GDPR-Ready Dashcams in Commercial Fleets (EU)

Practical Checklist for Safe & Compliant Deployment

Purpose.
This checklist helps commercial fleet teams deploy dashcams and in-vehicle video telematics in a GDPR-ready way focusing on road safety, incident handling, data minimization, and driver trust.
It is based on official EU legal sources and practical fleet deployments. It does not replace legal advice.

CORE SETUP (FOUNDATION)

1. Purpose of Use (must be defined and documented)

Tick all that apply:

☐ **Road safety and incident prevention** *(Identify risky situations and reduce repeat incidents (near-misses, harsh manoeuvres, distraction))*
☐ **Incident and insurance claims investigation** *(Provide objective context after an incident to speed up internal review and claims handling)*
☐ **Driver coaching and training** *(Use a limited set of safety events to support coaching and improve driving habits over time)*
☐ **Legal protection and evidence** *(Preserve evidence when legally necessary (e.g., serious incidents, disputes), with controlled access and retention)*
☐ Other (specify): _____

🚩 **Red flag:** continuous employee monitoring as a primary purpose

Note: Purpose must be documented and clearly communicated to drivers before rollout.

---

2. Recording Mode

Select the primary recording approach:

☐ **Event-based video clips (recommended)** (*The system stores only short clips when a safety event happens (e.g., collision, harsh braking, near-miss))*
☐ **Continuous recording (high GDPR risk)** (*Video is stored continuously. This is often considered excessive and increases compliance risk)*

If event-based:
☐ **Short clips triggered by safety-related events** *(Only defined events trigger storage)*
☐ **Limited pre-/post-event buffer.** *(Example: a few seconds before and after the trigger)*
☐ **Automatic overwrite when no incident occurs.** *(If there is no incident, footage is overwritten automatically and not kept longer than necessary)*

Note: Event-based recording strongly supports GDPR data minimisation and acceptance by drivers.

---

3. Personal Data Involved

Dashcam video may include:

☐ **Driver face** *(direct identifier)*
☐ **Passengers / pedestrians** *(third parties in public space)*
☐ **Vehicle registration plates** *(can identify individuals in many cases)*
☐ **Location, time, route context** *(can reveal behaviour and routines)*
☐ **Audio (high risk — avoid unless strictly necessary)** *(often captures private conversations — higher risk; disable unless strictly necessary)*

Note: Only collect data that is necessary for the defined safety purpose.

---

4. Lawful Basis (high-level)

Primary lawful basis used:

☐ **Legitimate interest** (most common for fleet safety) *Used when the fleet has a clear safety/incident-handling need and applies safeguards (event-based recording, short retention, restricted access). A short Legitimate Interest Assessment (LIA) should be documented.*
☐ **Legal obligations** *(Used when a specific law or regulatory requirement applies (e.g., mandatory incident documentation, sector-specific safety rules). Document which requirement you rely on.)*
☐ **Consent** (rarely suitable in employment context) *(Usually not recommended for driver monitoring because consent may not be considered "freely given" in an employer–employee relationship. Use only if your legal counsel confirms it is appropriate.)*
☐ **Other**: _____

Note: Where legitimate interest is used, necessity and balancing against individual rights must be documented.

OPERATIONAL CONTROLS (EXECUTION)

5. Data Retention & Deletion

Confirm that the following are defined:

☐ **Short default retention period** *(Example: keep non-incident clips for a limited number of days)*
☐ **Longer retention only for confirmed incidents** / claims *(Store longer only when a real incident happens and evidence is needed)*
☐ **Automatic deletion rules configured** *(System deletes/overwrites footage automatically when the retention time ends)*
☐ **Manual deletion process defined** *(Clear steps for deleting footage on request or when it is no longer needed (with the right approvals))*

Note: Retention must be proportionate to purpose — not "just in case".

---

6. Access Control & Use of Video

Confirm controls are in place:

☐ **Role-based access (no open access)** *(Only authorized roles (e.g., Safety Manager, Claims) can view video — not everyone in the company)*
☐ **Clear rules on who can view video** *(Define who can view which clips and for what purpose (safety, incident investigation, claims)*
☐ **Export allowed only for defined cases** *(Export/share video only when needed (e.g., incident, claims, legal request) and follow an approval step)*
☐ **Audit log of access and exports** *(The system records who viewed/exported which clips and when (accountability))*

🚩 **Red flag:** video accessed out of curiosity or without justification

---

7. Driver Communication & Transparency

Before rollout, ensure:

☐ **Written internal camera policy** *(A short internal policy (1–2 pages) describing why cameras are used, what is recorded, who can access video, and how long it is kept)*
☐ **Clear explanation of purpose and limits** *(Explain that the purpose is safety/incident handling (not constant monitoring))*
☐ **Explanation of what is recorded and what is not** *(Example: event-based clips only; no continuous recording (if applicable); audio off (if applicable))*
☐ **Retention periods explained** *(Explain how long footage is kept by default and when it may be stored longer (incidents/claims))*
☐ **Contact point for questions or complaints** *(Provide a named contact (e.g., Safety Manager or DPO) for questions and requests)*

Note: Transparency is essential for trust and long-term success.

---

8. DPIA (Data Protection Impact Assessment) / Risk Assessment

Assessment status:

☐ **DPIA required and completed** *(Completed before rollout (often needed for in-cab cameras, large fleets, or systematic monitoring))*
☐ **DPIA not required (decision documented)** *(A short note explains why DPIA is not required for this setup (e.g., event-based, limited retention, strong access controls))*
☐ **To be reviewed before scaling** *(If starting with a small pilot, confirm DPIA requirements before expanding to the full fleet)*

Note: DPIA is often required for in-cab cameras or systematic video processing.

FINAL CHECK — BEFORE SCALING

☐ Pilot tested on limited vehicles
☐ Rules applied consistently
☐ Driver feedback collected
☐ Adjustments made before full rollout

EU Legal Sources & Guidance (Official References)

This checklist is based on the following **official EU legal sources and guidance**:
General Data Protection Regulation (GDPR) — Regulation (EU) 2016/679
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
EDPB Guidelines 3/2019 — Processing of personal data through video devices
https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en
EDPB Guidelines 1/2024 — Legitimate interests (Article 6(1)(f))
https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en
EDPB Guidelines 4/2019 — Data protection by design and by default (Article 25)
https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
EU Charter of Fundamental Rights — Articles 7 & 8
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12016P/TXT
Court of Justice of the EU — Ryneš (C-212/13)
https://www.dpcuria.eu/case?reference=C-212/13

Extended EU Dashcam Compliance Framework

To save time and avoid searching across multiple legal documents, we provide a **consolidated compliance framework** with:

- mapped GDPR articles relevant to dashcams
- EDPB guidance explained in fleet context
- country-specific notes (e.g. Austria, Luxembourg, Portugal)
- practical answers used in real deployments

EU Dashcam & Video Telematics Compliance Framework
https://safefleetview.eu/eu-legal-framework-for-dashcams

Disclaimer This checklist is provided for informational purposes only and does not constitute legal advice.