement provides that the Municipal Executive of Enschede is the controller for the

processing of personal data. It has also been determined that the processor, Bureau RMC, processes the data

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

the Municipal Executive of 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

submitted to the Municipal Executive of Enschede with regard to the processor agreement. Desk

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

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

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

The Municipal Executive of Enschede has had a guiding role in the number and locations of the sensors that

be used for the WiFi measurements. In addition, the Municipal Executive of Enschede has, in response to the

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

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

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

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

Finally, on April 30, 2020, Enschede has instructed Bureau RMC to provide data as of May 1, 2020

to turn off sensors.

3.2.3 Assessment

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

natural or legal person, public authority, agency or other body which, solely

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

in this case, the processing of the mobile device's MAC address, time (in seconds) and

the date of detection by the sensor and the sensor ID. It is not required that the

controller has the personal data in its possession.27

The AP is of the opinion that the Municipal Executive of Enschede is the controller 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 for the processing. She justifies this as follows.

The person who determines the purpose of the processing of the personal data is the person who determines why the

processing takes place. As discussed in section 3.2.2, the Municipal Executive of Enschede was the one
who has decided to carry out WiFi measurements. In addition, the data is processed for a
the Municipal Executive of Enschede for a specific purpose, namely measuring the effects of municipal
investments in the city center of Enschede. The other purposes that the B&W Enschede college in
cites her point of view for the WiFi measurements (for example, measuring the effects of
road works, city center promotion and Sunday shopping) have also been determined by the college and are
moreover based on the Municipalities Act.28 Furthermore, the Municipal Executive of Enschede on 30 November 2018
Have Bureau RMC temporarily pause processing and have the sensors switched off on 1 May 2020. It
B&W Enschede board was also the one who determined with its board decision that there
personal data are processed, and the person who can therefore decide to stop doing so. With that
the Municipal Executive of Enschede has control over whether or not the personal data is processed. The
AP concludes that the B&W Enschede Commission has not yet determined 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 The Municipal Executive of Enschede argues in its view that the measurements also provide insight into the effects of road works,
the holding of Sunday shopping and market days, inner-city promotion, the attractiveness of events, the acquisition of
shops and catering establishments and determining whether and when action must be taken in the context of order and safety.

The person who decides how the processing takes place must be regarded as the person who provides the means
determines. As discussed in section 3.2.2, the Municipal Executive of Enschede has decided to

processing personal data using a service provider, namely Bureau RMC. The
technical elaboration of the processing of the personal data has been delegated to Bureau RMC,
whereby the Municipal Executive of Enschede, on the basis of the processor agreement, did have the option to
to give instructions. The Municipal Executive of Enschede has also exerted influence on 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 B&W Enschede Commission must determine by whom the processing is carried out
would be carried out and also the way in which the processing takes place, for example by the number of
sensors and their locations, has partly determined how the processing of personal data
took place.
On the basis of the above, the AP concludes that the B&W Enschede Commission both achieves the goal and partly
has determined the means for the processing and thus qualifies as
controller within the meaning of Article 4, preamble and section 7, of the GDPR for the
processing of personal data via sensors in the city center of Enschede.
3.2.4 View of the Municipal Executive of Enschede and response from the AP
In its view, the Municipal Executive argues that it is not a controller within the meaning of the
AVG is. In doing so, it makes a distinction between its responsibility as a client, which it does 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, there are
according to its factual circumstances which indicate that they do not, 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) storage period determined by
Office RMC. The B&W Enschede Board 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
Enschede states that it does not prescribe the frameworks and/or conditions within which the data is collected
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 this.

Below, it will first be explained why the AP is of the opinion that the Municipal Executive of Enschede does

is the controller. The AP will then discuss why there is no

joint processing responsibility.

Processing Responsibility

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

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

has in the way of processing, the College B&W Enschede is the one that has chosen to

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

would be placed and where they would be placed. With this, the municipality has (also) determined

which means are used for the processing.

The fact that the municipality would not have access to the data that Bureau RMC processes 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 that all information used by the

the person concerned can be identified, is owned by one and the same person.29

The Municipal Executive of Enschede further points out that Bureau RMC can determine the data to a third party

lot to sell. The AP makes a distinction between different processing operations. First of all,

there is the processing of personal data by Bureau RMC for the purpose of the Board of B&W

Enschede, namely measuring the effects of municipal investment in the city centre. This is the

processing that is the subject of the investigation and what the DPA is responsible for as the controller

qualifies. This responsibility is limited to the processing operations for which the Board of Directors has
Enschede determines the goal and partly the means. In addition, there is the possible processing whereby Bureau
RMC can give other parties access to the information that it also uses to provide the
data to the Municipal Executive of Enschede. Bureau RMC may have these because in the
processor agreement it has been determined that Bureau RMC is entitled to an auction file (stripped of
personal data), a copy of the data that can be used by anyone who makes an application
about, for example, crowds in a certain place in the city center of Enschede. In the second situation, there is
there is a processing that falls outside the purposes of the Enschede Municipal Executive, and therefore also
beyond its responsibility as a controller. That the B&W Enschede college
this other, second processing operation is not a controller does not affect the conclusion that
the Municipal Executive of Enschede is still the one who determines the purpose and partly the for the first processing
resources and therefore qualifies as a controller.
The Municipal Executive of Enschede further argues that it does not prescribe the frameworks and/or conditions
in which the data is processed. The AP does not follow this argument. In the processor agreement,
determined Bureau RMC will follow all reasonable instructions of the Municipal Executive of Enschede. Desk
RMC has already done this by ceasing processing twice at the request of the Municipal Executive. The
The AP concludes from this that the Commission, if desired, does specify the frameworks and/or conditions within which the
data can be processed. That the municipality has not always used this
possibility, or does not intend to, does not alter 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
Board of B&W Enschede laid down in the processing agreement concluded between them that it is precisely the Board
B&W Enschede is the controller. Now that the processor agreement between the parties

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

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

agreement is concluded, in contrast to the privacy protocol of Bureau RMC, connection must be
are 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 factual situation deviates from a “paper” reality, such as the privacy protocol, is the factual
leading the situation.

Joint Processing Responsibility

The Board of B&W argues that if the AP is of the opinion that the Board
controller is that there is only a joint
processing responsibility. The AP does not follow this argument and justifies it as follows.

Article 26 of the GDPR provides that when two or more controllers jointly
determine the purposes and means of the processing, they are joint controllers.

Article 4, preamble and section 7, of the GDPR also provides that the controller
is the person who, alone or jointly with others, determines the purposes and means of the processing. In both
Articles stipulate that the (joint) controller determines the purpose and means for the
processing determines. It appears from the factual circumstances cited by the Enschede Board of B&W:
that Bureau RMC has a degree of influence on the means of processing. However, it has not been shown
that Bureau RMC determines the purposes for the processing of personal data for the Municipal Executive
Enschede. Now that Bureau RMC has not determined the purposes for the processing, it cannot
be a controller. As a result, there can also be no joint
processing responsibility. That Bureau RMC partly influences the determination of the means

this does not change for the processing, because the (joint) controller has the 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 of Enschede de

is the controller for the processing in the context of the WiFi measurements. The AP will be in the

the following assess whether the Municipal Executive of Enschede can make a successful appeal for this processing

on one of the grounds from Article 6 of the GDPR.

3.3.2 Assessment and response to opinion

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

processed in a manner that is lawful with regard to the data subject. Trading in

accordance with this principle of legality, if there is a sound legal basis for the

processing is present.

