tapestry

COACH | kate spade | STUART WEITZMAN

Employee CCTV Policy

Policy Overview

This policy applies to Coach Stores Limited, a private limited company incorporated in England and Wales, and all of its subsidiaries operating in the European Union, Switzerland and the United Kingdom (collectively "we" or "us" or "our" or "Company"). We utilize Close Circuit Television ("CCTV") in order to maintain a safe and secure environment at our workplaces, including Coach, Kate Spade and Stuart Weitzman stores, warehouses and offices. Whenever our CCTV cameras capture an individual, the captured image will be that individual's personal data provided they are identifiable from it ("CCTV Data"). Your employer is a "data controller" in relation to CCTV Data. As a data controller, the Company reasonably determines how and why CCTV Data is used. We are required to process CCTV Data in compliance with applicable data protection laws. This policy is intended to assist you to comply with these legal obligations. We also want to inform those individuals that may be captured by CCTV recording about how we use their CCTV Data.

Table of Contents

SCOPE

European Union and European Economic Area

POLICY SECTION

CCTV Policy v1.0

ISSUED BY

Tapestry Privacy Office

DEPARTMENT/SUB-FUNCTION

N/A

DATE ISSUED

February 4, 2020

EFFECTIVE DATE

February 4, 2020

SUPERSEDES ISSUE DATED

N/A

Employee CCTV Policy

1. Introduction

This policy seeks to ensure that the CCTV used at Company workplaces complies with applicable data protection and privacy laws (including the European Union General Data Protection Regulation ("GDPR")) and includes the principles governing the processing of personal data. Company uses CCTV only where it is necessary in pursuit of a legitimate interest that does not outweigh the interest that individuals have in their right to privacy.

This policy covers all Company employees, directors, contractors, interns and agency workers (collectively referred to as "employees"). We may amend this policy at any time.

A breach of this policy may, where appropriate, be treated as a disciplinary matter. Following an investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

2. Responsible Parties

This policy will be reviewed annually by a Company security manager from Loss Prevention ("Security Manager"). Company has overall responsibility for ensuring compliance with the relevant laws and the effective operation of this policy. The Privacy Office will inform the Security Manager of changes to applicable laws or guidance provided by the relevant authorities that may affect this policy. Store management and keyholders ("Authorized Personnel") are responsible for CCTV Data at each workplace, and have day-to-day management responsibility for CCTV Data. Authorized Personnel are responsible for following the Security Manager's guidance on what information is recorded, how it will be used and, in certain circumstances, to whom it may be disclosed. Any matter requiring the permission or approval of your Security Manager may also be permitted or approved by the Privacy Office, which can be contacted at Privacy@Tapestry.com. To find out who the keyholder is for your workplace, please contact the Security Manager at RetailEuropeLossPrevention@Tapestry.com.

3. Use of CCTV Data

Company has a legitimate interest in the CCTV monitoring that it carries out for the following reasons, which we call the "CCTV Monitoring Purposes":

- Promote a safe and secure working environment for employees and customers.
- Assist in the investigation of material breaches of Company's policy and procedures.
- Assist in the prevention, investigation and detection of crime, with a primary focus on loss prevention of Company merchandise.
- Assist in the apprehension and prosecution of offenders, including use of CCTV Data as evidence in criminal proceedings.
- Support employees and customers, and where relevant and appropriate, to investigate complaints.
- Otherwise, to comply with a legal obligation under applicable laws.

4. Location of CCTV

Employee CCTV Policy

Cameras are in plain view and do not capture audio recordings. Where required by law, signs are placed at entrances and at clearly visible locations within each workplace alerting employees and other individuals that CCTV is in use. If you believe that adequate signage is not present at your workplace, please follow the process outlined in the Complaints Procedure section, below. Under no circumstances should recordings take place in employee rooms, changing rooms, toilets, shower rooms or any other areas designated as employee rest areas, without the express prior written permission of the Security Manager and Privacy Office.

5. Who Handles CCTV Data?

Only Authorized Personnel are permitted to monitor CCTV Data. Non-Company employees are never permitted to view CCTV Data without express prior written consent from the Security Manager. Non-Company employees that view CCTV Data are generally limited to law enforcement and, in limited circumstances, our CCTV supplier. CCTV is not monitored continuously and is only viewed when necessary for any of the CCTV Monitoring Purposes. Authorized Personnel are given appropriate training to ensure they understand and observe this policy and the relevant legal requirements that underpin it.

6. Disclosure of CCTV Data

a. Internal Disclosure

No CCTV Data should be shared internally by Authorized Personnel at the relevant workplace without the express prior written permission of the Security Manager. CCTV Data is only viewed when required for any of the CCTV Monitoring Purposes.

Company will only use CCTV Data for internal investigations where it is appropriate to do so. Examples of such situations include incidents of theft or other criminal acts. The Security Manager may review CCTV Data and/or create a copy to show to another individual as part of any such investigation. It is possible that a copy of CCTV Data may become a part of an employee's case file following an investigation and subsequently shared with law enforcement.

Internal disclosures of CCTV Data may also occur in order to comply with a legal obligation under applicable laws.

b. External Disclosure

Law enforcement may request access to CCTV Data for clearly defined purposes. If this occurs, the Security Manager or Authorized Personnel will request that law enforcement officials complete a data request form that must be reviewed and signed by the Security Manager or Authorized Personnel with the approval of the Security Manager. All signed data request forms should be scanned and sent to the Security Manager. Signed forms should be uploaded to Egnyte by the Security Manager. Only after the data request form is complete, Authorized Personnel or the Security Manager may provide law enforcement with a copy of CCTV Data in question. In certain limited circumstances, our CCTV supplier may assist employees in this regard. CCTV Data is not shared with any other external parties, save where necessary to comply with a legal obligation under applicable laws.

Employee CCTV Policy

Note: the processing of personal data by competent authorities for purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, falls under the directive EU2016/680 and is distinct from the CCTV monitoring that is conducted by the Company.

7. Retention of CCTV Data

CCTV Data is not retained for longer than necessary, taking into account the purposes for which they are being processed. CCTV Data is automatically stored in a digital form, with historical data overwritten in chronological order.

Provided that there is no legitimate reason for retaining the CCTV Data such as for use in disciplinary and/or legal proceedings, the CCTV Data will be erased following the expiration of the relevant legal retention period. All retained CCTV Data is stored securely.

8. Complaints Procedure

Any complaints relating to the CCTV system should be directed, in writing, to the Security Manager or the Privacy Office as soon as possible and in any event no later than one month from the date of the incident giving rise to the complaint. A complaint will be responded to within a month following the date of its receipt. If additional time is required to respond to a complaint, the complainant will be notified of this in a timely manner. Records of all complaints and any follow-up action will be maintained by the relevant office (e.g. the Privacy Office or Security Manager).

9. Contact

To find out more about how we process personal data generally, you can find our privacy notices for Company employees by visiting the Privacy page on the Loop. Our public privacy notices can be accessed on any Company website.

If you have concerns or questions regarding this policy, please contact the Security Manager at RetailEuropeLossPrevention@Tapestry.com and the Privacy Office at Privacy@Tapestry.com.

Additional privacy and information security-related information may be found on the Privacy Office and IT Security page on the Loop. Company has the right with or without notice in an individual case or generally, to change any of its guidelines, policies, practices, working conditions or benefits at any time.