Anonymised Data & GDPR Exemption

F100361-01

FootfallCam™

Topic	Description
Target Audience	FootfallCam customers who are concerned that the use of the FootfallCam system will affect their organisation's GDPR compliance.
Scope of the document	• Overview of the purpose of the document. • Overview of the GDPR and its scope. • Reason why FootfallCam is exempt from the GDPR. • Steps taken for FootfallCam to be exempt from the GDPR. • Steps taken for FootfallCam to mitigate the risk of anonymised data being identified until it is remote. • Identify the need for a DPIA with the DPIA checklists provided by the Information Commissioner's Office (ICO).
Notes	A GDPR exemption document for FootfallCam.

Revision History

Revision Number	Description of Revision	Date of Revision
1	Initial Draft	15th June 2016
2	Revision	21st August 2016
3	Initial Release	9th February 2017
4	Revision and Update	20th December 2019
5	Update of Graphics	24th March 2020

Contents

Chapter 1: The Purpose of This Article

FootfallCam uses new technologies such as 3D depth maps and Wi-Fi tracking to perform people counting activities so that our clients can plan their own business strategies based on the collected data, which is aggregated and shown in summary form. With the new technologies that are used by FootfallCam, it is natural for people to be concerned that incorporating our technologies in their retail space will give rise to the risk of exposing collected personal data, which would go against the GDPR if the data breach was not handled properly. All in-house developed FootfallCam products excluding COTS (commercial off-the-shelf) are exempted from the GDPR.

We put continuous effort in designing our system and data processing activities to be exempt from the GDPR by default. This does not only protect the privacy of the individual visiting the venues installed with our technologies, but also ensures that the use of the FootfallCam system does not affect our clients' GDPR compliance. The aim of this article is to explain why we only collect, store and process anonymised data instead of personal data to accomplish our objective and why we are exempt from the GDPR.

Chapter 2: What is the GDPR and its Scope

2.1 What is the GDPR?

The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. It poses obligations onto organisations anywhere, as long as they target or collect data related to people in the EU. As stated in 'What is GDPR, the EU's new data protection law?' by the GDPR official authority:

...if you process the personal data of EU citizens or residents, or you offer goods or services to such people, then the GDPR applies to you even if you're not in the EU.

The primary purpose of the GDPR is to act as a standardised data protection law to protect the data privacy of EU residents, and simplify the regulatory environment for international business by unifying data protection regulations within the European Union.

2.2 Types of Data in GDPR Terms

This section will explain the types of data as stated in the GDPR, which are personal data, pseudonymised data and anonymised data. It will also highlight the type of data that is collected by FootfallCam, which is the hashed Media Access Control (MAC) address, that can be categorised as anonymised data.

2.2.1 Personal data

2.2.1.1 Definition

In Article 4, Subsection 1, the GDPR states:

'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;

2.2.1.2 FootfallCam does not collect any personal data

We do not keep any Personally Identifiable Information (PII) that could potentially be used to identify a particular person during the people counting activities.

2.2.2 Pseudonymised data

2.2.2.1 Definition

In Article 4, Subsection 5, the GDPR states:

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

2.2.2.2 Wi-Fi Media Access Control (MAC) address

A MAC address is a hardware identification number that uniquely identifies each device on a network. The MAC address is manufactured into every network card, such as an Ethernet or Wi-Fi card, and therefore cannot be changed.

According to the statement from Article 4, Subsection 5, if the processing of personal data requires the use of additional information to attribute the personal data to an identified or identifiable natural person, it will be considered as 'pseudonymisation'. Although a MAC address is a unique identifier to identify the device, it is not categorised as 'personal data' because we will not be able to identify a certain individual without the use of additional information. A MAC address is tied to a device, NOT to the person. This means the MAC address does not disclose the device owner's real-world identity nor any other personal data without the use of additional information, such as the device holder's name. This means that without additional information such as the details of the SIM card and the registered account holder from the phone company (which are categorised as 'confidential information' by the phone company), it is nearly impossible to identify a certain individual with the MAC address only.