Article 6(1) of the GDPR then provides an exhaustive list of the grounds for a

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

insofar as at least one of the six principles mentioned is 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 or public interest duties

Article 6(3) of the GDPR provides 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 defined in Union law or
Member State law, or is necessary for the fulfillment of the legal basis e)
a task carried out in the public interest or for the exercise of public authority vested in the
controller has been granted.
Recital 45 of the GDPR states: “This Regulation does not require that for each individual processing
specific legislation is required. It will suffice to have legislation that serves as the basis for various
processing based on a legal obligation to which the controller is responsible, or for processing that
is necessary for the performance of a task in the public interest or for a task in the exercise of
of public authority. (...)”
Recital 41 of the GDPR states that the legislation on the basis of which the processing takes place
should be sufficiently clear, precise and predictable: “This legal basis or legislative measure must
however, be clear and accurate, and their application must be 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 parties involved in the
processing of the personal data of the persons concerned should not be disproportionate in relation to the
purpose to be served by the processing. Under the principle of subsidiarity, the purpose for which the
personal data are provided in reasonableness not in another, for the processing of
personal data concerned, can be achieved in a less detrimental way.
In its view, the B&W Enschede Commission states that the processing operations in the context of WiFi counts
may be based on Article 6(1)(e) of the GDPR. According to the college, the AP misunderstands that the
Municipality of Enschede has a very broad task. It follows from the Municipalities Act that the municipality is responsible for the
'daily'

administration of the municipality. According to the Commission, this task is not simply formulated in broad terms,
but for a well thought out reason. In the eyes of the municipality, its responsibilities, and
in line with this, the need to perform the WiFi counts to meet those different
responsibilities, from various (formal and material) laws and regulations and documents.
30 In the present situation, the data subjects have not been asked for permission (ground a), the WiFi measurements are not
necessary for
performance of an agreement 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 for this 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, Vision
bustling city center and the mobility vision, the APV of Enschede, the assessment framework
event permits, the further rules for terraces, the municipal budget and the
subsidy regulation.
According to the Municipal Executive of Enschede, pedestrian counts can provide insight into various
aspects that are important for municipalities to be able to base its policy on various levels and
therefore to give substance to the 'public task' that it has towards its residents as a municipality. This one
According to the Commission, information is only really valuable if it is “continuous” information, that is, not
only information based on incidental events. In the eyes of the municipality, the
The chosen method of counting is more privacy-friendly than, for example, manual counting. manual
counting has many drawbacks: double counting cannot be avoided, so manual
counts are not a reliable picture. Moreover, this is very labour-intensive and therefore expensive. In the last

After all, the counter sees by definition which person is where. Other alternatives to
counts other than via WiFi are actually not available. There are infrared counts, but these too
method does not extract double counts 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 in this regard. At the start of the passer-by counts, the B&W Enschede college was alive
still assuming – on the basis of information that the College 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 board decision to switch to visitor counts
over Wi-Fi. According to the B&W Enschede Commission, this explains why in the Commission's view there are sometimes
about visitor flows. After the start of the visitor counts and the first results of
the counting data (around the beginning of 2018), however, it turned out that the Municipal Executive could not see any flows,
but that it was busy per
sensor point. The B&W Enschede board has therefore declared only the number of passers-by at a certain
point and moment needed.31
The AP does not follow the view of the Board of B&W Enschede and arrives at the following assessment.
First of all, the AP notes that the Municipal Executive of Enschede has no legal obligation,
laid down in Union or national law, to have the Wi-Fi measurements performed in the inner city. Also
does not find the processing of personal data to be based on a more broadly formulated duty of care or legal
obligation. The AP therefore first establishes that the B&W Enschede Board cannot successfully appeal
do on the basis of Article 6(1)(c) of the GDPR.
The AP then investigates whether the WiFi measurements could be processing that is necessary for
a task of general interest. The AP has already concluded that the WiFi measurements are processing in
within the framework of municipal government tasks. Government tasks are tasks of general interest. That's how it is
the Municipal Executive of Enschede, pursuant to Article 160 of the Municipalities Act, is empowered to ‘execute the
day-to-day management of the

to conduct the congregation." This concerns a task of general interest, where, for example, keeping the finances of the municipality, spatial planning and urban development can be under grouped.

The AP notes that Recital 45 of the GDPR states that not for every individual processing specific legislation is needed. In the present case, this means that the various processing operations determined based on a single legal provision. Recital 41 of the GDPR required however, a certain degree of concreteness of the legislation. This consideration states that the legislation, in this case the public interest task, must be clear, precise and predictable.32 This foreseeability requirement entails, among other things, that the (legal) consequences of certain actions must be foreseeable to the citizen to a certain extent.

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»). interference must be based on a duly published legal provision from which the citizen can determine with sufficient precision which data relating to his private life with a view to on the fulfillment of a particular government task can be collected and recorded, and under which conditions that data can be edited, stored and used for that purpose. So required is a sufficiently precise legal basis. This means that, for example, the general task of a public service cannot serve as a legal basis for data processing in all cases.33 It means also that an obligation for a public authority to provide data while that government agency has a legally regulated duty of confidentiality, expressly and clearly in a

must be laid down by law, and that it is not permissible for such an obligation
is solely inferred from the history of formation or the relationship between legal
provisions or is assumed due to the effectiveness of a statutory regulation.34
The AP comes to the conclusion that the legal task of 'leading the day-to-day management of the municipality' is not in place
above requirements, because this task is formulated too broadly, is not concrete and therefore not
is sufficiently predictable.35 A citizen cannot determine sufficiently from Article 160 of the Municipalities Act which
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
be edited, stored and used. The AP is aware that the legislator Article 160
Municipalities Act has deliberately broadly formulated. This alone has the consequence that this
formulated job description (because of the effectiveness of a statutory regulation) not without
more 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 February 3, 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
elaborate tasks
because 'such a list is almost by definition doomed to be inconclusive'. Parliamentary Papers II 2000/01, 27 751, no. 3, p. 61.

The Municipal Executive of Enschede further refers in its view to various articles in the
Municipalities Act, the APV and several documents. The AP notes that only Article 160 of the Municipalities Act
jurisdiction of the Municipal Executive of Enschede. The other articles concern powers of other

bodies of the municipality. The Municipal Executive has been designated by the AP as
controller, as a result of which the other articles of law do not apply for that reason
may be as Member State law in which the public interest task is assigned to the controller
assigned is arranged.
The AP has also gone through the entire APV of Enschede, but the AP did not come here with any articles
against which a citizen can deduce that the personal data referred to in paragraph 3.1 can be
are processed for government tasks and under what conditions that data can be used for that purpose
be edited, stored and used. The other documents cited by the Municipal Executive
Finally, Enschede cannot be a legal basis for the processing of personal data because this
are not legal requirements.
The AP therefore establishes that the Municipal Executive of Enschede cannot in this case successfully invoke the
basis in Article 6(1)(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 must
however, formulated more concretely for this situation and thus be sufficiently predictable.
Superfluously, the AP also maintains its position that in the present situation the requirements have not been met either
necessity requirement 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 are
sensors are captured and processed is disproportionate to the processing to be served
goal, namely to test the effectiveness of investments in the city center of Enschede. In this
assessment, the AP takes into account that the right to protection of the privacy of
weighs heavily on citizens in the public space, given the reasonable expectation of the public to act as
passer-by cannot be followed unnoticed and the fact that data is systematic and
were recorded for a longer period of time. Especially for residents and frequent visitors to the municipality
Enschede, the present processing of personal data is an extra major breach of protection
of private life. That the B&W Enschede Board did not aim to collect personal data
processing does not alter the fact that personal data is under the responsibility of the college

were processed. This detracts from the citizen's sense of being unnoticed in public

delusions and to have faith in government.

