Awareness raising campaign for SMEs

Guidance on the use of Body Worn Cameras or Action Cameras

Co-funded by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

THIS PROJECT HAS BEEN CO-FUNDED FROM THE EUROPEAN UNION'S RIGHTS, EQUALITY AND CITIZENSHIP 2014-2019 PROGRAMME UNDER GRANT AGREEMENT N°874524.

Contents

Overview

The use of body worn cameras and similar devices has been growing in both scale and variety over the last number of years. They have numerous potential applications including recreation, security, and journalism, to name a few. Under the General Data Protection Regulation (GDPR), any person or organisation that collects and processes the personal data of individuals **other than in a purely personal capacity is a 'controller'**, with certain responsibilities. The use of such camera technology for purely personal, recreational purposes will also be addressed below; however, in **professional contexts**, operators of body worn cameras must **respect the obligations** conferred on them by the GDPR, in particular by carrying out their activities in accordance with the principles of data protection found in Article 5.

Wearable technologies such as body worn cameras pose a particular challenge from a data protection perspective due to their **mobile nature**. Unlike CCTV systems, which can be carefully positioned to minimise the risk of inadvertent data collection, a body worn camera effectively turns the wearer into a mobile surveillance system that is highly **likely to capture the personal data** of passers-by. When this type of technology is combined with microphones and/or facial recognition technology the data protection concerns increase. Furthermore, if the video footage is stored on the device itself or on a memory stick, there is an additional **risk of loss or theft** of personal data.

As a result, the **necessity for the use of body worn cameras** will generally have to meet a relatively **high threshold** in order to comply with data protection legislation. You must show that your use of body worn cameras is **lawful and fair**; that it is **transparent**; that your cameras only **record the minimum** amount of personal data necessary for a **stated purpose**; that any recordings are **stored securely** and **retained** only for the minimum amount of time required; and that you respond appropriately to data subject requests.

You must also comply with the relevant law enforcement legislation if you are a competent authority acting in a **law enforcement capacity**, which is discussed briefly below, although the **focus of this guidance** is on the use of these sorts of cameras in **non-law enforcement situations**.

This guidance aims to help individuals and organisations who use body worn cameras (other than in a law enforcement context) to understand their obligations under the relevant data protection legislation and complements the guidance on our website on video recording and CCTV systems.

Utilisation of Cameras Must be Lawful and Fair

All processing of personal data which does fall under the remit of the GDPR must be lawful and fair. This essentially means that you must have an **appropriate 'legal basis'**, or justification, for using body worn cameras (or similar technologies, such as 'action cameras') as required by Article 6 GDPR (see also our detailed guidance on legal bases). Further, any video footage recorded must only be processed for purposes that are otherwise lawful and fair towards affected data subjects. The use of such cameras should avoid being unduly detrimental, unexpected, misleading, or deceptive to individuals who are recorded. Data controllers should also note that it is not enough that the use of body worn cameras and action cameras would be helpful towards achieving a desired goal, but it must actually be **necessary for achieving the purpose** which provides a legal basis.

Consent is unlikely to be the appropriate legal basis where these sorts of cameras are used, where gathering the consent of each person recorded may not be possible or practical. In most situations in which body worn cameras or action cameras are routinely used, it would be very difficult to obtain the valid, freely given consent of all affected individuals.

The most appropriate legal basis for the use of body worn cameras or action cameras in many cases may be where you can show that they are **necessary to pursue a 'legitimate interest'**, either your own or that of a third party (for example, where an organisation proposes using them for a safety or security purpose, it may be the interests of clients or others which are pursued, not just those of the organisations). If controllers wish to rely on legitimate interest as a legal basis for using body worn cameras or action cameras , they must assess whether they are necessary for pursuing this interest **('necessity test')** and whether that interest is overridden by the interests or fundamental rights or freedoms of the individuals concerned **('balancing test')**. In other words, they must demonstrate that they have a genuine legitimate interest in undertaking this processing, that body worn cameras are **necessary and proportionate** for achieving the purposes of the processing, and that they will not have a disproportionate impact on the individuals concerned.

The GDPR makes clear that public authorities cannot rely on the legal basis of 'legitimate interests' to justify the processing of personal data which is carried out in performance of their tasks. However, **public authorities** may have a legal basis where "*processing is **necessary** for the performance of a **task carried out in the public interest** or in the **exercise of official authority** vested in the controller*". Where processing is based on this legal basis, it should be grounded in EU or national law, which meets an objective or public interest and is proportionate and legitimate to the aim pursued. A data controller may rely on this lawful basis if it is necessary for them to process personal data either in the exercise of official authority (covering public functions and powers as set out in law) or to perform a specific task in the public interest (as set out in law).

