CASTLEBRIDGE
Changing how people think about information

Castlebridge Guidance Note

``

Dashcams and GDPR: Questions and Answers

What does my dashcam have to do with GDPR?

If you are recording video using a dashcam you are likely to be processing personal data. For instance, you are probably recording footage that includes people or number plates of vehicles connected to people. This is processing of personal data and therefore subject to the GDPR and the Irish Data Protection Act 2018.

- If your dashcam footage only records the road, and you aren't recording legible number plates and you are not recording people, you might not be processing personal data (*but there's always a risk you might be*).
- If your dashcam records images of people, you are processing personal data.
- If your dashcam includes sound and records people's voices, you are processing their personal data.
- If your dashcam records images of cars where licence plates are visible, you are recording personal data if you have the ability to single someone out based on that data or have access to the National Vehicle Driver File and can directly identify someone.

I'm only recording for my own personal use. Isn't there an exemption from GDPR? GDPR does not apply to processing of personal data for domestic use. A few cases decided by the European Court of Justice have helped define the limits of the "personal use" exemption.

Such a case decided in 2014 determined that personal CCTV surveillance for the safety of an individual's household must be strictly limited to the private property of the individual, and that filming of a public space is not to be considered domestic use.[i]

- If the dashcam is only recording the inside of your car for personal use and you are not publishing it, then it could fall under domestic use exemptions,

BUT….

- If your dashcam is facing outside and you are recording the street outside of your own vehicle and others, this is NOT domestic use.[ii]
- If you publish your recording on the internet, it is no longer domestic use. Personal use includes recording and storing, but not publication.
- If you want to publish, you should ***blur out or otherwise make un-recognizable*** people, number plates, etc.
- If you are driving for work (Taxis, cabs, etc.) and recording passengers, passers-by, or people you interact with, this is not domestic use. This is like having CCTV cameras in your place of business, and it falls under GDPR, and your passengers and passers-by need to be *informed* You should refer to the Data Protection Commissions guidance on CCTV in the work place (https://www.dataprotection.ie/docs/Data-Protection-CCTV/m/242.htm)

I've got my dashcam because my insurer gave me a discount if I had one. Am I OK?

If your insurer has incentivised you to get a dashcam to record the road in front of you, around you, or behind you, you are still processing personal data, the data is still being recorded in a public place, so the recording is outside the scope of the domestic use exemption.

You might be able to claim you have a legitimate interest for the processing of the data. For example, it's in your legitimate interest to have a recording of an accident where you might want to make a claim or would need to defend a claim. However, you need to consider the balance of your interests with the rights of others and ensure you have basic safeguards in place.

If you are incentivised to install a camera, you would also be able to argue that breaking that condition of your insurance contract and the implications of that means your use of the camera is necessary for compliance with a legal obligation to which you, as a Data Controller, are subject.

If your insurance company is incentivising you to buy and use a camera, you should ask them what supports they will give you to ensure you can meet your obligations under the legislation.

Who is the Data Controller?

Because you decided what and how to record video, you are "determining the means and purposes of processing". This means you are a Data Controller.
Some insurance companies are offering lowered rates to customers if they install a dashcam in their car.[iii] If you are using dashcam footage in partnership with your insurer to get lower rates, you and the insurance company are joint controllers.[iv] This means you are jointly accountable for compliance, and you need to have your respective responsibilities for GDPR compliance documented in a written agreement.

This applies even if your insurance company isn't actually obtaining and processing your recordings – the fact that they want you to record video, the fact that they are defining a format and medium for recording etc. means they are a Joint Controller (there's a European Court of Justice case on this very point).
You should check with your insurer what form of joint controller agreement and what other supports they will provide you in addition to the discount on your premium to help you meet your obligations under the legislation.

What do I need to do to stay on the right side of the law here?

There are a few key principles and obligations you need to consider.