In addition, the principle of subsidiarity is also not met because the objectives pursued by the

College B&W Enschede can be served in a different, less far-reaching way. Even on

ways that do not process personal data. The B&W Enschede college has, whether it

intended or unintentional, have personal data processed under his responsibility with which

it was possible to track civilians. However, the Municipal Executive of Enschede has stated that it is not

needs visitor flows but only the crowds per sensor point. As a result, the processing of

personal data under the responsibility of the Municipal Executive of Enschede between 25 May 2018 to

and with April 30, 2020 not necessary and also excessive. In addition to the fact that in the

Insufficient technical measures have been taken in the database used, the personal data

also unnecessarily (apart from the raw data) always kept for half a year.

There are sufficient methods to measure the crowds at a certain place where the protection of

personal data is better protected. For example, one can gain insight into crowds by:

market surveys. But also people count via an automatic visitor counter that uses an infrared beam

broadcasting is pre-eminently an effective technique. This technique is also affordable and gives the opportunity to

to provide the continuous information that the Municipal Executive of Enschede needs. Double counting is possible

can be filtered out with statistical calculations. Knows almost every methodology or technique used

measurement errors and requires calibration, often also at the level of individual sensors. This allows one to

correct any measurement errors in the counts. In addition, a small measurement error, insofar as this

calibration would still exist, given that one eventually totals and groups numbers, not

insurmountable.

3.3.2.2. Legitimate interest

The first paragraph of Article 6 of the GDPR provides that ground (f) legitimate interest does not apply to the processing by public authorities in the performance 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 ground should not apply to the processing by public authorities in the performance of their duties.”

Public authorities will not be able to use the basis in the performance of their duties 'legitimate interest', but will have to make use of other bases. This does not apply to insofar as the government agency carries out 'typically commercial acts' in which 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 scope of the task, there may be a basis can 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 provides that basis f) does not apply to 'processing by' public authorities in the performance of their duties'. This does not apply to the extent that the government agency carries out 'typically commercial acts'. The AP has already established that the purpose of the wifi measurements to test the effectiveness of municipal investments in the city center of Enschede, with a view to the responsible handling of public funds. the AP concludes from this that the WiFi measurements are processing in the context of the municipal government duties. The AP therefore finds that the Municipal Executive of Enschede cannot invoke the legitimate interest within the meaning of Article 6(1)(f) of the GDPR. It's up to the legislator to provide the legal basis for personal data processing for such cases create government agencies.

In its view, however, the Municipal Executive of 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 Enschede, the entrepreneurs, investors, visitors and residents. The AP has according to the B&W Enschede Commission, recognized in the Bluetrace case that there may be a legitimate interest in collecting such information.36

Furthermore, the B&W Enschede Commission states that the processing in the context of WiFi counts is met the necessity requirement. This is because the WiFi counts are necessary to described interests that are pursued. It is not possible to store this information on a less invasive way. With WiFi counts, according to the college B&W Enschede much more sustainable, efficient and reliable results are collected. Here comes according to the B&W Enschede board, Bureau RMC has taken all kinds of measures that involve entail compliance with the requirement of proportionality and subsidiarity. As before in In this view, the Municipal Executive of Enschede has always relied on the expertise of Bureau RMC as a professional contractor. Furthermore, the municipality of Enschede will inform everyone who enter the city center of Enschede, actively using warning signs about the WiFi counts. The stakeholders are also informed about this via the website of the municipality of Enschede.

Finally, the B&W Enschede Commission 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 the AP followed directions provided. In that regard, Bureau RMC was able - partly because the AP subsequently has not been heard from again – assuming that its working method is in accordance with the privacy laws and regulations and, moreover, has been approved by the AP.

The AP does not follow the view of the Municipal Executive of Enschede and maintains its position that it is College B&W Enschede cannot successfully invoke the basis of legitimate interest. It

After all, the B&W Enschede Board has explained in detail that the processing operations in the context of WiFi counts are necessary for municipal government tasks and not for 'typical business' actions'. The fact that the B&W Enschede Board itself has its statutory duties above referred underlines this assessment all the more. As a result, the AP does not have access to a balancing 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, which means that the comparison by the college B&W Enschede does not apply.

Finally, the AP notes that it has indeed closed the investigation into Bureau RMC with a formal letter. In this letter, the AP has expressly 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 As a result, Bureau RMC could assume that its working method is in accordance with the privacy legislation. and regulations and, moreover, has been approved by the AP, the AP therefore considers it incorrect.

36 CBP, Wifi tracking of mobile devices in and around stores by Bluetrace, z2014-00944, October 13, 2015, https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapport_db_bluetrace.pdf, p. 40.

4. Fine

4.1 Introduction

The Municipal Executive of Enschede has acted contrary to article from 25 May 2018 to 30 April 2020 inclusive 5, first paragraph, under a, jo. Article 6(1) of the GDPR by personal data of owners/users of mobile devices with Wi-Fi turned on in the city center of Enschede unlawfully process.

For the established violation, the AP makes use of its authority to inform the municipal executive

Enschede to impose a fine. To this end, the AP applies the Fine Policy Rules 2019.37 After this, the AP first briefly explain the fine system, followed by the motivation of the fine (amount) in the present case.

4.2 Fine policy rules of the Dutch Data Protection Authority 2019

Pursuant to Article 58, second paragraph, preamble and under i and Article 83, fifth paragraph, of the GDPR, read in in conjunction with Article 14, third paragraph, jo. 18 of the UAVG, the AP is authorized to the Municipal Executive of Enschede 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 the present violation of Article 5(1)(a) of the GDPR is: subject to 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 (Awb) taking 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. Assessment circumstances

When asking whether an administrative fine is imposed and the amount thereof, the AP takes into account: various factors. In this assessment, the AP takes into account, among other things, the nature, size and number of affected persons.

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

37 Stcrt. 2019, 14586, March 14, 2019.

38 Article 2, under 2.2 and 2.3 of the Fine Policy Rules in conjunction with. Appendix 2 of the Fine Policy Rules 2019.

government agency can base its actions on a sufficiently accessible, accurate and foreseeable legal requirement. With the collection of personal data without a basis, the B&W Enschede Commission has violated the principle of lawfulness. This touches the core of the right to respect for privacy and the protection of personal data. It detracts from the citizen's feeling of being unnoticed in public delusions and confidence in government.

From May 25, 2018 to April 30, 2020, the college B&W Enschede has no basis personal data of hundreds of thousands of citizens. This violation was thus structurally and lasted for a long period of time. From the data collected under responsibility of the B&W Enschede Board has been processed, a detailed picture can be obtained drawing up the behavior of (individual) citizens. For example, the living patterns can change a person's living or workplace, as well as more sensitive data such as visits to medical facilities or locations that can provide data about a person's sex life.39 The mere fact that this is possible can lead to citizens no longer feeling unnoticed by the government. In view of this, according to the AP speaks of a serious situation.

In addition to the fact that the Municipal Executive of Enschede is not based on a foreseeable statutory regulation, processed personal data, the AP also considers it wrong that the Board 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, the greatest possible care must be taken to prevent this data from being (indirectly) become identifiable.

In view of the above circumstances, the AP sees a reason to send a letter to the B&W Enschede board fine and the basic amount of the fine pursuant to Article 7, opening words and under a, of the

Fines policy rules 2019 to be increased by € 75,000 to € 600,000.

