Door People Counters

3D People Counting Solution + WiFi

2018 Privacy Statement

Privacy Statement

Effective date: April 25, 2018

Overview

Door People Counter respects and upholds the privacy of every individual. We put in continuous effort in designing a system that not only complies with the current regulations in place but also goes beyond in ensuring the privacy of the individuals visiting your venues. We follow three principles in designing our system:

- We have no intention of capturing any personal information that is identifiable
- Any information we collected will be rendered anonymous through pseudonymization
- Data are kept and processed as statistical data are unable to be identified to any individual

FootfallCam adheres and maintain our compliance to the General Data Protection Regulations (GDPR) and proactively works towards greater personal data protection.

Data Protection Policy

1. Data Protection Officer

Door People Counters has appointed the Director of Software Architecture as the Data Protection Officer (DPO) who will ensure that all personal data is obtained and processed in a manner that complies with this statement and data protection laws.

2. Data Protection by Design

All IT systems, processes and applications have undergone strict assessments are reviewed in accordance with GDPR requirements. An annual data protection compliance audit will be performed to ensure an adequate level of compliance with data protection laws and GDPR.

3. Data Protection Principles

3.1 Principle 1: Lawfulness, Fairness and Transparency.

Personal Data will only be collected for one of the purposed specified in the applicable Data Protection regulation and the method of processing that will occur will be thoroughly explained to the Data Subject. By providing Personal Data, Subject consent to the use of data to fulfil the purpose of collection or as requested by Subject.

3.2 Principle 2: Purpose Limitation.

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible or exceed those purposes.

3.3 Principle 3: Data Minimisation.

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and used.

3.4 Principle 4: Storage Limitation.

In line with Principle 3, Personal Data shall be kept for no longer than necessary for the purposes outlined to the Subject.

3.5 Principle 5: Accuracy.

Personal Data which needs to be stored for a defined period of time as requested must be kept accurate and up to date, thus out of date and redundant data shall not be retained unless specified by Subject.

3.6 Principle 6: Integrity & Confidentiality.

Personal Data shall be processed and stored in a manner that ensures appropriate security of data, including protection against unauthorised processing and accidental loss, destruction or damage.

Data Processing

1. What information does FootfallCam collect and why?

When you walk with your mobile device (with its Wi-Fi function enabled) into a retail space that uses our technology, Door People Counters sensor senses the following: the presence of the device, its signal strength, its manufacturer (Apple, Samsung, etc.), and a unique identifier known as its Media Access Control (MAC) address. This combination of numbers and letters identifies a specific device to the surrounding Wi-Fi networks. Because the MAC address does not disclose the device owner's real-world identity nor any other personal data, that information is never collected.

The MAC address is hashed immediately after it is collected, the hash performed is a one-way hash and is irreversible. Our sensors collects and aggregates only anonymous data from your device into reports for retail clients. These reports are used to improve store layouts, determine shopper engagement, timing for promotions and sales, measure the effects of advertising, and set staffing levels and store hours.

Our devices areinstalled downwards facing the ground, our device only tracks the height of an individual entering and leaving the area and is unable to pickup the facial features of the individual. During normal operations, the device will only send purely statistical data to the server, and any data we collected are non-visual and will not be able to be identified with any individuals.

2. How do we collect information?

When any Wi-Fi-enabled mobile device (such as a smartphone, tablet, or computer), the WIFI SSID is turned on, it regularly sends signals to announce its presence to nearby wireless networks. Our devices can sense when Wi-Fi-enabled devices make a signal. Our devices saves the information embedded in the signal, including a device's unique MAC address. We promptly hashes the MAC addresses it collects in order to de-personalize the data, and then transmits it to a database. The data is then used to produce the reports for our retail clients. We contractually prohibit downstream recipients from attempting to use the data to identify a particular individual.

The counting of visitors to the site is done purely in the device itself and only the statistics of the visitor count is uploaded and aggregated on the server. This design has in mind the privacy of the visitors to the site and also to optimize the bandwidth of the store's network.

Door People Counters software we provide by 3rd party vendor was specially written to limit the sensor to collect only the data we need to improve client operations. At no point is your name, phone number, or any other personal information collected.

3. If our data do not contain names or other personal information, how is it useful?

Our clients use the reports that generates to answer questions such as: How many new shoppers did I have this week vs. last week? Do more people stop and enter the store with one window display vs. another? How well did my marketing campaign work? How was the shopper engagement in the store? Answering these questions requires no personal information of any kind. We only need to determine the amount of traffic that came into the store.

4. With whom do we share information?

We share information only with our clients—the retailers from whose stores the anonymous data is captured. When we provides a third party with an analysis of foot-traffic trends, it never includes device-specific data nor any names of stores included in the analysis. Only aggregated data is used.

We do not sell, rent, or otherwise disclose device-specific information to third parties. By design, our data contains no personal information nor real-world identities of shoppers; none of that data is ever collected.

5. How do we store data?

Our counters record these signals and send them to the cloud. For privacy, every MAC address will be encrypted before it is being sent and stored in the server, preventing unauthorized users from accessing to these data. Because shoppers don't need to actually connect to your Wi-Fi network or install a mobile app, you can measure their activity without interrupting their shopping experience.

Hashed data cannot be reverse-engineered by a third party to reveal a device's MAC address. This means that anyone who gains access to the database—authorized or unauthorized—would see only long strings of numbers and letters. They would be unable to get any information that could be linked to a back to a particular mobile device owner. We retain data from individually hashed MAC addresses for 24 months unless we have to keep the information for legal purposes. After 24 months, we only retain data about hashed MAC addresses in aggregate form.

6. How do we work with governments and law enforcement?

We do not respond to government requests unless we belief in good faith that a response is mandated by law. We require a warrant or court order before disclosing any of the limited amount of device location data that we possess.

7. How do we protect consumer privacy?

In an effort to protect consumer privacy, Door People Counters and vendors comply with the Mobile Location Analytics Code of Conduct. This code was established as an industry-wide standard for protecting the privacy of consumers when dealing with their mobile device data. It also defines rules of engagement for technology companies like Door People Counters and vendors to inform consumers about foot-traffic analysis and provide an easy way to opt out.

8. Can anyone opt out and delete the data that has about a particular MAC address?

Yes. You can opt out by submitting your MAC address. We will remove any existing data about that MAC address and will collect no further data about that MAC address in the future.

Our Privacy Policy may vary from time to time and all updates will be posted on this page if any changes made. FootfallCam's Data Protection Officer is responsible for accuracy and maintenance of this policy. If you have any questions or inquiries regarding our Privacy Policy, kindly send us an email to info@doorpeoplecounters.com. Thank you.