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.

Dash cams can be outward- or rear-facing and can record video of the road ahead and/or of occupants of the vehicle. Versions exist that record both audio and video, and that record both inside the vehicle and the road outside. 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 will arise and it is important that drivers who install dash cams understand their potential obligations under data protection law.

It should also be noted, that any audio recordings inside a vehicle would require a very strong justification as to the proportionality and necessity for same, due to the high risk potential for recording of passengers private conversation.

Status of the Operator of a Dash Cam

Data protection obligations apply to those who collect or otherwise process personal information of individuals (including images and voice recordings) other than in a purely personal capacity. In an everyday context, individuals may process personal information in many different scenarios which are of a purely personal or household nature. This kind of processing is not subject to data protection obligations, due to what is known as the 'personal-' or 'household exemption'.

Nevertheless, 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), in a case concerning a fixed CCTV camera which covered both a private dwelling but also a public street, 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 for the purposes of the second indent of Article 3(2) of Directive 95/46.

Although case related to a fixed CCTV system, it has potential implications for any users of video surveillance technology that records video and/or audio in a public space. Users of dash cams will need to consider the nature and extent of any recording they undertake, and whether it falls under the purely personal exemption, or whether the recording may fall within the scope of data protection law.

Where a dash cam is used in a commercial non-personal context, such as by professional drivers, taxis, buses delivery companies, etc., the personal exemption will not apply in any event, and the operators of the dash cam (including potentially drivers, and/or employers or anyone involved in the decision to utilise the dash cam) will have to consider their obligations under data protection law, as set out below.

Controller Obligations

Where personal data is processed, and the personal or household exemption does not apply, the party responsible for the recording will likely be considered the 'controller', under data protection law. A controller is the person, company, or other body that decides how and why a data subject's personal data is processed.

For recordings made with a dash cam in a commercial context or in a public area, the user may be a data controller and thus required to be compliant with the GDPR and the Data Protection Act 2018 and to process data in accordance with the principles of data protection.

Some of the key points for controllers to consider are:

- ☑ **Personal data must be processed in a transparent manner**. Dash Cam activity presents some challenges in terms of transparency as the controller must provide range of information to anyone whose data is being collected.
  - In the first instance, there should be a clearly visible sign or sticker or other indication on and/or inside the vehicle, as applicable, to indicate that recording is taking place.
  - A policy detailing contact details, the legal basis for collecting the images or audio of others, the purposes for which the data is being used, and how long it will be retained for should be made available.
  - This information could be provided on request in written, digital, or verbal form, including through a policy available online, once the individuals whose personal data is processed are made aware of how to access it.
  - In the event of an accident, you should advise the other party that you have recorded footage of the accident for the purpose of transparency and allowing a person to make a Subject Access Request.
  - Further information on transparency obligations can be found on the DPC website and in Articles 12, 13, and 14 GDPR.

- ☑ **Personal data should only be retained for as long as required and for the purpose that it was obtained**. Controllers need to consider how long it is necessary to retain copies of recordings.
  - Recordings of an accident may be required for a criminal investigation by An Garda Síochána and may be retained for that purpose.

- As part of the above-mentioned transparency obligations, individuals should also be made aware of how long recordings will be retained for.
- Footage should not be retained indefinitely and should be routinely deleted, (i.e. a privacy by design feature allows for the footage to be erased and recorded over, unless it is intentionally saved) once it is no longer necessary for the purpose for which it was originally collected or any legitimate subsequent purpose.
- Further information on the principles of storage limitation and purpose limitation can be found in the DPC's guidance on the principles of data protection.

☑ **Personal data must be kept securely.** Controllers need to be aware of, and limit, who has access to their camera and any storage devices on which recordings are stored.

☑ **People have a right to access their data.** If a controller has a recording of someone, they have a right to access that data.

- The right of access includes the right of an individual to confirmation as to whether or not their personal data is processed or stored.
- The right of access also provides the individual with a right to a copy of their personal data, as well as further information about the processing of that data, as found in Article 15 GDPR.
- Controllers should be able to provide a copy of their data to anyone who requests it, within one month.
- Further detail on the right of access can be found on the DPC website, including an FAQ on data subject access requests.

The DPC has also published extensive guidance on its website on the responsibilities of controllers involved in the processing of personal data.

Publication of Footage

Those using a dash cam in a public area should be aware that the publication of footage, for example on social media platforms, could represent a further act of processing and could risk infringing the data protection rights of recorded individuals. In general, and in line with the CJEU's reasoning in the *Buivids* case (C–345/17), publication of material to an indefinite audience, such as on a fully public social media channel, cannot be considered to fall within the personal or household exemption.

For any use of recordings involving personal data, which do not fall within an exception to data protection law, the controller will need to ensure that they have a legal basis for doing so, and otherwise meet the principles of data protection.

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

Sharing Dash Cam Footage

An Garda Síochána may request a copy of dash cam footage from controllers in relation to the investigation of a crime. The provision of personal data, including dash cam footage, to law enforcement authorities may be 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, a request for such footage should be obtained in writing.

In the case of disclosure of dash cam footage to other third parties, unrelated to a criminal investigation, the decision of the CJEU *Rīgas* case (C–13/16) is relevant, as it related to a request for disclosure of personal data of a person responsible for a road accident in order to exercise a legal claim. The CJEU stated that there was no such obligation on the controller to grant the request for disclosure of the footage on the basis of legitimate interests.

The CJEU went on to say that if there was a national law in place to allow for such disclosure of personal data contained in dash cam footage to another third party for a civil liability claim than that would be permissible. To date, there is no Irish law that allows for third parties to obtain from a data controller dash cam footage that contains personal data. However the Superior Court Rules, on orders for discovery may apply in certain cases, but won't apply where the data controller has no direct involvement in the civil proceedings.

The Role of the DPC

The DPC handles complaints from individuals who consider that their data protection rights may have been infringed. Where the DPC identifies infringements of data protection legislation in any sector or scenario, it has powers to sanction, including to apply administrative fines.