View of the board of B&W Enschede and reaction AP

In its view, the Municipal Executive of Enschede states that there are never special and criminal law cases personal data has been processed. Given the very limited nature and seriousness of the alleged infringement of the AVG, the B&W Enschede Commission therefore believes that a fine-reducing circumstance exists.

In addition, according to the college, the parties involved did not suffer any damage. Furthermore, the municipality Enschede has never been tapped by the AP before because of a violation of the privacy law.

and regulations and the municipality of Enschede has always fully cooperated with the investigation of the AP. The Municipal Executive of Enschede therefore considers these circumstances to be fine-reducing factors.

The AP does not follow the view of the Municipal Executive of Enschede and motivates this as follows. Like mentioned above, sensitive data can be derived from the collected data. A

government agency that processes personal data without a legal basis for doing so is

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

certainly harmful to civilians. In addition, the B&W Enschede college has not substantiated why those involved have suffered no damage. Despite the AP not having the same breach before determined by the Municipal Executive of Enschede and according to the Municipal Executive of Enschede there is no question of

damage, the AP sees because of the seriousness of the violation and the culpability of the B&W Enschede Board there is 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 Enschede is no further

has gone beyond its legal obligation to comply with Article 31 of the GDPR. The college B&W Enschede has therefore not cooperated with the AP in a special way.

4.3.2 Blame and negligent nature of the infringement

Pursuant to Article 5:46, second paragraph, of the Awb, when imposing an administrative fine, the AP into account the extent to which this can be blamed on the offender.

Pursuant to Article 6(1) of the GDPR, processing of personal data is only lawful if this takes place on an accounting basis. This is a continuation of what already applied under Directive 95/46/EC and the Personal Data Protection Act. The basic principle is that the Municipal Executive Enschede has its own responsibility to comply with the law from the entry into force of the GDPR 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 alter this. The college B&W Enschede has the legal task of determining the processing purposes to assume responsibility for the data processing regarding the WiFi counts. The college B&W Enschede has left behind to carefully research the collected data or to obtain legal advice about it. Also the fact that Bureau RMC had stated in the offer that they convert and validate data to visitor flows and walking flows of the shopping public, the college B&W Enschede was alert should ensure that visitor flows could also be displayed from the collected data. In instead, the B&W Enschede Commission assumed that a third party, with a commercial interest, took on the responsibility. The AP considers this culpable.

The Municipal Executive of Enschede has argued that they have always focused on guaranteeing privacy with regard to the WiFi counts performed by Bureau RMC. According to the college, this is as a mitigating circumstance, as they are not intentionally or knowingly way of processing personal data. Furthermore, the B&W Enschede Board finds that they have not been negligent, given that the measures taken were aimed at processing purely anonymous data that are not traceable to individuals.

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

imposing an administrative fine or reducing the amount of the fine. The AP is of the opinion that the above-mentioned circumstances do not exculpate the Municipal Executive of Enschede. Of a government agency, also in view of the large scale of the data processing, it may be expected that it thoroughly ascertains and complies with the standards that apply to it. Especially in a society where it is increasingly difficult to anonymize data. The B&W Enschede college had more research to the data processed under its responsibility. Or Bureau RMC de

agreements with the Municipal Executive of Enschede have or have not been complied with, is a civil matter between Bureau RMC and the college. The AP also notes that the violated provision of Article 6, first paragraph, of the GDPR no intent required as a component. Since this is a violation, the imposition of a administrative fine, in accordance with established case law, does not require that it be demonstrated that there is intent.40 The AP may assume culpability if the perpetrator has been established.41

4.3.3 Proportionality and financial circumstances

Finally, on the basis of Articles 3:4 and 5:46 of the Awb (principle of proportionality), the AP assesses whether the applying its policy for determining the amount of the fine given the circumstances of the specific case, does not lead to a disproportionate outcome. Application of the principle of proportionality may among other things, play 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 in almost all municipalities in The finances are under pressure in the Netherlands due to, among other things, Corona.42

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

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

circumstances of the municipality. Regardless of this conflicting signal, the AP has

figures from the municipality of Enschede were consulted. 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 In view of 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

to reduce the fine. The AP considers the fine of € 600,000 proportional and there are no other options

facts and circumstances that require moderation of the aforementioned amount.

4.4 Conclusion

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

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

ECLI:NL:CBB:2015:312, para. 3.7 and 7 March 2016, ECLI:NL:CBB:2016:54, para. 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, para. 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 Enschede to the AP, page 3.

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

Our reference

[CONFIDENTIAL]

Date

March 11, 2021

5. Operative part

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

violation of Article 5, first paragraph, under a, jo. Article 6(1) of the GDPR imposes an administrative fine on amounting to €600,000 (six hundred thousand euros).44

Yours faithfully,

Authority Personal Data,

w.g.

drs. C.E. Mur

board member

Remedies Clause

If you do not agree with this decision, you can return it within six weeks of the date of dispatch of the decide to submit a notice of objection digitally or on paper to the Dutch Data Protection Authority. Submit it of a notice of objection suspends the effect of this decision. For submitting a digital objection, see www.autoriteitpersoonsgegevens.nl, under the heading Objecting to a decision, at the bottom of the page under the heading Contact with the Dutch Data Protection Authority. The address for paper submission is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague.

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

In your notice of objection, write at least:

- your name and address;
- the date of your notice of objection;
- the reference mentioned in this letter (case number); or attach a copy of this decision;
- the reason(s) why you do not agree with this decision;
- your signature.

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

Date

March 11, 2021

Attachment 1

1. Facts about the concept of personal data

1.1 The sensors installed in the city center of Enschede

If the Wi-Fi is turned on on a mobile device, the device will broadcast 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 receive these signals. An employee of [CONFIDENTIAL] has stated that consumer routers are used as sensors in Enschede used.45

The Municipal Executive of Enschede has stated that the WiFi measurements are carried out using eleven sensors. These eleven sensors were installed on 25 May 2018 and this number has not changed since.46 Office 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 . collected with the sensors data.

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

Figure 1: Two sensors found at two different retailers

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

and 55).

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

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

48 Citytraffic_nummer_telpunt 4 Excel sheets and Citytraffic_weekoverzicht 4 Excel sheets, appendices 14 and 15 in 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] on

December 12, 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, attachment to e-mail of 23 May 2019 from Bureau RMC to the AP (file document 25).

50 Statements of Official acts on the spot 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 the other side of the street.51 Bureau RMC states on the website www.citytraffic.nl that this range is 20 to 30 meters is .52

Based on the foregoing, the AP has established that there have been eleven sensors in place since 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 to use sensors to collect data from mobile devices on which the WiFi is located enabled to collect and process them into reports using the 'City Traffic method'. This City Traffic method is applied in the city center of Enschede. On the website of Bureau RMC there is a infographic visualizing this method (as of 1 January 2019).53 In this section, the AP discusses the different phases of data collection and processing by means of the City Traffic method.

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

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

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

53 Screen images of web pages on www.rmc.nl captured on 26 April 2019 (file document 10).

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

The first phase concerns the capture by the sensors of certain data from mobile devices on which the Wi-Fi is turned on. Each sensor has a specific range and in this section demonstrated that both on entry into range and on exit from range, data from the mobile device and then sent partially pseudonymized 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 has further stated that the functioning of the sensors is not changed since 25 May 2018.55

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

an employee of [CONFIDENTIAL] replied: “The MAC address, 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 tracked when you are first seen by the sensor and when you were last seen.” 56

A device's aforementioned MAC address is a factory-built globally unique

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

previously stated, a device with Wi-Fi turned on will transmit the signal at regular intervals

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

device detected by a sensor.

