May 25th, 2021

# FootfallCam Data Privacy Policy

For FootfallCam People Counter

FootfallCam™

## Revision History

| Revision Number | Description of Revision | Date of Revision |
|---|---|---|
| 1 | Initial Draft | March 31st, 2019 |
| 2 | Revision | August 1st, 2019 |
| 3 | Initial Release | January 21st, 2020 |
| 4 | Revision and Update | May 19th, 2021 |

# Introduction

FootfallCam is committed to protecting the privacy and confidentiality of personal data of clients, business partners and other identifiable individuals. As part of this commitment, this privacy policy governs FootfallCam actions relating to the collection, use and disclosure of personal data. Each employee bears a personal responsibility for complying with this policy in the fulfilment of their responsibilities at FootfallCam.

This policy describes how the personal data must be collected, handled and stored appropriately to allow the clients to understand the rules that govern their use of the personal data which they have access to.

# Definition

In this document, the following words shall have the following meanings:

“Data Controller” means a person, company, or other body that determines the purpose and means of personal data, either alone or jointly with another person/company/body.

“Data Processor” means a person, company, or other body that processes data on behalf of a data controller.

“Data Subject” means an individual who is the subject of the personal data.

“Personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

# Scope

This policy is for clients of the Company. In this policy, “the Company” refers to the FootfallCam.

This policy applies to all personal data processed by FootfallCam. This can include:

- Names of the individuals
- Postal address
- Email address
- Telephone numbers
- *… refer **“FootfallCam Responsibilities”** for more information regarding to the collected personal data*

This policy supplements other policies relating to data protection, which includes:

- Subject Access Request Policy
- Data Retention Policy
- Access Review Policy
- Data Breach Management Policy
- Policy on Recording Action/Access Logs
- Information Security & Risk Management Policy

FootfallCam may supplement or amend this policy by additional policies and guidelines.

# FootfallCam Responsibilities

As the data controller and data processor, FootfallCam holds the responsibilities to inform the clients regarding the types of collected personal data, the methods in collecting the personal data and the reason to collect them. This is to ensure that the clients are fully understand that these personal data are necessary to be processed in order to achieve the business goal. FootfallCam is also responsible to share the precautions that have been implemented in advance to store the collected personal data securely. This is to allow the clients to understand the efforts that have been taken by FootfallCam in securing the collected personal data.

## What information will be collected?

FootfallCam will collect the following data:

- Personal Identification Information (Name, email address, company name, company code, etc.)
- Login Credentials (Username and Password)
- Media Access Control (MAC) Address
- Client's Sales Data
- File Transfer Protocol (FTP) Server's Detail
- Floor plan of the sites (where the counter will be installed)
- Short Moments of Video of up to 30 minutes from the People Counter

## How will the data be collected?

Information is collected in a number of ways including but not limited to:

- Most of the data is provided directly by the clients to our company. This will occur when the clients:
    - Fill in the details of the company on the web-based control panel
    - Create user account along with user details on the web-based control panel
    - Upload the sales data on the web-based control panel
    - Fill in the detail of the consumers' FTP server on the web-based control panel
    - Upload the floor plan directly on the web-based control panel
- FootfallCam will also receive the data indirectly from the following source(s):
    - Installed people counter provided by FootfallCam; This will occur when:
        - The counter scans the MAC addresses in its surroundings, which are hashed and stored inside the counter before transferring to FootfallCam database
        - The counter records short moments of video of up to 30 minutes according to the schedule, which are transferred to the FootfallCam file server afterwards.

## How will the information be used?

The data stated above requires to be collected so that we can:

- The Personal Identification Information (PII) is required to identify and distinguish every client.
- The collection of the MAC addresses can be used as part of the FootfallCam Analytics Reports through the data aggregation techniques, so that the generated reports can be useful for the clients to make business decisions or plans to manage and improve their own business effectively.

- The detail of the FTP server is required so that the clients' sales data can be uploaded to FootfallCam file server and the FootfallCam data can be exported to client's FTP server. Client's sales data will be used as part of the data in generating reports for the clients to make business plans or decisions.
- Email address is required to receive generated reports automatically (Individual on the client side with administrator privilege in the web-based control panel is able to configure the groups and users to receive the reports).
- The password will be used as one of the security mechanisms to allow only authorised user from accessing the web-based control panel.
- The floor plan of the site is required to ensure the accuracy of the generated reports is not affected by any external factors, so that the clients can make a more accurate business plans or decisions.
- The recorded videos are used by FootfallCam employees to perform the accuracy audits through calibration and tuning, so that the People Counter can achieve higher accuracy.