It is important to note that the fairness requirement does not mean that all processing that negatively affects the individual concerned is in breach of this principle. For example, video footage from a body worn camera or action camera **could be used as proof of wrongdoing** by an individual, as long as the data controller had a valid legal basis for using a body worn camera or action camera and complied with their other obligations under data protection law. The fact that this will have **negative consequences** for the individual concerned **does not make the use of the camera unfair or unlawful per se**.

Body worn cameras may also be used on the basis that they are necessary for law enforcement, as discussed below, where a similar, but separate, set of rules apply.

The Obligation to be Transparent About Recording

You must make sure that all individuals whose personal data could be captured by body worn cameras are "***informed of the existence of the processing operation and its purposes***" (Recital 60 GDPR) in a timely manner. This information must include at least the **identity and contact details** of the data controller and the controller's data protection officer where applicable; the **purposes** of the processing and its **legal basis**; information on the legitimate interest being pursued where this is the legal basis of the processing; the **recipients** of the personal data if any; and you must confirm whether you intend to **transfer** said personal data to a third country or international organisation (see Article 13(1) GDPR for full details of the information to be supplied).

The principle of transparency requires that any information addressed to the public or to the data subject be concise, **easily accessible and easy to understand**, and that clear and plain language and, additionally, where appropriate, visualisation be used.

The appropriate measures to convey this information to the data subject **depend on the specific context and environment** in which the data is collected and processed, and in the case of body worn cameras may include **visible notices** containing the information, **badges** next to equipment containing information or links, public **signage**, or otherwise declaring to or bringing to the attention of data subjects the relevant information. Other measures for providing transparency information for data controllers who maintain a digital/online presence may include the use of an **electronic privacy notice**; however, depending on the circumstances of the data collection and processing, a data controller may need to use **other, additional measures** to provide the information.

A layered approach may be followed by controllers where they opt to use a **combination of methods** while ensuring that the most important information is always conveyed in the first measure used to communicate with the data subject (such as a visible sign or badge). Controllers should also remember that the wearer or user of the camera will likely be the first or easiest point of contact for affected data subjects, and therefore should be given **appropriate training** on how to respond to queries or data subject requests. Furthermore, under Article 24(2) GDPR data controllers are required implement data protection policies, where appropriate.

More information about transparency obligations can be found on the 'Right to be informed (Transparency)' section of the DPC website. Further information on transparency is also available in the Article 29 Working Party Guidelines on Transparency.

Minimising the Amount of Personal Data Recorded

You must ensure that any personal data recorded by your body worn cameras is **adequate, relevant and limited to what is necessary** to achieve the **stated purposes** of the processing. In other words, they must **only record the bare minimum** of data needed for the stated aims of having the cameras. The DPC recommends that data controllers considering the use of body worn cameras **undertake detailed assessments** as to how the use of such equipment meets with these requirements. This could include a **risk assessment**, necessity and balancing test (particularly where relying on legitimate interests as a legal basis), and/or a **Data Protection Impact Assessment** (DPIA).

A DPIA is a process whereby an individual or organisation assesses all risks related to stakeholders involved in its data processing activities and takes steps to reduce these risks as much as possible. DPIAs are necessary where data processing "*is likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1) GDPR), and are particularly appropriate for relatively **new or invasive technologies**, such as body worn cameras. It is highly advisable for data controllers to undertake a DPIA when considering the use of body worn cameras, even where it is not strictly speaking mandatory, as they are a useful tool for ensuring compliance with data protection law.

For example, where a body worn camera records **both audio and video data**, each data stream must be considered separately and be **justified in its own right** under the principles of data minimisation and necessity in order to be permissible. Also where footage from a body worn camera or action cam is used for **more than one purpose**, each data processing activity must be considered and justified **its own right**, particularly with regard to the principles of data minimisation and necessity in order to be permissible. A DPIA undertaken by a data controller in these scenarios may determine that the processing results in the excessive processing of personal data, if it is not required for the stated purpose for which it is recorded, and would therefore not be justifiable. More information on DPIAs can be found on our website.

In line with any risk assessment or DPIA conducted, and the necessity of recording to achieve the stated purpose of the processing of personal data, data controllers should consider when it is appropriate to **switch on or off** a body worn camera to **avoid constant, and excessive, recording.** Camera operators should also provide a warning to individuals prior to starting the recording function. Cameras should only be turned on and used in a proportionate manner, for as long as it is necessary to achieve the legitimate purpose of the recording.

