How to use dashboard cameras in a compliant way

Anna Rak-Kozerska, Associate, and Lore Leitner, of Counsel, Privacy and Data Protection Practice at Wilson Sonsini Goodrich & Rosati LLP, offer tips on how to use dashboard cameras in vehicles

With EU privacy laws developing rapidly over the last few years, widely used and seemingly innocent dashboard cameras ('dash cams') are beginning to be considered 'privacy intrusive.' Supervisory Authorities that have so far issued statements or guidance on dashboard cameras all confirmed that recording images in a vehicle is considered 'processing of personal data' where individuals are involved. That is why most drivers using dash cams will need to make sure they do so in a compliant way.

This article offers several practical tips on how to legally use dashboard cameras in vehicles, based on the main questions surrounding dash cams.

1. When are dash cams subject to the GDPR?

Dash cams are usually installed on a vehicle's windscreen. Depending on its purpose, the device may be facing outwards to record traffic, facing inwards to record the driver and passengers, or both. Some cameras may also allow for voice recording.

Most dash cams currently in use are outward-facing because they can be used to determine liability for traffic accidents or other violations. Inward-facing cameras are most frequently used by taxi drivers to record passengers and in such cases, are predominantly used for personal security. Recordings may contain images of identifiable individuals (passengers or members of the public) and their cars, as well as recordings of their voice if possible. These are all considered 'personal data' under the General Data Protection Regulation ('GDPR').

However, not all dash cam use is subject to the GDPR. Drivers who use dash cams only to watch themselves or to share videos with a limited group of friends, do not have to comply with the GDPR because they fall under the 'domestic purposes' (or household) exemption. As such, any other purpose or use will need to comply with the GDPR. These other purposes cover scenarios such as commercially operated vehicle fleets with pre-installed dash cams, self-employed taxi drivers, or consumers using dash cams which are provided by their insurer and can help keep policy costs down.

Whether a dash cam needs to comply with the GDPR will need to be assessed on a case-by-case basis. This was affirmed in the *Ryneš* case (C-212/13, December 2014), in which the European Court of Justice concluded that where a surveillance camera on a private domestic property is fixed in a way that it monitors a public space, the recording cannot be considered as taken only for domestic use. In light thereof, it's safe to say that only inward facing dash cams can fall within the household exemption.

2. Who is the controller?

Usually, the controller will be the driver of the vehicle, or in a fleet setup, the company operating the fleet. In certain cases, there may be more than one controller. For example, when an insurer offers the incentive to a policyholder of installing a dash cam in his or her vehicle in an attempt to reduce fraudulent injury claims, both the insurer and the relevant policyholder are controllers. This was specified by the Irish Data Protection Commission, which also stated that such a scenario requires the parties to enter into a joint-controllership agreement. This type of agreement establishes the distribution of responsibility between the two controllers and they are often complex, and take time to negotiate. However, in an insurance setup, it is difficult to envisage how this could work on a large scale unless through the use of pre-completed forms and non-negotiable terms.

In an employment context, controllers operating a fleet of vehicles should be careful when using inward-facing dash cams, as this may qualify as employee-monitoring in certain EU countries. In such cases, dash cam use should be proportionate to the concern it is addressing, and employees should be clearly informed about the purposes and how their privacy at the workplace is respected. Even though dash cam use does not have to be notified to the local Supervisory Authority, complaints from disgruntled employees can result in a regulatory investigation, so companies need to make sure they get it right.

In particular, the main obligations for controllers in relation to dash cam use are:

- defining the lawful basis for collecting and using the data (i.e. the ground for processing);
- keeping personal data secure and only for a definite period of time;
- handling personal data in a transparent manner; and
- being able to provide a copy of a recording.

3. Ground for processing

First and foremost, the controller should determine its ground for processing. This is important because it may impact the first interactions with the vehicle passengers.

The two obvious grounds are consent and legitimate interests. As a general rule, controllers should keep in mind that the legitimate interest of the controller, i.e. the vehicle owner or driver, may be overridden by the interests of individuals. In simple terms, this means that, if a recording is privacy intrusive, it will most likely require consent of the recorded individual. For inward-facing dash cams, both grounds are potential options.

There are a number of ways in which an individual's consent can be obtained under the GDPR. For example, recording the oral consent of a passenger, using digital devices to provide a tick box consent form, or getting into the car labelled with a dash cam disclaimer, may all be acts of consent.