Later in the statement, an employee of [CONFIDENTIAL] indicated that 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 phone tracking (e.g. by Apple). Spoofed

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

It appears from the software code provided by [CONFIDENTIAL] to the AP that runs on the sensors that the

next on the sensor happens as soon as a Wi-Fi enabled device is within range of the sensor

coming:59

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

2. The date and exact time of receipt will be determined.

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

and 55).

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

and 55).

56 Page 1 of report of statement of 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 report of statement of 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).

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, associated with 'status 1' to indicate that the relevant data relates to the moment the mobile device entered the range came.63

About the moment when the MAC address is pseudonymised, the director of Bureau RMC declared: “It will be replaced on the sensor immediately, so the sensor will have the MAC address immediately.”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 sensors software code. It shows namely, as explained in the previous marginal number, 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 Wi-Fi enabled device is within range of a sensor: “The MAC address will be used throughout the time captured, the sensor checks if the MAC address has been seen before, if so, it increases the last seen time and this process repeats 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 effect.67

An employee of [CONFIDENTIAL] 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 passer-by, data is sent twice.”68 The software code and our own analysis of this software code by a supervisor of the AP confirms this effect.69 Collecting both the time when the MAC address first comes in range (state 1) as the last seen time (state 2) is used to determine the dwell 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 report of statement of Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

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

62 This is a unique number associated with each sensor.

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

64 Page 3 of report of statement of 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 to signify pseudonymization.

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

66 Page 3 of report of statement of 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 of Bureau RMC and employees [CONFIDENTIAL] made on May 29, 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 that the following data is sent to the server: Status '2', pseudonymised MAC address, last signal strength measured in range, last measured date and time in range (this refers to the time 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 is no longer in 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 an own analysis of this software code by a supervisor of the AP confirms this operation.72

On the basis of the foregoing, the AP concludes that from May 25, 2018 to the present, every sensor had the same effect in the city center of Enschede. During this period, the sensors have all mobile devices within range with Wi-Fi enabled the MAC address, signal strength, date and time collected and temporarily stored in the working memory of the sensor. This save lasted as long as the device was within range of the sensor plus two minutes.

The AP also notes that the sensors are continuously scanning. Finally, the AP establishes that there are of each detected device on entry and two minutes after leaving the sensor range 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 the same on every sensor in Enschede pseudonymization method is applied and that this method has not been changed since May 25, 2018.73

When asked by the AP which method is used, an employee of [CONFIDENTIAL]

replied: “[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 yields practically one hashed number, there is minimal chance of collision namely that 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 of 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 (document document 78).

73 Pages 2 and 4 of report of statement of Bureau RMC and employees [CONFIDENTIAL] made on May 29, 2019

(file documents 49 and 55). The [CONFIDENTIAL] employee has also stated that the same method is used on all their sensors running in the Netherlands.

74 Page 4 of report of statement of Bureau RMC and employees [CONFIDENTIAL] made on May 29, 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).

hashed value.”77 The document on the pseudonymization method shows that

[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 been changed since 25 May 2018. In addition, the AP determines 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, the AP has established that in any case from May 25, 2018 in the city center of Enschede van any mobile device with Wi-Fi turned on that has passed through the range of a sensor there data from the mobile device twice, i.e. when entering range and two minutes after departure from the range, real-time are sent to the server. In addition, the AP concluded that per January 1, 2019 all pseudonymized MAC addresses incoming to the server will be truncated. About this, an employee of [CONFIDENTIAL] stated: “If the hashed 79 MAC address comes in it is truncated in memory (real time) and it is then written into a raw table, (…).”80 Also, an employee of [CONFIDENTIAL] stated: “We use two tables on the server. A short-term table containing today's data and a long-term table containing 6 months' data.”81 The AP will first deal with the short-term table.

About what will be truncated 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 clipped and the rest of the data doesn't change that.”83 software code confirms the foregoing, with the addition that also the colons from the clipped pseudonymised MAC address are removed.84 The result after clipping is a series of [CONFIDENTIAL] consisting of 0-9 or a-z without colons (see MACNUMBER column in Figure 3).

77 Page 5 of report of statement of Bureau RMC and employees [CONFIDENTIAL] made on May 29, 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 (document 43).

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

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

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

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

83 Page 6 of report of statement of 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] contacted the supervisors of

gave the AP access to the short-term table.85 In addition, these employees have a

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

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 with which the device was detected.

'STATUS' 1 is the moment he was first sighted and status 2 is the moment he was 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 (document 39).

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

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

87 Pages 9 and 10 of report of statement of Bureau RMC and employees [CONFIDENTIAL] made on May 29, 2019 (file documents 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 recorded to the second. The HOSTNAME is the unique sensor ID, each of the eleven sensors in the city center of Enschede has a unique [CONFIDENTIAL] code.88

In the screenshot above there are two consecutive status 1 and status 2 records in blue and in red of the same truncated pseudonymised MAC address boxed ([CONFIDENTIAL]). Later shows the AP recommends that each of these two records be merged into one record in the long-term table.

On the basis of the foregoing, the AP has established that, at least since 25 May 2018, the data collected 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 when the device was scanned by the sensor is exactly to the second. In the period up to January 1, 2019, the pseudonymised MAC-address is not cut off on arrival at the server, in the period from January 1, 2019 it is. cutting it off involves removing the last three characters of the pseudonymised MAC address (without colon). The other data sent to the server, namely 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 May 29, 2019, an employee of [CONFIDENTIAL] stated that on the short-term table, covered in the previous paragraph, every night certain filters are applied and the remaining records are added to the long-term table added.90 This employee of [CONFIDENTIAL] explained about this in a document: “The code for the filters (…) run in the morning at 00:15:00 in time zone 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 containing the data for a longer period of time. These are the opt-out filter and the resident filter.”91

The explanation of [CONFIDENTIAL] on the opt-out filter concerns: “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 B&W Enschede college has been giving about this opt-out list since the start of the WiFi measurements on the website of the municipality the following explanation: “Everyone has the possibility to use their MAC addresses from mobile phones.” devices on the City Traffic website for an opt-out register. After this, these MAC addresses are not longer counted and included in our studies. The opt-out register can be found at http://citytraffic.nl/site/page/opt-

88 During the on-site investigation at Bureau RMC on May 29, 2019, the AP was given a list with 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 when the sensors were disabled, see

appendix 1, paragraph 2.5.

90 Page 7 of report of statement of 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 20 June 2019 (document 46).

out."93 The webpage mentioned at www.citytraffic.nl contains a field that allows someone to enter the MAC address of his/her mobile device 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 that MAC addresses that have been specified are no longer captured by the sensors.