2.2.2.3 FootfallCam does not collect pseudonymised data

When you walk with your mobile device (with its Wi-Fi function enabled) into a retail space that uses our technology, FootfallCam 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.

The MAC address (pseudonymised data) is hashed immediately using a one-way hash function after our FootfallCam has scanned the original MAC address, turning the MAC address into anonymised data. Only the hashed values will be collected and transferred to our FootfallCam database. As we do not require the original MAC address (pseudonymised data) to achieve our objective, we DO NOT collect any pseudonymised data.

This security mechanism is applied as an additional security layer to turn the data into anonymised data that cannot be used to identify a natural person anymore. The process is irreversible as it uses a one-way hash function (for more details, please refer to 'Anonymised Data' in 'Types of data in GDPR terms').

2.2.3 Anonymised data

2.2.3.1 Definition

In Recital 26 the GDPR defines anonymised data as:

...information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

2.2.3.2 One-way hashed MAC address & data aggregation

A one-way hash function is used to hash the MAC address, converting it into a hashed value that is irreversible. This is because the one-way hash function is designed in such a way that it is difficult to reverse the process, that is, to find the original string that has been hashed to a given value, and thus it is called 'one-way'.

Aggregated data (or data aggregation) is the process of gathering data and presenting it in a summarised format. The data may be gathered from multiple data sources with the intent of combining these data sources into a summary for data analysis, which can be useful for everything from finance or business strategy decisions, to product, pricing, operations, and marketing strategies. As the aggregated data will only be shown in a summarised format, the report should not contain any device-specific data nor individual-specific data. This allows the data aggregation technique to act as an additional security layer on top of the anonymised data to secure any collected data.

2.2.3.3 FootfallCam only collects anonymised data

FootfallCam has implemented the one-way hash technique to hash the MAC address, making it irreversible with the one-way hash and turning it into 'anonymised data'. This anonymising technique was added as an additional security layer to minimise the potential risk of exposing the MAC address that could possibly be associated to a certain individual. This technique makes it possible for FootfallCam to collect only anonymised data when achieving our objective to perform people counting activities and securing the MAC address (pseudonymised data) of a device at the same time.

Besides, we do not share any device-specific data to our clients - the retailers from whose stores the anonymous data is captured. From business and security perspectives, FootfallCam has added another measure by implementing the data aggregation techniques to summarise the information and only shows aggregated data to our clients. This ensures that, while we are able to deliver the content that our clients want effectively, the privacy of the shoppers is also protected.

2.3 Anonymised Data is Exempt from the GDPR

2.3.1 An organisation is exempt from the GDPR if they only process anonymised data

As stated in Recital 26 by the GDPR:

...The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

This means, if an organisation only processes anonymised data, then they are exempt from the GDPR as anonymised data is no longer able to be used to identify the data subject. The article named *Anonymisation:*

managing data protection risk code of practice that is provided by the Information Commissioner's Office (ICO) has further defined how anonymised data is exempt from the GDPR. As stated in the article:

There is clear legal authority for the view that where an organisation converts personal data into an anonymised form and discloses it, this will not amount to a disclosure of personal data. This is the case even though the organisation disclosing the data still holds the other data that would allow re-identification to take place. This means that the DPA no longer applies to the disclosed data, therefore:

- *there is an obvious incentive for organisations that want to publish data to do so in an anonymised form;*
- *it provides an incentive for researchers and others to use anonymised data as an alternative to personal data wherever this is possible; and*
- *individuals' identities are protected.*

Chapter 3: Why is FootfallCam Exempt from the GDPR?

