PRACTICAL GUIDE FOR FLEET OPERATORS

AutoSense DRIVING SAFETY

Driver monitoring systems and the NZ Biometric Processing Privacy Code

This guide is for fleet operators who use — or are considering — driver-facing safety systems to help detect fatigue and distraction. It explains what the Biometric Processing Privacy Code is, what you're responsible for, and how to meet those responsibilities without unnecessary complexity.

What is the Biometric Processing Privacy Code?

The NZ Biometric Processing Privacy Code is a binding privacy code issued by the Privacy Commissioner. It applies to systems that analyse biometric information — such as a person's face, eyes, or head movement — to categorise or assess a person.

For fleet operators, this most commonly includes driver monitoring systems used to detect:

- fatigue
- drowsiness
- distraction or inattention

Important: A system can be covered by the Code even if it does not identify who the driver is. If it analyses facial or eye movement to infer alertness or attention, it may still be in scope.

When does it apply?

The Code came into force in two stages:

- **3 November 2025** — new biometric systems
- **3 August 2026** — systems already in use before November 2025 (a transition period)

Existing fleet systems must now be able to show they have been reviewed and aligned with the Code.

Who is responsible?

Fleet operators are usually responsible — not just the technology supplier.
Even where a supplier provides the device and platform, the fleet operator decides:

- why the system is used
- who can access data
- how long information is kept
- when footage can be shared or exported

The good news is that you don't need to start from scratch. With AutoSense and Guardian, much of what the Code expects is already built in or supported through templates and practical guidance.

PRACTICAL GUIDE FOR FLEET OPERATORS

AutoSense DRIVING SAFETY

Why Driving Monitoring Systems matters

Fatigue and distraction are major safety risks in fleet operations. Technology that helps manage these risks can save lives.
At the same time, biometric information is sensitive — especially in a workplace setting. Problems usually arise not because systems exist, but because:

- the purpose is unclear
- too many people can access footage
- footage is handled informally
- drivers don't understand how the system is used

A clear Data Protection Impact Assessment (DPIA), tight access controls, and plain-English communication prevent most issues.

How the Guardian driver monitoring system works

A simple way to explain Guardian is:

> **Detect → Alert → Expert review → Act (only when needed)**

- the device analyses facial, eye, and head movement to detect fatigue or distraction risk
- if risk is detected, the driver receives an in-cab alert
- a short event clip and supporting data are created
- trained experts review and classify events before follow-up action is taken

This expert review step improves accuracy and helps ensure action is taken only on valid safety-related events.

Guardian

Both Guardian Gen 3 and Guardian Gen 2 are event-based safety systems. Their primary design is to create events when safety risk is detected — not to operate as general CCTV.
The difference is:

- Gen 3: event-based clips only
- Gen 2: event-based, but can also provide short-term continuous footage that may be extracted for defined purposes

Where short-term continuous footage exists (Gen 2), operators must be clear about:

- why it can be extracted
- who can approve extraction
- how extracted footage is stored, shared, and deleted

These details should be documented in the DPIA and explained to drivers.

PRACTICAL GUIDE FOR FLEET OPERATORS

AutoSense DRIVING SAFETY

Is this CCTV? PIA vs DPIA

Traditional CCTV and dashcams are usually assessed using a Privacy Impact Assessment (PIA), focused on continuous footage handling.
Driver monitoring systems that analyse biometric cues require a Data Protection Impact Assessment (DPIA), because the processing is higher risk.
Practical takeaway: ,If your system involves biometric processing, complete a DPIA. That same DPIA should also cover how any recorded footage is handled.
If you meet the Biometric Code standard — clear purpose, transparency, tight access, secure handling, defined retention, and proper rights handling — you will generally also be meeting good-practice privacy expectations for continuous footage.

Data Protection Impact Assessment (DPIA) in everyday language: what a good one covers

A practical DPIA answers:

- what safety risk are we managing?
- what does the system analyse and produce?
- why is it necessary for safety?
- what are the realistic privacy risks?
- what controls apply (purpose, access, retention, exporting, training)?
- how do we explain this to drivers?

Most content can be reused unless the system or its use changes.

Safe handling and access control

One rule that prevents most problems: Keep footage in the portal unless you genuinely need it out.
Good practice includes:

- limiting video access to a small safety group
- restricting exporting to a very small, trained group
- defining retention and deletion rules

Screenshots and screen recording: Even where downloads are restricted, footage can still be captured via screenshots or screen recording. Treat unauthorised screen capture the same way as unauthorised exporting and make this clear in policies and training.

Driver rights and your obligations

Drivers should:

- know what the system does and why
- understand what is recorded and when
- know who can access footage and for what purpose
- be able to request access or corrections
- have a clear way to raise questions or concerns

Fleet operators need simple, deliberate processes so these rights are handled consistently, not informally.

If something goes wrong: privacy breaches

A privacy breach may include:

- unauthorised access to footage
- unauthorised sharing or exporting
- loss of exported footage
- disclosure to the wrong person

If a breach is suspected, fleet operators should:

- act quickly to contain the issue
- preserve evidence
- assess the risk of harm
- notify the Privacy Commissioner and affected individuals where required
- fix the root cause and update controls

Having a clear DPIA and access controls makes this much easier.

Next steps

For most fleets:

1. Confirm your system and generation
2. Complete or refresh your DPIA and Safe Driving Policy
3. Lock down access and exporting
4. Update driver and manager communications
5. Put a clear access and correction process in place
6. Review if the system or its use changes

Existing systems must be aligned by 3 August 2026.

You don't need to become a privacy expert. With an event-based system, clear boundaries, a practical DPIA, and sensible handling controls, compliance becomes manageable, explainable, and defensible — without undermining safety. Guardian with Guardian Live is designed to support that approach and with support from AutoSense, take much of the leg work away.

NEW ZEALAND
+64 9 303 1416
support@autosense.co.nz
autosense.co.nz

AUSTRALIA
+61 370 532 306
support@autosenseaustralia.com.au
autosenseaustralia.com.au

AutoSense DRIVING SAFETY