The explanation of [CONFIDENTIAL] on 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 between 05:00 and 07:00 has been seen as between 22:00 and 23:59:59." 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 that's clipped pseudonymised MAC address between 5 a.m. and 7 a.m. and between 10 p.m. and midnight in or out of range of the same sensor. There must be a detection in both time periods. This effect has

As a result, if, for example, a person with a mobile device with Wi-Fi turned on

lives within range of a sensor and is at home all day, the records of his/her mobile
device are not filtered out. The same applies, for example, to residents who only live between 5 and 7 or
leave the house or come home between 10 p.m. and midnight.
With regard to the resident filter, the AP notes that it collected every night on the daily
data is applied, which means that every day it is determined again whether someone qualifies as
resident or not.96 It follows from Figure 7 on page 48 that the qualification can differ from day to day.
Since the start of the WiFi measurements in September 2017, the B&W Enschede college has published on the website of
the municipality the following Q&A are for residents of the city center of Enschede:97
“I live in the city centre, what is done with my data?
City Traffic counts the number of passers-by in the shopping street. The sensors therefore have an automatic filter to protect
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 a
seen during the day, once in the morning and once in the evening, this is a signal from a resident. These signals become
automatically filtered out every day from then on. 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 filtering
apply while this is done on the server. Second, it is suggested that once
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 January 6, 2020.
94 Page 3 of source code, clipping and filters.pdf, received from [CONFIDENTIAL] on 20 June 2019 (document 46).
95 ConvertWifi.php, received from [CONFIDENTIAL] on June 20, 2019 (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 (document document 78).
97 Q&As, appendices 5 and 6 to the letter of 24 May 2019 from the Municipal Executive of Enschede to the AP (file document

26).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

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.

On the basis of 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 result in

certain records from the short-term table do not end up in the long-term table. In addition

the AP notes that the resident 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 truncation of the pseudonymised MAC address was introduced on January 1, 2019, the

long-term table until January 1, 2019 pseudonymised MAC addresses and after January 1, 2019 only

truncated pseudonymised MAC addresses. An employee of [CONFIDENTIAL] has

stated: “We have retroactively deleted the hashed mac addresses that were in the database around that period

cut off. 98

On September 6, 2019, at the request of the AP, [CONFIDENTIAL] released the long-term table with the

data about Enschede for only 29 May 2019.99 A screenshot of the first few

records from this long-term table, filtered by the two truncated pseudonymised MAC addresses

boxed in the short-term table in Figure 3 concerns:

Figure 4: Screenshot of Long-Term Table Section

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 sequenced and the Retention in

98 Page 3 of source code, clipping and filters.pdf, received from [CONFIDENTIAL] on June 20, 2019 (document 46) and page 6 of

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

99 Export Enschede 29-5-2019 long term table.zip, received from [CONFIDENTIAL] on 6 September 2019 (document 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 in a document on 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

TimeOff = end time observation

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 AP notes that in the above list by [CONFIDENTIAL] the column “[CONFIDENTIAL]” per

was mistakenly not included, this column refers to the aforementioned sensor ID. In addition, the AP . notes

that the TimeIn and TimeOUT are in seconds, so the Retention is also in seconds.

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

Municipality of Enschede, it was a storage period of six months from the start of the counts, this has not been the case since

then

changed.”102 It was later explained by the director of Bureau RMC that on the first of the month the

data from the month from six months ago will be deleted.103

On the basis of the foregoing, the AP concludes that, after applying the filters to the short-term table,

two consecutive records of the same (truncated) pseudonymized 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

pseudonymised MAC address. The AP also notes that in the long-term table from May 25, 2018

data covered a period of between six and seven months.

The processing of the raw data and the figures that the Municipal Executive of Enschede receives from Bureau RMC

The data in the long-term table form the basis for the figures that the Municipal Executive of 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 is first deduplicated and then statistical operations are performed on it

are applied.

100 See also Appendix 1, paragraph 1.2, page 35, which includes the statement of employees [CONFIDENTIAL] that spoofed

MAC

addresses are not included in the counts.

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

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

and 55).

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

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

An employee of [CONFIDENTIAL] during the on-site investigation on May 29, 2019

declared: “Yes, within a zone we deduplicate.” The director of Bureau RMC added: “We want this

deduplicate 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 10 times is not 10 times a buyer, but is 1x a buyer who has been seen 10 times. The customers want

know the number of unique visitors within a zone. (…). So when the two of you walk into the city center of Enschede and there is no one else, then you only return to the first sensor where you were seen in the aggregated half-hour image. 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 right in the raw data.” 104

An employee of [CONFIDENTIAL] then stated: “In order to deduplicate we have it

pseudonymised MAC address. We count unique numbers, so if a MAC address is captured 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 cut off on the server, but with a certain degree of certainty we can say that the same

phone went to sensor A and later to sensor B.”

The director has informed about the statistical operations that are subsequently applied to the deduplicated data

van Bureau RMC stated: “A one-off 'manual calibration' was carried out during the installation of each sensors. Then the conversion becomes

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

one-off and further, we conduct market research into the possible increase or decrease in Wi-Fi use.” 105

And: “During the manual calibration, it is determined what percentage of the passers-by is, for example, a cyclist. This percentage is later deducted from the collected data so that we are left with only the passers-by. This is a probability calculation. This makes our counts a little less reliable because 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 our customers this very emphatically.” 106

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

received to the AP.107 It follows from this that the B&W Enschede Commission first of all made estimates

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

Enschede. Below is a screenshot shown with the numbers 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 of Bureau RMC and employees [CONFIDENTIAL] made on May 29, 2019 (file documents 49

and 55).

105 Page 8 of report of statement of Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

106 Page 8 of report of statement of 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 Enschede to the

AP (file document 3). Citytraffic_nummer_telpunt 4 Excel sheets and Citytraffic_weekoverzicht 4 Excel sheets, appendix 14 and 15 to the letter from

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

108 enschede_Whole_export_2019w14.xls in Citytraffic_weekoverzicht 4 Excel sheets, annex 15 to the letter of 24 May 2019 from the

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

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

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

On the basis of the foregoing, the AP concludes that the Municipal Executive of Enschede receives estimates of different variables about unique visitors to the city center of Enschede. For this the applicable data in the long-term table is deduplicated based on the clipped pseudonymised MAC address and then certain statistical calculations are performed on it applied.

Privacy protocol City Traffic method of Bureau RMC

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 25 May 2018 to 21 April 2020 there will be two successive 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 passer-by data. The passer-by details include data from passers-by that can be traced directly or indirectly to an individual passer-by. The passer-by details are therefore to be regarded as personal data within the meaning of the General Data Protection Regulation (GDPR). (…).

3.1 (…) The analysis results are reported to our clients on an aggregated basis only. This
means that the data in these reports can no longer be traced back to the encrypted number (of 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 Answer to 'Questions about the information that the municipality of Enschede receives from the RMC office' and Citytraffic_nummer_telpunt 4
Excel sheets, appendix 14 to a letter dated 24 May 2019 from the Municipal Executive of Enschede to the AP (file document 26).

110 Privacy protocol for pedestrian counts Bureau RMC last update April 10, 2018 (file document 8) and Privacy protocol for pedestrian counts
Bureau RMC last update January 22, 2019 (file document 11).

In the first passage Bureau RMC declares that in the context of the City Traffic method
personal data within the meaning of the GDPR. The privacy protocol does not specify until which moment in
the phase 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 infers that Bureau RMC is of the opinion that it
personal data is processed up to the moment of anonymisation. The text reads: "On the server
the pseudonymised data is truncated so that it cannot in any way be traced back to a unique device or
individual. The data we have is therefore anonymous."
On the basis of the foregoing, the AP concludes that Bureau RMC specifically sees this in its privacy protocol
to processing via the City Traffic method, has stated that it and/or its partners from any
case 25 May 2018 processing 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.

Life patterns can be traced from the long-term table

As is established by the AP in Appendix 1 paragraph 2.5, Bureau RMC has the

'anonymize on the server' entered. This means that for each pseudonymised MAC address at

reception on the server the last three characters (without colon) are removed.

The AP notes that, unlike about pseudonymizing the MAC address, the AP of

[CONFIDENTIAL] whether Bureau RMC has not received a document with an extensive explanation of

the cutting and why this method of anonymization was chosen.111 In general, it applies that

snipping an attribute is an anonymization technique that makes an attribute

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

time interval (hour, day, month).