## What is the information that will be shared?

FootfallCam will share the following data to the clients:

- FootfallCam Analytical Reports (Aggregated FootfallCam People Counter generated data and imported data such as Sales Data)
- People Counter Information and Connection Logs
- Installation Paring Key (For paring to site after People Counter Installation)
- Email Scheduler Logs
- FTP Import and Export Job Logs
- FootfallCam People Counter Verification Reports (Consists of Video Recordings)
- The Internet Protocol (IP) addresses of the FootfallCam's servers (For whitelisting purpose)

## Why IP whitelisting is necessary?

This is to ensure the following actions can be performed:

- For FootfallCam People Counter,
  - To upload the data (floor plans, sales data etc.) from the counter to the FootfallCam Cloud Server as part of the FootfallCam Analytical Reports
  - To upload the live counting data from the counter to the FootfallCam Cloud Server for Occupancy Reports
- For FootfallCam Support Team personnel,
  - To provide support and error diagnosis through remote access via the Virtual Private Network (VPN)

**Note**

For more detail regarding the IP whitelisting, please refer to https://www.footfallcam.com/Service/Download for the "**IT-Infrastructure-Setup**" document under the "**Guide**" category.

## How is the personal data stored and protected?

- The collected personal data will be stored as shown in the table below:

| Location (in FootfallCam) | Personal Data |
|---|---|
| Database | Personal Identification Information (PII) |
| | Hashed Password |
| | The detail of the FTP Server |
| | Hashed MAC Addresses with timestamp |
| File Server | Clients' Sales Data |
| | Floor plan of the sites |
| | Videos recorded from People Counter |

- **Access Control Mechanisms –** Access control mechanisms such as Page Access Control and Site Access Control have been implemented to prevent unauthorised individuals from accessing the client's personal data.
- **User Control -** Only the user with the administrator privileges on the client side is able to add, modify or delete the user accounts. FootfallCam has ***no privileges to add, modify or delete*** the consumers' user account.
- **One-way Hashing –** The MAC addresses that are collected by the installed counter will be hashed and stored inside the FootfallCam database. The data subjects are unable to be tracked as the hashing process is irreversible. Same goes to the passwords that are used by the users to enter the web-based control panel, the password will be hashed for better security purpose and stored inside the database.
- **Precaution for Forget Password –** In the circumstances where the user forgets the password for accessing the control panel, a "reset password" feature is provided so that a link will be sent to the corresponding email address for the user to reset password instead of disclosing the sensitive personal data to the user directly. This is to prevent the possibilities that the personal data might be disclosed to unauthorised parties and lead to undesirable changes.
- **NO sharing/disclosure of personal data with/to unauthorised parties –** No personal data will be shared to any individual or third party without the consent of the clients.
- **Low-resolution videos (320 x 240)** – FootfallCam People Counter is designed to be at a very low resolution of 320 x 240, which is classified as too low a resolution to be able to identify any individual, not to mention the counter is installed on the ceiling and facing down towards the ground.

# Subject Access Request Policy

Subject Access Request Policy is to ensure that the clients are fully aware of all the available data protection rights.

All individuals who are the subject of personal data held by FootfallCam are entitled to the following:

- **The right to access –** The client has the right to request FootfallCam for copies of his/her personal data. *(A small fee for this service may be charged.)*
- **The right to erasure –** The client has the right to request FootfallCam to erase his/her personal data, under certain conditions.
- **The right to data portability –** The client has the right to request FootfallCam to transfer the data that was collected to another organization, or directly to the consumer, under certain conditions.

- **The right to be kept up-to-date –** The client has the right to be informed how to keep the product/service up-to-date and how FootfallCam is meeting its data protection obligations.

# Data Retention Policy

## Introduction

This policy is to outline how the reports, documents, personal data and any other related data will be retained in FootfallCam.

## The Description for Data Retention

| Types of personal data | Retention Time Period |
|---|---|
| Personal Identification Information (PII) | Permanent * |
| Hashed Password | Permanent * |
| The Detail of the FTP Server | Permanent ** |
| Clients' Sales Data | Permanent ** |
| Floor Plan of the Sites | Permanent unless deleted by users with administrator privileges |
| Hashed MAC Address with Timestamp | 30-Days |
| Videos Recorded from People Counter (Unverified Footages, Verified Footages, Verified Footages (used in FootfallCam Analytics Reports)) | • Unverified Footages – 14-days<br>• Verified Footages – Permanent unless deleted by users with administrator privileges<br>• Verified Footages (used in FootfallCam Analytics Reports) – Permanent ** |

**Note**

- **Permanent *** – Soft Delete; This type of data will still be retained in the FootfallCam database after deleted from the client side *(the client can request for data deletion as stated in **Subject Access Request Policy**).*
- **Permanent **** – This type of data cannot be deleted from the client side. It can only be deleted by FootfallCam employees upon client's request. *(refer to request for data deletion as stated in **Subject Access Request Policy**).*

# Access Reviews Policy

## Introduction

Access Review is a control activity that assures the users has the appropriate privileges to access the essential resources in the system.

FootfallCam has the obligation to ensure the client data to be kept secure and protected. However, the cooperation of customers is required to come to success in implementing a successful access review to control the access to the resources appropriately.