Under the GDPR, controllers need to be able to demonstrate that consent has been obtained. Therefore, it is best practice for consent to be stored for evidence purposes, and to ensure that a recording cannot be made before a passenger provides their consent. Dash cam users should choose a consent method that would enable easily fulfilling both requirements in their business. In turn, for outward facing dashboard cams, it is only technically feasible to record traffic on the basis of the motorist's legitimate interest (such as gathering evidence or route monitoring).

"For inward-facing dash cams used by taxi drivers, the recording will be stored until the local statutory limitation period for civil claims expires, whereas for an individual using a dash cam provided by an insurer, it seems sufficient to delete recordings daily unless a traffic accident or other traffic violation necessitates a longer retention period."

4. Storing the Recordings

It is important to note that dash cam recordings cannot be kept indefinitely. The retention period will need to be based on reasonable criteria. Depending on the controller's type of business activity, the retention period may range from days to years. For a dash cam provided by an insurer, it seems sufficient to delete recordings daily unless a traffic accident or other traffic violation necessitates a longer retention period.

In this context, dash cam users should consider whether they have a real interest in keeping the dash cam turned on constantly. In Germany for example, permanent 'preventive' recording of ones' surroundings, including recording traffic participants, is not allowed. Rather cameras should be activated on purpose by drivers or triggered automatically (e.g. by noise), and should otherwise remain in a standby mode.

5. Transparency

In addition, controllers need to ensure that the vehicles with dash cams are marked with appropriate signs to provide a notice to passengers. Depending on the images being recorded, the sign should be clearly visible on and/or inside the vehicle, to indicate that recording is taking place (e.g. a large red sticker with a camera icon in visible places).

In addition, it is a best practice for a policy to be presented in the vehicle, and this policy should outline the controller's contact details, purposes and grounds for processing, how long the footage will be kept and with whom it may be shared. The driver should always have a copy of the policy ready in case a passenger or passer-by requests it. However, the Irish Data Protection Commission has confirmed that this information may also be given verbally.

6. Access rights

In case a recording contains personal data (e.g. voice, or image), the controller should be able to provide this footage to the relevant data subject upon their request. In order to minimise the impact of these rights, it is advisable to delete the recording as soon as reasonably possible. As such, if a recording has been deleted, access can no longer be granted.

7. Sharing the recordings — do's and don'ts

The most controversial coverage in the news of dash cam recordings has been brought on by YouTube publications of traffic violations and reckless behaviour. Even though this may seem like a way to generate likes, controllers should make sure that drivers are banned from any such sharing because of the high risk of violating privacy laws. This is also true in individual cases.

(Continued on page 12)

(Continued from page 11)

However, the problem may be solved by redaction. For instance, in Germany, recordings may be shared where personal data are blurred out. In very specific circumstances, publication of a video recording may be justified by journalistic purposes, but such purposes are generally unlikely if someone is using a dash cam for security or accident liability evidence. Thus, even in such a case, there is a large body of case law which governs the relationship between freedom of speech and an individual's right to privacy as protected by Article 8 of the European Convention on Human Rights.

In certain situations, public authorities or enforcement agencies may request access to recordings. It is important to emphasise that any authority making such a request should be in a position to demonstrate that the recording is necessary for the purposes of an investigation or a prosecution of a criminal offence and, as a rule, such a request should be made in writing. Otherwise, dash cam controllers should not disclose such information unless they receive a binding order.

In the context of 'preventive' recording, drivers are generally allowed to use recordings as evidence (e.g. by submitting footage to an insurance company in the event of an accident). However as controllers, drivers should ensure that the insurer has appropriate data processing and retention policies in place.

Conclusion

Recent guidance and case law on dashboard camera use have set a new standard for using vehicle monitoring in everyday life. Drivers or fleet owners qualify as controllers and therefore need to meet a set of data processing obligations under the GDPR and local privacy laws.

Although this article outlines general benchmark requirements for using dash cams, it is still recommended to review the latest local laws or guidelines before using dash cams in certain European jurisdictions. Future guidelines may also cover further recording devices, such as helmet cameras used by cyclists.

Anna Rak-Kozerska and Lore Leitner
Wilson Sonsini Goodrich & Rosati LLP
arakkozerska@wsgr.com
lleitner@wsgr.com