The truncation results in not one but several pseudonymised MAC addresses leading to

one and the same truncated pseudonymised MAC address.112. The clipping refers to worldwide

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

In order to test whether the cutting 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 transfer the data

anonymity, an AP supervisor has the long-term table of data from a number of

common truncated pseudonymised MAC addresses for weeks 23 through 34 of

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

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

the data. This is because it concerns the 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 Opinion 5/2014 on anonymization 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 (file documents 69 and 72).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

After its own investigation, the AP has found that the data of certain cut-off 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 of four truncated pseudonymised MAC addresses.114 In each visualization, the days are displayed horizontally of the week and vertically the week number in 2019. Each gray square represents a whole day, from 0:00 s night until 23:59:59. The hours 8:00 and 18:00 are highlighted. A colored line or area means that the truncated pseudonymised MAC address in question from the start moment to the end moment in range of that sensor.

The first visualization below shows consistent presence within the range of the sensor [CONFIDENTIAL] (red), namely every Monday afternoon, Wednesday and Saturday from about 10:00 to 18:00 and Thursday from about 10:00 to 21:00. The pattern closely resembles the shopping hours that apply in the city center of Enschede, where it is shopping evening on Thursday.115 Also follows from the pattern that the truncated pseudonymised MAC address every last Sunday of the month before was within the red sensor for a few hours. Given this pattern, the AP does not consider it inconceivable that the belongs to an employee or manager of one of the stores in the Langestraat in Enschede, where the [CONFIDENTIAL] sensor hangs.116

Figure 6: First Visualization of Clipped Pseudonymized MAC Address

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

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

116 Excel list location sensors, attachment to e-mail of 23 May 2019 from Bureau RMC to the AP (file document 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). Here it is striking that on one day there is either no
registration is visible (no dashes) or registrations spread over the day. This is the result of the
page 40 and 41 described the fact that the resident filter is applied daily and therefore a different one every day
outcome (resident or not). In addition, it can be seen in, for example, the Tuesday in week 23 that
if there are registrations between 5 and 7 a.m. but not between 10 p.m. and midnight, the resident filter does not
is activated (after all, there are dashes in this day). The AP does not consider it inconceivable, given the
nightly registrations, that the above pattern belongs to a resident.

Figure 7: Second Visualization of Clipped Pseudonymized MAC Address

The third visualization below shows a truncated pseudonymised MAC address that is on Tuesday through
with Friday every day between about 8:00 AM to 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 Clipped Pseudonymized MAC Address

The fourth visualization below shows a truncated pseudonymised MAC address on Tuesday through

with Saturday between 04:00 and 05:00 at night by some of the sensors in the city center of

Enschede has been received. Perhaps this concerns a person who likes to take a walk at night.

Figure 9: Fourth Visualization of Clipped Pseudonymized MAC Address

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

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

conclude that the records associated with the pattern belong to one mobile device.117

1.3 Duration of processing and number of data subjects

The AP has established above that at least since 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 in the period from December 10, 2018 to January 3, 2019, the sensors

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

data has been stored in the long-term table during this period, so there were

period data is processed.

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

WiFi measurements are still being performed. This is how 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 is neither of the Municipal Executive of Enschede nor of

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

the enforcement procedure of the AP, the Municipal Executive of Enschede has stated in its view that it is

college has discontinued the WiFi counts. The B&W Enschede college has asked the Bureau on April 30, 2020

RMC commissioned data to switch off the sensors as of May 1, 2020. The sensors do not supply counting data more from 1 May 2020.121 The AP therefore determines that the duration of the processing is the period from May 25, 2018 to April 30, 2020.

The exact number of people involved of whom in the period from May 25, 2018 to April 2020, via his or her mobile phone device data processed cannot be determined because [CONFIDENTIAL] and Bureau RMC's data will not be kept for 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 June 1 period 2019 to December 6, 2019, an estimate can be made of the number of mobile devices of data subjects of whom data was processed in the period from May 25, 2018 to April 4, 2020.122

The graph 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 pseudonymized MAC-address therefore appears once in the graph, namely in the week in which it is for the first time detected by a sensor in the city center of Enschede.

117 Registrations outside of this pattern may come from other mobile devices.

118 See also appendix 1, paragraph 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 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, during this 27-week period, there was data from 671,701 unique mobile phones devices in the long-term table.

If previous figures for the period June 1 - December 6, 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 here that the first 27 weeks after May 25, 2018 will be the same as the graph above. It has also been assumed that after the 27 weeks until April 4, 2020 the number of new detections is 16,000 weekly.123 This number holds does not take into account the fact that for residents and persons who work in the city center of Enschede and those who have enabled Wi-Fi on their mobile device, they do not have to do this once, but (a lot) more often detected by the sensors.

On the basis of the foregoing, the AP concludes that the B&W Enschede Board will in any case be from May 25th 2018 to date 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, 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.

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

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 Municipal Executive of Enschede. This follows from the Board decision, the first page of which is shown below.124

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

124 Board decision of September 5, 2017, appendix to e-mail of September 23, 2019 from the Municipal Executive of Enschede to the AP (file document
62).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

It follows from this page that the B&W Enschede Board approved the proposal on September 5, 2017.
of the alderman to switch from 1 yearly manual counts to . as of September 6, 2017
24/7 WiFi measurements.

After the decision of 5 September 2017, the Municipal Executive of Enschede, the municipal council of Enschede informed by letter.125 In addition, there is also a press release on the municipality's website as a number of Q&As about the WiFi measurements.126 In this communication it is stated that City Traffic B.V. would carry out the WiFi measurements.

City Traffic B.V. was at the time a company owned by Bureau RMC and [CONFIDENTIAL]. on
This company was dissolved on 24 May 2018.127 Since then, Bureau RMC has been commissioned by the Commission to B&W Enschede carries out the WiFi measurements, whereby Bureau RMC purchases certain services from [CONFIDENTIAL]. Bureau RMC now uses the term 'City Traffic' for its service to use WiFi measurements to count unique visitors in cities, among others.128

The director of Bureau RMC informed the
stated the following: “City Traffic has been in existence since 2010 and has positioned itself as an alternative to Locatus to do passenger 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 to propose to do wifi counts there. (…) The reason for the request from the municipality was the fact that through wanted to roll out a certain subsidy free WiFi 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 make a correlation show between counts of NDIX. It was later decided not to use the NDIX counts." 130

The offer submitted by Bureau RMC confirms that the B&W Enschede Commission had requested connection to the network of NDIX.131

To questions from the AP about the influence of the municipality 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, annex 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 to the letter of 24 May 2019 from the Municipal Executive of Enschede to the AP (file document 26).

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

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

131 Page 2 of the quotation Monitoring Visitor flows Inner City Enschede from Bureau RMC, annex 1 to letter dated 24 May 2019 from the college B&W Enschede at the AP (file document 26).

Date

March 11, 2021

Our reference

[CONFIDENTIAL]

The municipality has therefore determined the locations of the sensors. (…) the municipality had the coordinating role in the awarding of contracts. In front of

As for the number of sensors, I would have preferred many more. 132

On the basis of the foregoing, the AP concludes that the Municipal Executive of Enschede has taken the initiative and the has taken the final decision to start with 24/7 measurements via sensors in . on September 6, 2017.

the city center of Enschede. The B&W Enschede college has sent two companies a quote for this

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

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

2.2 Purpose of the WiFi measurements for the Municipal Executive of Enschede

In the municipal decision of September 5, 2017, the Municipal Executive of Enschede has set the purpose of the WiFi measurements

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

do people walk through the streets, how many visitors does 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 . from September 6th

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 of this.

