Privacy protocol footfall counts

Bureau RMC is responsible for the processing of personal data as laid down in this Privacy protocol.

Contact details:
Marnixkade 109F
1015 ZL Amsterdam
+31 20 653 5588
info@rmc.nl
www.rmc.nl

Pieter Paul Verheggen is Bureau RMC's external Data Protection Officer. He can be reached via p.verheggen@motivaction.nl.

Bureau RMC is a member of MOA and a Fair data member.

This Privacy protocol replaces every older version thereof. We may adjust this Privacy protocol from time to time. Last update: November 2023.

Bureau RMC uses the **CityTraffic method** for footfall counts. Thanks to the high-quality technology used for this method, we are able to, in cooperation with our **partners**, measure footfall in a location and how many visitors there are during a specific period.

Our **clients** are mainly municipalities and retailers, to enable them to adjust their policies based on **footfall data analysis**. For example, so they can optimize the development and layout aspects of an area to improve safety at events. The footfall data is also regularly used to provide insight into the effects of events and to assess measures in the context of combating a pandemic.

We value the careful handling of the footfall data. We are happy to inform you, with this privacy protocol, about the processing of footfall data in the context of our services. This privacy protocol, therefore, is aimed at anyone who happens to enter our measurement areas. This privacy protocol also aims to inform our clients about how we deal with personal data. The relationship with our clients is detailed in the agreements made with them about our services.

Footfall is measured using different methods. Some of our technical solutions process personal data, such as stereoscopic counts with scanners or Wi-Fi signal counts. Footfall is measured by counting the devices that are signaled in a measuring area by picking up the Wi-Fi signal from this **device** (such as a smartphone). When a pedestrian enters one of our measurement areas, their device is counted automatically. For an up-to-date list of measurement areas, visit our website https://www.rmc.nl/citytraffic/ or the website of the municipality you are visiting.

You may also be informed about the footfall measurement upon entering a measurement area. If the locally provided information regarding the processing of your data and the method of cancellation, deviates from the information given here, the information provided locally will prevail.

1 Processing of footfall data

1.1 To make our services possible, we process various types of footfall data. The footfall data includes data from footfall that can be directly or indirectly traced to an individual pedestrian. Footfall data can, therefore, be regarded as personal data within the meaning of the General Data Protection Regulation (**Dutch AVG**). Bureau RMC is the party responsible for the processing of MAC addresses by Bureau RMC and/or our partners within the scope of the AVG, insofar as they (alone or jointly with others) understand the purposes and means of processing MAC addresses.

1.2 We can also engage our Partners for our services. Bureau RMC will act as the jointly responsible party for the processing of MAC addresses of pedestrians in our measurement areas by us and/or our partners.

1.3 Bureau RMC has, also on behalf of its partners, reported the processing of MAC addresses to the Dutch Data Protection Authority at the time (College Bescherming Persoonsgegevens, CBP), which is known as the Autoriteit Persoonsgegevens (**AP**) from January 1, 2016.

1.4 Bureau RMC is not responsible for the privacy protocol as implemented by third parties.

2 Which data does Bureau RMC process?

2.1 Bureau RMC uses the fact that most pedestrians now carry a device that typically has the Wi-Fi and/or Bluetooth antennae activated, such as a smartphone, to process footfall data. Based on the MAC address, a randomized code fabricated by the device itself, in combination with the Bluetooth and/or Wi-Fi signals that a device transmits, and/or measurements via counting cameras, we can measure the footfall in a particular measuring area.

2.2 When a person visits a measurement area and has Bluetooth and/or Wi-Fi activated on their device, we process the following technical data from the device, to compile footfall data and perform the necessary analysis on it: the randomised and non-randomised MAC address that belongs to the device or is randomly created by the device and is transmitted by the device, which is instantly pseudonymized by the sensor and not stored, the location and visitor flow in the measuring area, as well as the corresponding time-stamps of the counts, which are determined using the Bluetooth and/or Wi-Fi signals transmitted by the device.

NB, our measuring systems do not collect any other data from a device.

2.3 We will only process the data that we need to perform analysis for our clients. We, therefore, ensure that the collected technical data is converted as quickly as possible into data that can no longer be linked to the device by third parties. The sensor encrypts the device's MAC address irreversibly to another number and never stores this number. There are no original MAC addresses of devices in our systems. We analyze the Wi-Fi signals when they’re already encrypted as explained above, and not based on the original MAC addresses.