3.1 Only Anonymised Data is Collected

3.1.1 Non-identifiable data:

1. 3D depth maps for people counting activities
2. Recorded videos and low-resolution live views for accuracy audits
3. Hashed MAC addresses

3.1.2 Aggregated data, including but not limited to:

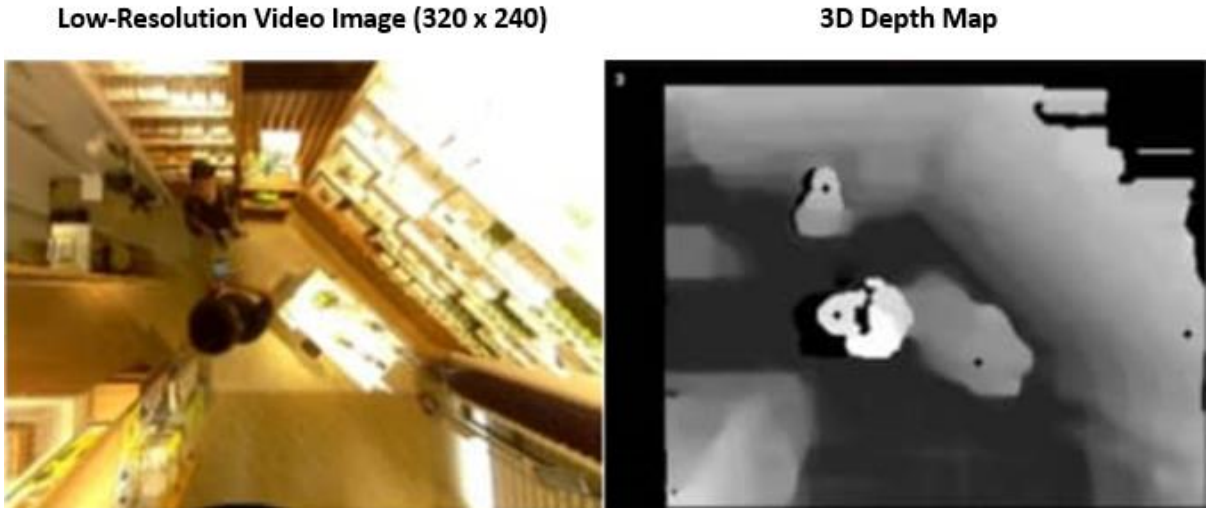
1. Number of visitors,
2. Rate of outside traffic in hourly instalments,
3. Queue counting,
4. Heatmaps,
5. Number of returning customers,
6. Occupancy rates *etc.*

Chapter 4: How is FootfallCam Exempt from the GDPR?

4.1 Video

4.1.1 Using the 3D depth map instead of video images for counting purposes

The 3D depth map is a technology that is used in 3D computer graphics and computer vision. It is comprised of grey pixels and contains information relating to the distance of the surfaces of scene objects from a viewpoint, as shown in the right side of the diagram below:



This 3D depth map technique is used by FootfallCam to track movement and perform the counting activities, which is far more accurate than using the 2D image (as shown in the figure on the left) only.

3D depth map counting is used for the purpose of counting visitors purely in the device itself and only statistics of the visitor count will be uploaded and aggregated on the server. This process is performed to determine the amount of traffic that comes into the store only, and the aggregated data is served as statistical reports for our clients to plan business strategies. It is hardly to be recognised as identifiable data as we ONLY record the numbers of the visitor count, instead of the personal data of each individual that comes into the store. As the people counter is installed on the ceiling, it is improbable for the video to capture the entirety of consumers, nor does it recognise facial features of consumers. Please be noted that FootfallCam does not function as Closed-Circuit Television (CCTV); it only records short moments of video of up to 30 minutes, for the purpose of accuracy audits to compare manual people counting against systematic counting. NO videos are captured by FootfallCam afterwards to guarantee complete consumer privacy. The 3D depth map tracks the visitor count using the height of individuals entering and leaving the area only.

4.1.2 Low-resolution videos (320 x 240) for verification only

The FootfallCam is installed on the ceiling and facing down towards the ground so it is difficult for the video to capture the entirety of consumers, nor does it recognise facial features of consumers. However, some might still have doubts as to the chances of the passer-by's face getting recorded by the camera whenever they look up to it. The following contents will be able to answer the concerns of our clients.