Storage or Retention of Recordings

Another strategy for minimising the processing of personal data is by **limiting the periods for which data is retained or processed**. You must retain recordings by body worn cameras only for the minimum amount of time necessary to achieve the stated objectives of using said cameras, and this should take into account the principle of data protection by design and default.

The law does not define a specific retention period, so you must **calculate** your own **based on clearly justifiable criteria** related to the processing activities of your organisation. You should keep a copy of your calculations, perhaps as part of your DPIA. As mentioned above, under Article 24(2) GDPR controllers are required to have data protection policies, where appropriate, and this should include a retention schedule. The length of this retention period, or how it will be determined, must also be provided to the data subject concerned as part of the data controller's **transparency** obligations.

It is **not acceptable**, however, to keep copies of recordings on a **'just-in-case' basis**. Where footage has been identified that relates to a specific incident such as the investigation of a workplace accident or that may be used as evidence in criminal proceedings, you may consider a longer retention policy. This footage should be isolated from the general recordings and kept securely for the purposes that has arisen.

Maintaining Security and Integrity of Recordings

You must have appropriate technical and organisational measures in place to ensure that all personal data captured by your cameras are **protected against authorised or unlawful processing, accidental loss, theft, destruction or damage**. You will need to assess the level of risk posed by the use of body worn cameras by your organisations and adopt measures that mitigate those risks. These measures must provide an appropriate level of **security and confidentiality** to the personal data, taking into account the state of the art measures and technology available and the costs of implementation (see Recital 83 GDPR).

A key part of these measures will be ensuring that all personal data captured by body worn cameras are **only stored in a safe format**, with limited access permissions, and for the minimum amount of time necessary to achieve the purposes of the processing (see above). The security measures should include not only cybersecurity, but also physical and organisational measures.

Data controllers should pay particular attention to whether the video footage is stored on the device itself or on a portable storage medium such as memory stick, and take steps to mitigate any additional risk of loss or theft of personal data, through both technical and organisational measures. Controllers should also **routinely check** that their security measures are up to date and effective.

As body worn cameras are likely to be issued to and used by individual users, controllers should be aware of the **importance of training these individuals** as a key security measure, and ensure the implementation of usage policies and regular review of same.

For further information on how to ensure the security and confidentiality of personal data which is collected and otherwise processed, see the DPC's guidance on data security available on our website.

Responding to Data Subject Requests

You must ensure that all personal data that you retain is **accurate and, where necessary, up-to-date**. You must take every reasonable step to rectify or erase inaccurate data as swiftly as possible, as mentioned in Article 5(d) GDPR in relation to the principle of accuracy. Individuals have the **right to access to, rectification of, and in many cases the erasure** of any recordings that contain their personal data.

The right of access applies in all circumstances subject to certain limitations such as the need to protect the rights and freedoms of third parties. The right of erasure only applies if one of several criteria under Article 17 GDPR are met, such as (but not limited to) where the personal data is no longer necessary, the personal data has been processed unlawfully, or where the data subject has objected to the processing and there are no overriding legitimate grounds for the processing.

If an individual makes an **access request** for any personal data recorded by your body worn cameras, you are obliged to **(a) confirm** whether you do retain any of their personal data; **(b)** upon request, you must **provide a copy** of their personal data along with other information. Further details on the information to be provided in response to an access request can be found on the DPC's website and FAQ on subject access requests.

You must respond to an access request **without undue delay** and at the latest within one month of receipt of the request – this may be extended by two further months, depending on the

complexity of the request, but only where necessary and justified. You may ask for clarification if the nature of the request is unclear.

You must provide the required information and a copy of the data subject's personal data **free of charge**, unless additional copies are requested, in which case a reasonable fee based on administrative costs may be charged. Further, in very limited cases where a request is 'manifestly unfounded or excessive', you may charge a reasonable fee, based on administrative costs, or even refuse to act on the request.

Where **images of third parties**, individuals other than the requesting data subject, appear on the recording the data controller needs to consider, on a case-by-case basis, whether the release of the unedited footage 'adversely affects' the rights or freedoms of the third parties, such as their data protection rights, trade secrets, or intellectual property rights such as copyright. The controller needs to conduct a balancing test between the right of the data subject (requester) to access his or her personal data as against the identified risk to the third party that may be brought about by the disclosure of the footage. The GDPR notes that these considerations should not result simply in a refusal to provide all relevant information to the data subject. Where necessary, measures may include pixelating or otherwise de-identifying the images of other identifiable parties before supplying a copy of the footage to the requester.

If an individual makes a valid **erasure request**, you must respond within the same timeframe as an access request and pass on the erasure requests to all recipients of said data subject's data, unless this is impossible or would involve disproportionate effort. More information on erasure requests can be found on the DPC's website.