2.4 We also measure footfall at several locations in the Netherlands by using counting cameras. We use these counts to validate the footfall volume automatically among other things. The data cannot be traced to individual passers-by. We do not record the images or save them. We also do not link the images to the collected technical data of a device.

2.5 Our clients only receive the results (counts) of our analysis, based on the encrypted/aggregated footfall data. Schematically:

2. 5. 1 Phase I: Processing of randomized MAC addresses of devices from pedestrians by the sensor, which encrypts and aggregates the footfall data.

2. 5. 2 Phase II: Processing of Wi-Fi signals in combination with the processing of the counts by counting cameras.

2. 5. 3 Phase III: 2nd time anonymizing the pseudonymised counts by clipping the pseudonym.

2. 5. 4 Phase VI: Analysis of the encrypted/aggregated data.

2. 5. 5 Phase V: Providing the results of our analyzes to our client(s).

3 For what purposes do we use MAC addresses?

3.1 We only process MAC addresses for conducting our analysis based on encrypted/aggregated footfall data, preparing reports for our clients, and complying with applicable laws and regulations. The analysis is reported to our clients only on an aggregated basis. This means that the data in these reports can no longer be traced back to the encrypted number (of the device's MAC address) of a pedestrian, or to the data of a device that a pedestrian carries with him. We, therefore, do not provide any personal data to our clients.

3.2 We analyze this data for the benefit of our clients to gain insight into the following data over a certain period in a certain area: the number of pedestrians.

4 Who has access to the MAC addresses?

4.1 In addition to our partners, we also engage other external service providers. These external service providers perform services for us as (sub) processors in the scope of services determined in the AVG, in the context of which personal data may be processed. Processors may only process the data as per our order and according to our instructions. We have entered into a processor agreement with each processor per the AP's security guidelines.

4.2 We may also process pedestrian data on behalf of one specific client, who independently determines the specific measurement area and the footfall data to be compiled with regard to that defined area. In that case, we will make the requested pedestrian data available encrypted, exclusively to this exclusive client. Furthermore, we will only store the encrypted data for the period specified by the exclusive client. In the event of such exclusive commissioning, this exclusive client (in

addition to, or instead of Bureau RMC, depending on the agreements made between the parties) is responsible for processing the footfall personal data in the relevant measuring area for its purposes. There are two options:

4. 2. 1 Differentiated responsibility, whereby Bureau RMC and the exclusive client are each independently responsible for processing the personal data for which they determine the purposes and means, or

4. 2. 2 Only the exclusive client is the responsible party, and Bureau RMC is the processor within the meaning of the Personal Data Protection Act.

4.3 Where appropriate, Bureau RMC, in consultation with the exclusive client, will appropriately inform pedestrians exactly how they can exercise their rights concerning the processing of personal data.

4.4 Apart from the situations mentioned in this privacy protocol, we cannot disclose the MAC addresses to others, simply because the sensor immediately encrypts these, and the original MAC addresses are never stored. Encrypted data can only be provided when we deem this necessary to comply with our legal obligations, to protect our or other people's rights, or to enforce compliance with this privacy protocol.

5 Security and retention

5.1 We have taken appropriate technical and organizational security measures to protect against loss and misuse of MAC addresses that fall under our control. For example, we irreversibly encrypt the MAC address of a device to another number. Moreover, all communication, such as between our measurement systems and servers, the access of partners to the available footfall data and the maintenance of systems, takes place via encrypted connections.

5.2 Without prejudice to the provisions elsewhere, we store encrypted MAC addresses for a maximum of 24 hours after we have obtained them. At the end of these 24 hours, we only save the aggregated and anonymous data.

6 Do you have any questions, or would you like to make use of the opt-out?

6.1 Do you have questions about how we process the MAC addresses? Then contact us.

6.2 If you do not want us to collect your MAC address, you can choose to turn off Bluetooth and Wi-Fi on your device when you visit one of our measurement areas. As of 2022, you can’t use the opt-out register, because the smartphone manufacturers have now implemented randomization on iOS and Android.

6.3 This means that a smartphone broadcasts different WiFi addresses at different locations, making WiFi tracking impossible. This makes WiFi counting completely anonymous and according to the guidelines of the AVG.

This is an English translation of the original Dutch PRIVACYPROTOCOL PASSANTENTELLINGEN. The Dutch version will prevail whenever there is a divergent interpretation between the translation and the original.