4.1.2.1 Video images only appear in the Live View page for checking the camera angle, and recorded videos are for verification purpose only

Although FootfallCam has implemented the 3D depth map technique to perform the people counting activities, video images ARE NOT captured NOR stored for this counting purpose. Video images will only appear in the Live View page for checking the camera angle whereas recorded videos are for verification purposes only. FootfallCam has also taken our clients' concerns about the facial features of the data subject being recorded into consideration, which is why we have implemented the following features:

These are at a very low resolution of 320 x 240, which is classified as too low a resolution to be able to identify any individual

The video images in the Live View page are used to check whether the camera position is correct and accurate, whereas the recorded videos are used to draw the configuration line to check whether the counter is counting correctly. The collected video images and recorded videos are designed to be at a very low resolution of 320 x 240, as low-resolution images and videos are sufficient for us to carry out our objective in performing the people counting activities. As stated in Recital 26 by the GDPR:

...The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Any personal data, such as the facial features of the data subjects, that cannot be used to identify or relate to a specific person is exempt from the GDPR.

Our camera is full HD (1920 x 1080) but we are using low resolution only

Although our camera is capable of recording the video footage as full HD (1920 x 1080), we use low resolution instead because high resolution is not needed for accuracy audits and verification. Most importantly, we aim to retain the resources in real-time at a high frame rate for the 3D depth map to perform people counting activities.

4.2 Wi-Fi Tracking

4.2.1 What is it used for and how do we protect the data?

Our FootfallCam product is also equipped with Wi-Fi tracking technology to perform the people counting activities. During this time, the MAC address will be detected by FootfallCam when a mobile device (with its Wi-Fi function enabled) is nearby the retail space installed with our technologies.

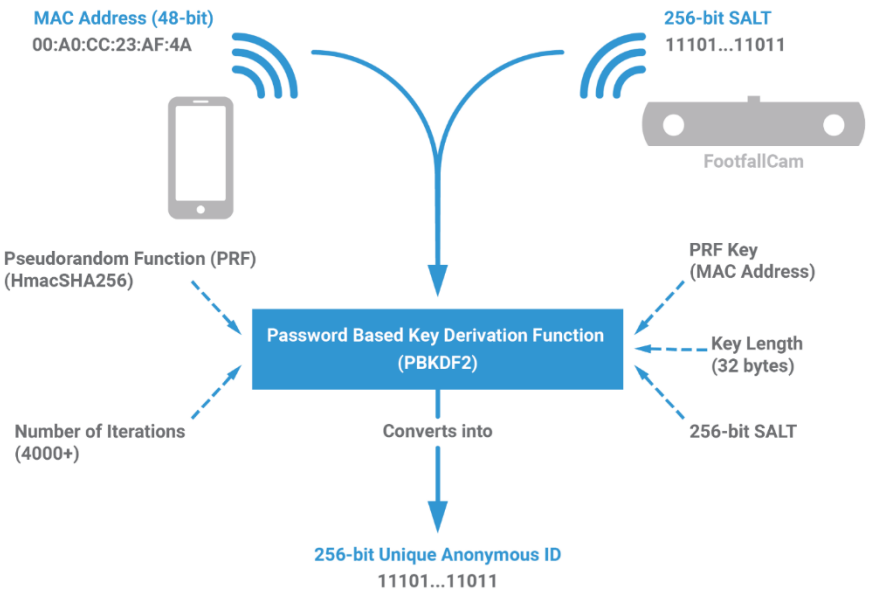
As mentioned in *Types of data in GDPR terms in the What is GDPR and its scope* section, the original MAC address is a type of pseudonymised data as the MAC address is tied to a device, NOT to a specific person. Therefore, the MAC address alone would not be able to identify the individual without additional information to link to a person (e.g. by getting the individual personal data from the phone company - but this kind of information is classified as confidential data by the phone company). To better secure the detected MAC address, we DO NOT STORE the original MAC address in our FootfallCam device. We have implemented a one-way hash function as an additional security layer to hash the MAC address, turning it into anonymised data to protect the original MAC address.

