SAMPLE DASH CAMERA POLICY DOC

Introduction

The Company uses connected dash camera video to protect the Company's property and to provide a safe and secure environment for employees and the public. This policy sets out the details of how the Company will collect, use and store video and images. For more information on your privacy rights associated with the processing of your personal data collected through connected camera images please refer to the Company privacy notice and data protection policy.

The Company's dash cameras will only record images. There is no audio recording i.e. conversations are not recorded on the cameras.

Purposes of connected dash cameras.

The Company has carried out a data protection impact assessment and on the basis of its findings it considers it necessary and proportionate to install and use a connected dash camera system. The data collected from the system will assist in:

· Prevention or detection of vehicle incidents or equivalent malpractice.

· Identification of offenders in case of vehicle damage.

· Monitoring of the security of the Company's vehicles.

· Ensuring that health and safety rules and Company procedures are being complied with.

Location of dash cameras

Cameras are installed on the windscreen of the vehicle facing outwards. For some fleet vehicles a rear facing camera as the back of the vehicle may also be installed. The Company has positioned the cameras so that they only cover the outside of the vehicle. No camera focuses, or will focus, on the interior cab of the vehicle or internal rear compartments.

All cameras are also clearly visible.

Appropriate signage via stickers on the vehicle are prominently displayed so that employees, clients, customers and the public are aware that the vehicle has CCTV capabilities.

Recording and retention of images

Images produced by the connected camera equipment are intended to be as clear as possible so that they are effective for the purposes set out above. Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly and that the media is producing high quality images.

Images will be recorded when vehicle is on or can wake if a gshock event is detected.

As the recording system records digital images, any images that are held on the SD card of the camera are deleted and overwritten on a recycling basis.

Images that are stored on, or transferred on to, the cloud based system and stored digitally are erased or destroyed once the purpose of the recording is no longer relevant. In normal circumstances, this will be a period of _____. However, where a law enforcement agency is investigating a crime, images may need to be retained for a longer period.

Access to and disclosure of images

Access to, and disclosure of, images recorded on the cameras is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purposes for which they were originally collected.

The images that are filmed are recorded centrally and held in a secure virtual server location. Access to recorded images is restricted to the operators of the camera system and to those line managers who are authorised to view them in accordance with the purposes of the system. Viewing of recorded images will take place in a restricted area to which other employees will not have access when viewing is occurring. If media on which images are recorded are removed for viewing purposes, this will be documented.

Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

· The Garda and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.

· Prosecution agencies

· Relevant legal representatives.

· Line managers involved with Company disciplinary and performance management processes.

· Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

The Managing Director of the Company (or another senior director acting in their absence) is the only person who is permitted to authorise disclosure of images to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

Individuals' access rights

Under the EU's data protection laws, including the General Data Protection Regulation (GDPR), individuals have the right on request to receive a copy of the personal data that the Company holds about them, including dashcamera images if they are recognisable from the image.

If you wish to access any camera images relating to you, you must make a written request to the Company's Data Protection Officer_____. This can be done by using this email address _____. The Company will usually not make a charge for such a request, but we may charge a reasonable fee if you make a request which is manifestly unfounded or excessive, or is repetitive. Your request must include the date and approximate time when the images were recorded and the location of the particular dashcamera, so that the images can be easily located and your identity can be established as the person in the images.

The Company will usually respond promptly and in any case within one month of receiving a request. However, where a request is complex or numerous the Company may extend the one month to respond by a further two months.

The Company will always check the identity of the employee making the request before processing it.

The Data Protection Officer will always determine whether disclosure of your images will reveal third party information, as you have no right to access camera images relating to other people. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.

If the Company is unable to comply with your request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, you will be advised accordingly.

Staff training

The Company will ensure that all employees handling camera images or recordings are trained in the operation and administration of the camera system and on the impact of the laws regulating data protection and privacy with regard to that system.

Implementation

The Company's Data Protection Officer is responsible for the implementation of and compliance with this policy and the operation of the camera system and they will conduct a regular review of the Company's use and processing of camera images and ensure that at all times it remains compliant with the laws regulating data protection and privacy. Any complaints or enquiries about the operation of the Company's camera system should be addressed to _____

Data Protection

The Company will process the personal data collected in connection with the operation of the camera policy in accordance with its data protection policy and any internal privacy notices in force at the relevant time. Inappropriate access or disclosure of this data will constitute a data breach and should be reported immediately to the Company's Data Protection Officer in accordance with the Company's data protection policy. Reported data breaches will be investigated and may lead to sanctions under the Company's disciplinary procedure.