We do this via the passer-by counts via sensors that give us daily insight into the number of visitors and the number of visitors visitor flows in the city center. This gives us a picture of the attractiveness of our city centre, of the

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

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 WiFi measurements had started, the complainant submitted a complaint to the Enschede B&W Board.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 its effects);

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

On the basis of 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 handling of public funds. The Municipal Executive of Enschede considers the WiFi measurements to be lawful

because, in its view, they take place on the basis of the 'legitimate interest' basis.

132 Page 11 of report of statement of Bureau RMC and employees [CONFIDENTIAL] made on May 29, 2019 and email of

May 19

August 2019 from Bureau RMC to the AP (file documents 49 and 55).

133 See Figure 1 in this report.

134 Q&A amended in December 2017, appendix 6 to the letter of 24 May 2019 from the Municipal Executive of Enschede to

the AP (file document 26). A

text with a similar meaning was available on the municipality's website from the municipal executive decision of September 5,

2017.

135 Letter of 10 November 2017 from the complainant to the municipality of Enschede, appendix to the letter of 16 July 2018

from the complainant to the AP (document 1).

136 Letter of 21 December 2017 from the Municipal Executive of Enschede to the complainant, annex 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 B&W Enschede and Bureau RMC

On September 26, 2017, the B&W Enschede Board 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 processor 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 person, legally represented by: [CONFIDENTIAL] and City Traffic, established in Amsterdam, hereinafter referred to as the processor, validly represented for this purpose by [CONFIDENTIAL], declare that they have agreed (…)”

The first, third and fifth paragraph of article 4 of the processor agreement provides the following about the rights and obligations of the two parties:

“1. The College of Mayor and Aldermen of the Municipality of Enschede is responsible within the meaning of the Wbp.

3. The processor processes data on behalf of 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 and will follow all reasonable instructions in this regard, unless otherwise required by law.

6. The processor will at all times at the first request of the responsible party immediately provide all of the Municipal Personal data originating from Enschede with regard to this processor agreement to the responsible party shake hands.”

Article 7, on the involvement of third parties, states:

“1. The processor is only entitled to outsource the execution 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 will have the data processed by [CONFIDENTIAL]. Editor has with this party has entered into a processing agreement.

(…)”

On the basis of the foregoing, the AP concludes that the B&W Enschede Commission itself as controller considers within the meaning of the Wbp (currently the AVG) for the execution of wifi measurements. In addition, the AP notes that City Traffic B.V., now Bureau RMC, uses personal data processed on behalf of the Municipal Executive of Enschede, must follow its instructions and at the request of the Municipal Executive of 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 for monitoring visitor flows in the city center of Enschede dated September 26, 2017, annex 2 to letter dated October 29 2018 from the Municipal Executive of Enschede to the AP (file document 6).

2.4 The services provided by [CONFIDENTIAL] 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 buys 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]. Subsequently, the municipality Enschede subscribe 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 dated October 31, 2016 confirms that [CONFIDENTIAL] the installation and 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, [CONFIDENTIAL] employees generally have answered detailed questions from the AP about the collection and processing of the data142 and the required documentation. It also follows from the invoice submitted that [CONFIDENTIAL] pays for the rented server space at Amazon AWS.143

Article 7 of the service level agreement contains the following information about the data collected with the sensors:

agreement entered into 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 other than primarily applicable to the customer. (…) The customer can at any time demand the data as well as the oblige the contractor to delete data."

On the basis of the foregoing, the AP concludes that Bureau RMC hires [CONFIDENTIAL] for the installation and maintenance of the sensors in the city center of Enschede and for the collection and validate 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 of Bureau RMC and employees [CONFIDENTIAL] made on 29 May 2019 (file documents 49 and 55).

139 Page 8 of report of statement of 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 May 29, 2019 (document 39).

141 The introduction to the Service Level Agreement [CONFIDENTIAL]-Bureau RMC (document 39).

142 Report of statement of 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).

2.5 Decision to pause Wi-Fi measurements and switch to 'anonymize on the server'

On November 30, 2018, the AP released a news item stating that under the GDPR, companies are only allowed to follow people with WiFi tracking in very exceptional cases.144 In response [CONFIDENTIAL] within the municipality of Enschede, sent an e-mail to the director 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 (ed: City Traffic) fall below this?

- If so, is anonymization perhaps still an option?

- (…)”

Following the news item from the AP, the B&W Enschede board contacted Bureau RMC and instructed her to pause the WiFi measurements. This follows from the Municipal Executive of Enschede sent a letter of 6 December 2018 to the city council:

“(…) 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 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 picked up again from January 1, 2019

because from that moment on, counting is anonymized. (…) Can you confirm to us by email that you actually

counting anonymously as of January 1, 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 pseudonymization on the sensor, will anonymize on the server. (…)"

As proof of the actual implementation of this 'anonymization on the server', [CONFIDENTIAL] has issued a

screenshot of the change in the server software code submitted to regulators of the

AP.148 It follows that at the end of December 2018 the 'anonymization on the server' was implemented, at least

dat [CONFIDENTIAL] of the pseudonymised MAC address (without the colons) will be

cut off. Appendix 1, pages 38 through 40, describes clipping in more detail.

On December 18, 2018, the municipal council was informed by letter B&W Enschede by letter

of the fact that the WiFi measurements would be resumed.149 This letter states:

144 www.autoriteitpersoonsgegevens.nl/nl/nieuws/bedrijven-mogen-mensen-only-bij-hoge-exception-with-wifitracking-follow.

145 Email dated 3 December 2018 from [CONFIDENTIAL] to [CONFIDENTIAL] from Bureau RMC, annex 7 to the letter dated 24 May 2019 from

the Municipal Executive of Enschede to the AP (file document 26).

146 Letter of 6 December 2018 to the Enschede Council to pause WiFi counts, annex 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, annex 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 June 20, 2019

(file item 46).

149 Letter of 18 December 2018 to the Council for restarting WiFi counts, annex 11 to the letter of 24 May 2019 from the Municipal Executive of 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 address that is encrypted on the sensor). This is seen by the AP as personal data and must therefore comply with the General Regulations Data Protection (GDPR). (…) With anonymized data, there is no question of personal data. In that case, the General Data Protection Regulation not applicable. This is confirmed in the publication of the AP 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 visitors to our website safeguard the inner city. From January 1, 2019, the sensors will be reactivated and we will be able to resume monthly report on the counts.”

It follows from the information from the Municipal Executive of Enschede that Bureau RMC for the period from December 10th 2018 up to and including 3 January 2019 has not reported any figures to the Municipal Executive of Enschede.150

On the basis of the foregoing, the AP concludes that the Municipal Executive of Enschede, as a result of the publication of the AP of November 30, 2018 Bureau RMC has commissioned the WiFi measurements in the city center of Enschede and that over the period from December 10, 2018 to January 3 inclusive 2019 no figures have been reported to the B&W Enschede board by Bureau RMC. the AP concludes on this basis that the sensors in the city center of Enschede were deactivated in the period mentioned have stood. The AP also notes that Bureau RMC (at the request of the Municipal Executive of Enschede)

has introduced the so-called 'anonymisation on the server' as of 1 January 2019, whereby the last three characters of the pseudonymised MAC addresses are truncated.

150 shareperingang.xls in folder 20190212, appendix 14 to a letter dated 24 May 2019 from the Municipal Executive of Enschede to the AP (file document 26).