4.2.2 How do we perform the hashing?

We have used PBKDF2WithHmacSHA256 as the hashing algorithm to hash the MAC addresses.

PBKDF2, which is also called Password-Based Key Derivation Function 2, is a key derivation function that is designed as password hashing to reduce the vulnerabilities to brute force attacks in cryptography. It applies a pseudorandom function (PRF), such as hash-based message authentication code (HMAC), to the input password or passphrase along with a SALT value and repeats the process many times to produce a derived key that can be used as a cryptographic key in subsequent operations.

This hashing algorithm is implemented into FootfallCam to secure the MAC address as shown in the diagram below:



4.2.3 Is there any way to re-identify the original MAC address?

As explained, FootfallCam has implemented Wi-Fi tracking as a technique to perform the people counting activities by tracking people's movement with their device's MAC address, and this data will be hashed and aggregated into statistical reports for our clients. Some of our clients might be concerned about the risks of the original MAC addresses being re-identified, either by reverting the hashed value to the original value or through a successful brute force attack.

4.2.3.1 It is nearly impossible to match a hashed value from 281 trillion combinations of MAC addresses

An original MAC address looks something like '00:0a:95:9d:68:16'. As explained above, FootfallCam anonymises this MAC address using the PBKDF2WithHmacSHA256 hashing algorithm to generate the anonymised MAC address which looks like 'wQIPO8yUuDT08qQpPMgLydJY+NmdQabDZVdclpejmqkg='.

This one-way hashing process is irreversible, even to FootfallCam's own employees.

The only way to guess the original MAC address from its anonymised counterpart is to find a match by brute force. There are 281 trillion combinations of MAC addresses. One will first need to put all the 281 trillion possible MAC addresses through the same hashing algorithm (and that is provided one knows the exact same SALT key), and then find the corresponding match. To put it in time perspective, a standard PC will take 10-20 centuries to make these 281 trillion tries to find the match for one original MAC address (which itself is pseudonymised data).

It is therefore reasonable to say that the possibility of re-identification is remote.

Chapter 5: The Risk of Identification is Remote

According to the Information Commissioner's Office of the UK (ICO), The Data Protection Act '*does not require anonymisation to be completely risk free – you must be able to mitigate the risk of identification until it is remote.*'

5.1 It is Nearly Impossible to Identify the Person Using Low-Resolution Video

As the collected video images and recorded videos are designed to be at a very low resolution of 320 x 240, it is nearly impossible to identify or recognise the facial features of an individual, not to mention that the counter is installed on the ceiling and facing down towards to the ground.

5.2 Re-Identification of the Original MAC Address (Pseudonymised Data) is Nearly Impossible

A one-way hash function is used to hash the original MAC address into a hashed value. As its name suggests, this function only allows the original value to be hashed into an anonymised hashed value and this process is irreversible. With the current technologies, the only possibility to match the hashed value is to perform a brute force attack on the 281 trillion combinations of MAC addresses along with the same hashing algorithm and SALT value. As the hashing algorithm that we have used, which is PBKDF2WithHMacSHA256, is designed to reduce the vulnerabilities to the brute force attack (and there are a total of 281 trillion MAC addresses which might take 10-20 centuries to find an exact match), it has greatly reduced the possibilities of the original MAC address being re-identified.

