Guidance for Drivers on the Use of Dash Cams

An Coimisiún um Chosaint Sonraí
Data Protection Commission

The use of dashboard-mounted video recording systems – 'dash cams' – has increased in recent years as devices have become more affordable and of higher quality. Reasons for installing a dash cam in a vehicle appear to range from mitigating personal security concerns to having a means to establish liability in the event of an accident. Today, some insurance companies are offering discounts on policies to drivers who purchase a dash cam (whether they install/use it, or not).

Dash cams can be outward-only facing and record video of the road ahead. Equally, versions exist that record both audio and video, and that record both inside the vehicle and the road outside. Clearly, where both video and/or audio of individuals in a vehicle (typically a taxi or bus) is recorded, or where video of a road user captured by an outward-facing dash cam is recorded, data protection implications may arise and it is important that drivers who install dash cam understand their obligations under data protection legislation.

Status of the Operator of a Dash Cam

EU data protection legislation recognises those who collect and process personal information of individuals (including images and voice recordings of people) as either "data controllers" or "data processors". Clearly, in an everyday context, many of us process the personal information of our family and friends in many different scenarios. The legislation exempts this latter kind of processing under what is known as a "household exemption". This makes common sense.

However, case law from the highest Court in the EU makes it clear that this exemption must be construed narrowly. In its judgment in the case of *Rynes vs Urad* (2014), the Court of Justice of the European Union (CJEU) considered 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 for the purposes of the second indent of Article 3(2) of Directive 95/46.

This case related to a fixed CCTV system, however it has clear implications for users of dash cams that record video and/or audio footage inside and outside of their vehicles.

Data Controller

If you are recording with a dash cam, you are likely to be a data controller for the purposes of data protection legislation and should therefore give due consideration to the legal responsibilities that you may be taking on. Data controllers are required to be compliant with this legislation and to process data in accordance with the principles of data protection.

Some of the key points to consider are:

- Personal data must be processed in a transparent manner. Dash Cam activity presents some challenges in terms of data protection law as EU law (the GDPR) requires a controller to give a whole range of information to anyone whose data is being collected. In the first instance, there should be a clearly visible sign or sticker on and/or inside the vehicle, as applicable, to indicate that filming is taking place. A policy sheet detailing your contact details, the basis on which you are collecting the images and audio of others, the purposes for which the data is being used and how long you will retain it for (read Articles 12 and 13 of the GDPR here) should be prepared by you and made available on request to anyone who asks for further information. Alternatively, you may provide the information verbally. In the event of an accident, you should advise the other party that you have recorded footage of the accident.
- Personal data should only be retained for as long as required and for the purpose that it was obtained. You will need to think about how long you keep hold of footage. Footage of an accident may be required for a claim or investigation and can be retained for that purpose. Other footage should not be retained indefinitely and should be routinely deleted.
- Personal data must be kept securely. Be aware of, and limit, who has access to your camera and any external storage devices.
- People have a right to access their data. If a person is aware that you have a recording of them, they have a right to access that data. You should be able to provide a copy of their data to anyone who requests it, within one month. You should also avoid sharing the data of other people, which may need to be redacted from the footage.

Please note the guidance of the Data Protection Commission (DPC) on the responsibilities of Data Controllers.

Publication of Footage

If you are using a dash cam for security or accident liability purposes, you should be aware that the publication of footage, for example on social media platforms, represents a further processing and risks infringing the privacy rights of recorded individuals and data protection legislation.

Publication of personal data can be justified in certain circumstances for journalistic purposes but this must be carefully balanced with the privacy rights of the individuals concerned.

Sharing Dash Cam Footage

An Garda Síochána may request a copy of dash cam footage from you in relation to the investigation of a crime. The provision of personal data, including dash cam footage, to Law Enforcement authorities is permitted under Section 41 of the Data Protection Act 2018. The relevant law enforcement authority should be in a position to demonstrate that the footage is necessary for the investigation or prosecution of a criminal offence and, where possible, a request for footage should be obtained in writing.

Equally, you may wish to submit footage to an insurance company in the event of an accident. You must be satisfied that the third party with which you share will restrict its use of the data to only what is necessary and will keep it secure and retain it no longer than is necessary.

If your insurance company requests dash cam footage of an accident in relation to a claim, they themselves will likely be a data controller of that footage once it is handed over. As such, they must ensure that any personal data in the footage is processed in a manner compliant with data protection legislation.

Insurance Companies and Dash Cams

The DPC is aware that some insurance companies are offering discounts on motor insurance policies to drivers who use dash cam. Where the use of a dash cam is incentivised in this way, the driver is exhibiting a clear prior purpose and intention to obtain and process the personal data of other persons, for the purpose of recording accidents. This prior intention to obtain personal data in public moves the activity further away from the personal or household exemption and more clearly indicates that the driver is acting as a data controller.

If you enter into an arrangement with your insurer that requires you to own or operate a dash cam to avail of a discount, your insurer may be acting as a joint data controller of any personal data that you record with the dash cam. This may arise in particular if any of the following is a requirement of your insurance policy:

- You are required to install and use the camera;
- You are required to provide footage to your insurer at their request or to upload it to their website;
- Your insurer monitors your use of the camera; and/or
- Your insurer instructs you as to which model of camera or application you must use.

Where two parties are joint controllers of personal data, there should be an arrangement in place that transparently sets out their respective data protection responsibilities.

Before entering into an arrangement with your insurer to use a dash cam, you should ask them to outline their policies in relation to the personal data that you will record, and what responsibilities they will have as data controllers.

The Role of the DPC

The DPC handles complaints from individuals who consider that their data protection rights may have been infringed. If we receive a complaint from an individual in relation to a driver operating a dash cam, where for example the driver has refused to give access to the images when requested, or refused to give information about why they are collecting the data, the DPC will look into the issue.

Where the DPC identifies infringements of data protection legislation in any sector or scenario, it has powers to sanction, including to apply large administrative fines.