## Scope

This policy is for clients of the Company to understand the responsibilities of the FootfallCam and the client in implementing a successful access review to ensure that only essential privileges or activities are allowed in the FootfallCam-related resources.

In this policy, “the Company” refers to the FootfallCam.

## FootfallCam Responsibilities

To secure the integrity and confidentiality of the client data, FootfallCam has the obligation to provide essential privileges to the authorised users (including systems, applications and databases) based on the following principles:

- Need to Know – Users or resources will be granted access to systems that are necessary to fulfil their roles and responsibilities
- Least Privileges – Users or resources will be provided with the minimum privileges necessary to fulfil their roles and responsibilities

FootfallCam has the responsibilities to ensure that the application and service accounts will be used by application components requiring authentication. Besides, FootfallCam will ensure that accessing to the password will be restricted to authorised IT administrators or application developer **only**. The password will be stored and handled in accordance with the “**Password Policy**” *(refer Password Policy for more detail)*.

### Registration of new users

After the client has bought at least one FootfallCam counter from FootfallCam reseller or FootfallCam directly, FootfallCam will open an administrator account for the client based on the information provided to access the FootfallCam control panel upon successful review and approval.

FootfallCam will have **ONE** account for the FootfallCam-related employees to access the client’s control panel and information for assisting and troubleshooting purpose **ONLY**. FootfallCam **does not** hold the privileges to **create, modify** or **delete** any client-related data **without the client’s consent**.

### Removal of users

Upon the confirmation that the client has decided to discontinue our products/services, FootfallCam will **disable** the access to the client’s FootfallCam-related application (including systems, applications and databases) **within 24 hours**.

Please be noted that FootfallCam will only **disable the accounts from accessing the FootfallCam-related application and resources (soft delete)**, FootfallCam does not hold the privileges to delete the client data unless requested by the client. Please refer to “**Data Retention Policy**” and “**Subject Access Request Policy”** respectively for more detail.

## Client Responsibilities

As mentioned in the "**FootfallCam Responsibilities**", FootfallCam does not have the privileges in creating, modifying or deleting any client-related data without the client's consent. Hence, it is critical for the client to cooperate with FootfallCam as the client will be handling the accessing to most of their own resources, especially the user management. Only the user account that is assigned with the administrator privileges will be able to **create**, **modify** or **delete** the administrator account or normal user account.

It is recommended for the client to perform access reviews **at least once a year** to ensure that the authorised users are able to access the FootfallCam-related resource with essential privileges at that moment.

FootfallCam has provided a guideline on performing access reviews so that the client can gain a basic idea in protecting their own data as listed below:

1. **Classifies the business owners of every application**
   The client should assign at least one representative to manage the users that will be accessing each FootfallCam resources (including counters, applications and databases) to simplify the process in user management. Through this process, the client will be able to gain a clearer overview on the people that will be involved inside.

2. **Creates two lists; One for the approved departments and other one for rejected departments.**
   These two lists will give an overview on the given privileges and the restricted privileges for each user in accessing or using the FootfallCam-related resources. This process will help in the next access review as it can give the person in charge a quick overview whether to remain or modify the permissions.

3. **Informs the related people (both the approved departments and rejected departments)**
   After the list is created or modified, the person in charge should inform the related people so that they can know their rights in accessing or using the FootfallCam-related resources.

The guideline above is **OPTIONAL** for the client to follow as it aims to guide the user in simplifying the user management, it would be the best if the client has their own procedure in managing user management. Please be noted that FootfallCam **does not** have the privileges to manage the client's user accounts or any client-related data, therefore, it is suggested that the client will implement an appropriate procedure or mechanism to protect own resources.

# Data Breach Management Policy

## Introduction

A personal data breach refers to a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

As the data controller and data processor, FootfallCam collects, holds, processes and shares large amounts of personal data. Therefore, FootfallCam has the obligation to ensure that the collected personal data are kept secure and protected appropriately.

## Purpose

The purpose of this policy is to ensure that:

- Personal data breaches are detected, reported, categorised and monitored consistently.
- The individuals who are involved in the personal data breach incident will be informed without undue delay.
- Decisive action will be taken to reduce the impact of a breach.
- Improvements will be implemented and communicated to prevent recurrence or future incidents.

# Training, Auditing & Monitoring

Training

- All FootfallCam employees will be trained to handle and process the collected personal data appropriately and securely. This is to prevent the situations of personal data mishandling by the FootfallCam employees.

Auditing & monitoring

- Methods of collecting, holding and processing personal data will be regularly evaluated and reviewed. All employees working on behalf of FootfallCam will be made fully aware of both their individual responsibilities and FootfallCam responsibilities.

# FootfallCam Contact Information

If you have any questions about FootfallCam privacy policy, the collected personal data, or you would like to exercise one of your data protections rights, please do not hesitate to contact us.

| | |
|---|---|
| **Email:** | support@footfallcam.com |
| **Telephone no.:** | +44 (0) 1344 937275 |
| **Address:** | 46 Abbotswood, Guildford, GU1 1UY, United Kingdom |