Action Cameras and Personal Use Exception

Another technology similar to body worn cameras, or indeed simply a different application of the same technology, is the **recreational use** of what are commonly referred to as **'action cameras'** – digital cameras designed for recording action while taking part in it. These cameras are typically worn or mounted in such a way that it can shoot from the point of view of the user, such as by mounting on a helmet, bicycle, or even a drone.

These technologies function very similarly to body worn cameras, which are generally used in a commercial context; however, whether or not data protection law applies to the use of action cameras will very much depend on the purpose and nature of the use of those cameras – in short, it will **generally not apply** where they are used **purely for personal recreational purposes**.

Individuals who use or intend to use action cameras or body worn cameras in a public place should consider whether or not the recording falls under the **'personal' or 'household exemption'** from the GDPR (see Article 2(2)(c) and Recital 18 GDPR). This exemption states that the GDPR does not apply to processing of data (such as recording video) by an individual "in the course of a purely personal or household activity". If the recording does not fall within this category, then it is possible that the person making the recording has the obligations of a data 'controller' under the GDPR, as set out above.

When assessing whether or not recording is of a purely personal or household nature, users should ask themselves a number of questions, such as:

- ☑ Does it have any **connection** to a **professional or commercial activity**;

- ☑ **Who** were the people **involved** in or captured by the recording – were they known to the person making the recording; and
- ☑ **What area** did the recording cover – did it cover **public or only private** spaces.

A case from the Court of Justice of the European Union (CJEU) assists in understanding the extent of this exemption, making it clear that this exemption must be **interpreted narrowly**. In its judgment in the case of Rynes vs Urad (2014), the Court noted that:

> To the extent that video surveillance… covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity…

Although this case related to a fixed CCTV surveillance system and depended on the specific facts of that case, it is still helpful in assessing whether the exemption applies in cases where individuals are using other types of video recording equipment, such as action cameras. Where **filming in a public place** it may be **harder** to **establish** that the use of such cameras was **purely personal**.

Similarly, where the resulting footage is **published online**, the degree to which it is made **available to the public at large** may also impact whether or not it can be considered 'purely personal'. The publishing of personal data captured by these cameras online could be considered to be processing of personal data, even if the original filming fell within the personal or household exemption. The CJEU has indicated that an individual may still assume the responsibilities of a controller under the GDPR, depending on what they do with the personal data of others that they have collected. For example, in the Bodil Lindqvist (2003) case, the CJEU held that the personal exemption did not apply where an individual **posted content online** which was accessible to an **"indefinite number of people"**.

Therefore, two key questions for users of these sorts of cameras, when determining whether data protection obligations apply to them, as part of the general assessment of whether the use of the camera is 'purely personal', are **(a)** how public the **filming** of the footage was, and **(b)** how public the **publication** of that footage was. Ultimately, whether or not a recording was of a purely personal nature will depend on the **facts of each case**.

Rules for Recordings Made for Law Enforcement Purposes

Data processing that is carried out by a **competent authority for law enforcement purposes** falls **outside the scope of the GDPR** and is covered instead by the **Law Enforcement Directive (LED)**, transposed into Irish law by the Data Protection Act 2018, in particular by Part 5 of that Act. Many of the same principles, obligations, and rights which are discussed above are also contained in the LED and Part 5 of the Act, but are outside the focus of this guidance note.

The term 'competent authority' can apply to a **wide range of public and private organisations**: in addition to law enforcement authorities such as An Gardaí Síochána, it can also encompass municipal authorities carrying out a law enforcement function (e.g. prosecuting speeding offences, littering etc.), and even private organisations contracted to carry out a law enforcement function on behalf of a public authority. However, processing carried out by a law enforcement authority for **non-law enforcement related purposes** (e.g. administration) will **still fall under the GDPR**.

If your use of body worn cameras meets the above criteria (i.e. you are a competent authority undertaking for the purpose of carrying out a law enforcement function as defined in Section 70 of the Act) then your activities may fall under the scope of the LED. Although the focus of this

guidance is on explaining the provisions of the GDPR, in essence **similar data protection principles apply** in the case of the LED and Part 5 of the Data Protection Act 2018, but with slightly different rights and obligations.

In particular, recording by body worn cameras in these circumstances must **either be done with the consent** of the data subject (however, this is unlikely to be an appropriate legal basis in the context of this technology, for the reasons discussed above) **or be necessary for the purposes of preventing, investigating, detecting or prosecuting criminal offences** including safeguarding against threats to public security or the **execution of criminal penalties**. For more information, please consult the Law Enforcement Directive section of the DPC website.