1. **Fair and Transparent Processing:** People need to know you are recording, what your purpose for recording is, and how to contact you. You should ideally have visible prior notice. At the very least, if you are involved in an incident and the dashcam records it, you should immediately inform the other people involved about your recording.
2. **Purpose Limitation and Storage Limitation:** What is your purpose for recording? Are you limiting your recording to what is necessary and proportionate for that purpose?
    a. Proportionality: Where are you pointing the camera? Does it need to be high resolution? Does it need to be continuous capture? Who has access to it? Is there a less invasive way to get the result you want? How long are you keeping it? You should only keep your recording as long as it is necessary for your purposes.
    b. Necessity: Can you explain to a reasonable person why the use of cameras is absolutely required?
3. **Integrity and Confidentiality:** Who has access? Is it secure? (Many connected devices do not have good security.) You need to ensure that people don't have unauthorized access to your recordings.
4. **Accountability** and **Rights**: Anyone you record has a right to know you are recording them, access and a copy of the footage you recorded of them, to object to your processing their data, and to ask you erase it. That means:

- You need to ensure ***they can contact you*** to request a copy of all data you have on them.
- You need to be able to identify them to give them all the footage you may have of them.
- You must ***provide them a copy of the recording of themselves*** within ***30 days*** of the request
- Where there are people other than the subject in the footage you have, their images cannot be shared without their consent This means you need to **redact their faces and other identifying marks** from the video. This can be notoriously expensive and time consuming.

Balancing Rights: Privacy and Freedom of Expression

The rights to privacy and data protection are not absolute rights, and they are balanced with the right to freedom of expression. GDPR and the Irish Data Protection Act 2018 take this into account when it comes to journalism and artistic purposes.[v] Before you publish recordings of people for these purposes, you need to balance the benefits of the publication against the possible harms to the people who you have recorded.

- Is your recording newsworthy? Publishing personal data for journalistic purposes when it is newsworthy is allowable. Is there clear public benefit to publishing your recording, or might it be harassment and a violation of people's privacy? (Getting people's permission before you publish recordings of them is a very good way to make sure you land on the right side of that balance, as well as complying with the Fair, Lawful, and Transparent principle of GDPR.)

- Is it necessary to publish identifying personal information or can you de-identify the people you've recorded?

- Can you accommodate people's rights to objection, rectification, and erasure? Allowances for journalistic purposes and artistic expression are also not absolute, and compliance with GDPR is only exempted where it would be *incompatible* with the rights of freedom of expression and information in a democratic society.[vi]

Dashcam Footage and evidentiary purposes

If your dashcam footage incidentally records a crime, Section 41(b) of the Irish Data Protection Act 2018 allows for it to be used as evidence. Law Enforcement Authorities may request you to provide this footage under Section 70 of the Data Protection Act 2018. The Data Protection Commission advises that requests from the Gardaí should be in writing and signed by someone of Chief Superintendent level or higher.[vii] Disclosing data without proper authorisation would be a violation of GDPR and the Irish Data Protection Act 2018.[viii]

---

[i] Case Case C-212/13 František Ryneš v Úřad pro ochranu osobních údajů. Guidance on Dashcams published by the Belgian and Hungarian Data Protection authorities were written before this CJEU decision and may need updating to reflect clearer understanding of the limits of the domestic use exemption. Case Case C-25/17 Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta (Jehovah's Witness Community v.Data Protection Authority of Finland) also discussed the limits of domestic use exemptions.

[ii] This was clarified by the European Courts of Justice in Case C-212/13 František Ryneš v Úřad pro ochranu osobních údajů.

[iii] https://www.independent.ie/business/personal-finance/drivers-who-install-dash-cams-will-now-get-insurance-discount-37526616.html

[iv] CJEU decisions clarifying joint controller relationships include: Case C-210/16, Schleswig-Holstein DPC v Wirtschaftsakademie , and Case C-25/17 Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta

[v] Section 43 Data Protection Act 2018.

[vi] Section 43 (1) Data Protection Act 2018.

[vii] https://www.dataprotection.ie/docs/Disclosures-Permitted-under-Section-8-of-the-Data-Protection-Act-Section/237.htm