Chapter 6: DPIA is Unnecessary According to ICO Checklist

According to the ICO checklists, FootfallCam **does not require** a Data Protection Impact Assessment (DPIA) as we only process anonymised data. DPIA is an assessment to help with identifying and minimising the data protection risks of a project. It is a key part of your accountability obligations under the GDPR. The DPIA which, when done properly, can help to assess and demonstrate how to comply with the data protection obligations. A DPIA must be done for processing that is likely to result in a high risk to individuals. The ICO has provided an official DPIA screening checklist as a resource to decide whether to do a DPIA. The ICO has also provided a DPIA awareness checklist as a standard to ensure that the organisation's relevant employees are well aware of the DPIA and are trained to conduct a DPIA if necessary. 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 the venues installed with our technologies. FootfallCam is aware of the need for a DPIA.

However, it is proven that our processing does not require a DPIA after completing the checklists provided by the ICO, which are the DPIA Awareness Checklist and the DPIA Screening Checklist. **For more details, please refer to the DPIA Awareness Checklist and DPIA Screening Checklist below.**

6.1 DPIA Awareness Checklist

- ✓ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.
- ✓ Our existing policies, processes and procedures include references to DPIA requirements.
- ✓ We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.
- ✓ We have created and documented a DPIA process.
- ✓ We provide training for relevant staff on how to carry out a DPIA.

We will also ensure that our relevant staff have the resources and awareness to identify the need of a DPIA for our products.

6.2 DPIA Screening Checklist

- ✓ We consider carrying out a DPIA in any major project involving the use of personal data.
- ✓ We consider whether to do a DPIA if we plan to carry out any other:
  - ☐ Evaluation or scoring;
  - ☐ Automated decision-making with significant effects;
  - ☐ Systematic monitoring;
  - ☐ Processing of sensitive data or data of a highly personal nature;
  - ☐ Processing on a large scale;
  - ☐ Processing of data concerning vulnerable data subjects;
  - ☐ Innovative technological or organisational solutions;
  - ☐ Processing that involves preventing data subjects from exercising a right or using a service or contract.

We are not involved in any of the activities stated above as our FootfallCam data processing activities do not need to process any of the individual's personal data.

- ✓ We always carry out a DPIA if we plan to:
  - ☐ Use systematic and extensive profiling or automated decision-making to make significant decisions about people;
  - ☐ Process special-category data or criminal-offence data on a large scale;
  - ☐ Systematically monitor a publicly accessible place on a large scale;
  - ☐ Use innovative technology in combination with any of the criteria in the European guidelines;
  - ☐ Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
  - ☐ Carry out profiling on a large scale;
  - ☐ Process biometric or genetic data in combination with any of the criteria in the European guidelines;
  - ☐ Combine, compare or match data from multiple sources;
  - ☐ Process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
  - ☐ Process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
  - ☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
  - ☐ Process personal data that could result in a risk of physical harm in the event of a security breach.

None of the activities above are in line with the FootfallCam product as FootfallCam only collects and processes anonymised data during the data processing activities.

- ✓ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.
- ✓ If we decide not to carry out a DPIA, we document our reasons.

Based on the DPIA Screening Checklist, we do not fulfil any of the data processing activities stated above. This is because we do not collect or process the personal data of any individual. Instead, we only store and process anonymised data to accomplish our objective. As stated in Recital 26 by the GDPR:

...The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

At the present stage, our FootfallCam product does not require a DPIA because only anonymised data is processed instead of personal data. However, FootfallCam still follows rules to achieve data minimisation and implements security mechanisms to ensure the risk of identification is able to be mitigated until it is remote.

FootfallCam will review our data processing activities periodically, especially when introducing a new data processing procedure, to ensure we are able to secure the privacy of the data subject while accomplishing our objectives at the same time. If we find out that our new data processing activities are involved in the scope of the DPIA Screening Checklist, we will take action to ensure it is compliant with the GDPR and carry out a DPIA if necessary.

Chapter 7: Future Updates

Our Privacy Statement may vary from time to time and all updates will be posted on this page if any changes are made. This statement is maintained and reviewed periodically to reflect the updated privacy laws and GDPR compliance. The FootfallCam Data Protection Officer is responsible for the accuracy and maintenance of this policy. If you have any questions or enquiries regarding our Privacy Policy, kindly send us an email at support@footfallcam.com