B-Cam GDPR suggested Guidance

This document is just a basic guide to help you manage the use of body worn cameras and media solutions in accordance with the GDPR. Please, note this is just a guide for basic advice, as B-Cam is not a regulation company.

First of all, as the use of this solution is related to safety, as long as the video surveillance is proportionate, consent is not required. The law requires that data collected is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that the data from such processing should be limited to what is strictly necessary to achieve a security purpose (evidence collection as a primary function).

As a user of body worn cameras solutions, you will need to respect some basic rules, to be compliant with GDPR.

In terms of general organisation

- Appoint a so-called Data Protection Officer, who will be in charge for the processing of personal data.
- Set a written Body Worn Camera Usage Policy in place, which includes reference to the collection, processing, retention, disposal and security of personal data being processed. This policy should draw up for use of the devices in a limited and defined set of circumstances only.
- Report leaks of personal data (or security breach) to the Office for Personal Data Protection (ICO, for UK) within 72 hours.
- Train your staff and make sure they comply with the GDPR rules and your policies. All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images will be required to undertake data protection training.
- If the operation of the BWCs is to be outsourced to a third-party security company, ensure the appropriate contracts are in place.

In terms of the use of camera

- Announce to the subject(s) of an encounter that video and audio recording is taking place using a body worn camera.
- Recording should only commence at the start of an incident and should terminate once the incident is concluded. Under no circumstances should recordings be used to monitor staff in their general duties.
- Make sure there is a clear signage indicating mobile image recording is in operation (this can be similar or an addition to the current CCTV signage).
- Make sure downloading of images from cameras will only be conducted by trained security staff and cameras will be cleansed following each shift.

B-Cam GDPR suggested Guidance

In terms of data management

- Use a software that automatically deletes the data collected once the task is completed (as BCMM does).
- Keep data for no longer than necessary for the particular purpose; media held in excess of their retention period should be reviewed in accordance to your internal Data Protection policies, and any not required for evidential purposes should be deleted.
- Keep data secure on your internal system and report any security breach. If you use BCMM's cloud storage, your data is covered under both the B-Cam Ltd and AWS data protection policies.
- Make sure, access to retained footage is restricted to the authorised staff only.

Any specific question or concern, don't hesitate to contact us: datacontroller@b-cam.net

For further information, consult the ICO site: https://ico.org.uk

B-CAM Ltd.