Connected vehicles & mobility data: When to act and what to do

EDPB European Data Protection Board

GUIDELINES AT A GLANCE

June 2026

When your organisation develops or provides services for connected vehicles and mobility related applications, it may collect and record a wide range of personal data, such as driving habits, location data, or biometric data. These personal data may be (i) processed inside the vehicle, (ii) exchanged between the vehicle and personal devices connected to it (e.g., the user's smartphone) or (iii) collected locally in the vehicle and exported to external entities (e.g., vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing.



The EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications clarify the rules for this ecosystem. Importantly, a **connected car is a "terminal equipment" (just like a computer or a smartphone)** and you should design your services to keep users in control of their data, including by preferring local, in-vehicle data processing over cloud computing infrastructures, where possible.

Key responsibilities at a glance

Here is a checklist of your organisation's key responsibilities:

When to act	What to do
Before accessing vehicle data	**Check ePrivacy rules.** Accessing data from a vehicle usually requires prior consent under the ePrivacy Directive (Art. 5(3) ePrivacy Directive). **Check the GDPR** for any processing operations of personal data following the above processing operations (i.e., Art. 6 GDPR and Art. 9 GDPR for sensitive data). **Ask yourself: Are we relying on the right legal basis to access the vehicle's data?**

When to act	What to do
During product design	**Prioritise local processing.** Keep data processing inside the car itself (or on the user's connected smartphone) instead of sending data to outside actors, whenever possible. Consider developing a secure in-car application platform, physically divided from safety relevant car functions so that the access to car data does not depend on unnecessary external cloud capabilities. **Ask yourself: Do we really need to export this data to the cloud, or can the car calculate the result locally?**
When collecting sensitive data	**Apply strict safeguards.** Processing location, biometric and data revealing criminal offenses or other infractions ('offence-related data' such as speeding) requires compliance with strict rules and putting in place security controls, such as encryption. **Ask yourself: Do I really need the sensitive data i am processing, and am I applying the appropriate safeguards?**
When a vehicle changes hands	**Enable an easy wipe.** Provide a simple way to delete all personal data from the dashboard. **Ask yourself: Will the next owner or driver be able to see the previous driver's location or call history?**

The ePrivacy interplay with the GDPR: the key role of consent

Because a connected vehicle is a "terminal equipment," the **ePrivacy Directive** also applies.

- **The rule:** Storing information or accessing information stored in the car (e.g., reading telemetry data) requires the user's prior **consent**.
- **The exceptions:** Consent is not necessary when access to this data is for the sole purpose of carrying out the transmission of a communication over an electronic communications network or is strictly necessary to provide an "information society service" explicitly requested by the user (e.g., requesting GPS navigation services).
- **No bundling:** Consent cannot be bundled with the contract to buy or lease the car. If a user refuses data collection, they must still be able to buy and drive the vehicle.



Principles in practice: High-risk data categories

If your company processes the following types of data, elevated security and privacy measures are needed:

1. Location data

Location data can be particularly revealing of the life habits of individuals (as it might reveal a driver's religion, sexual orientation, or lifestyle habits based on the places they visit). Do not collect it continuously by default. You must inform the car users about the processing. You should also provide users with an option to deactivate it at any time and use clear dashboard icons (e.g., an arrow that moves across the screen) to warn passengers when location tracking is active.



2. Biometric data

If you use fingerprints, voice recognition, or facial scanning to unlock the car or load a driver's profile, you should provide a non-biometric alternative (like a physical key or PIN). You would need to ensure that the biometric solution is sufficiently reliable. Biometric templates should be stored locally in the vehicle in an encrypted form and never sent to external servers. The raw data used to make up the biometric template and for user authentication should be processed in real time without ever being stored, even locally.

3. Offence-revealing data

Data that reveals a traffic violation (e.g., crossing a white line, or instantaneous speed combined with location) is subject to strict rules. External processing of this data is generally forbidden; it should only be processed locally within the vehicle where the driver retains full control. Strong security measures must be in place to offer protection against the illegitimate access, modification and deletion of this type of data.

Practical examples

Here are specific scenarios extracted from the Guidelines illustrating how these rules apply in practice:

Example

(section 3.1, paragraphs 105-120, pages 26-29)

Context: An insurance company tracks driving habits (braking patterns, rapid acceleration) to reward safe drivers with lower premiums.

What to do: The insurer should offer a standard, non-usage-based insurance policy for consent to be freely given. If possible, raw data regarding driving behaviour should be processed inside the vehicle or by an independent telematics provider. The insurance company should **only** receive the final aggregated score, never the raw tracking data.

Example

(section 3.4, paragraphs 161-173, pages 35-36)

Context: A service provider offers a tracking feature to locate a stolen vehicle.

What to do: You cannot continuously track the vehicle "just in case" it gets stolen. The use of location data should be limited to the strict needs of the investigation and to the case assessment by the competent legal authorities. Location data can only be transmitted as of the declaration of theft and cannot be collected continuously the rest of the time.

The accountability checklist

Your organisation's action plan for compliance in the connected vehicle and mobility related applications ecosystem:

Action point	Why it matters
1. Design for local processing	Processing data in the vehicle reduces security risks and strengthens the user's control over their personal data.
2. Create a simple "Delete" function	Cars change hands (rentals, leases, second-hand sales). Users should be able to simply wipe their navigation history, contacts, and profile data permanently.
3. Separate vital functions	Infotainment systems can be highly vulnerable to hackers. You should physically or logically partition the vehicle's critical safety functions from its telecommunication capacities.
4. Standardise dashboard icons	Passengers and drivers shouldn't be taken by surprise. Use clear, standardised icons on the dashboard to alert them when location or audio recording is active.
5. Conduct a DPIA early	The scale and sensitivity of connected car data may result in a likely high risk to individuals. Conducting a Data Protection Impact Assessment early in the design phase is essential to identify and patch vulnerabilities.

This document provides a simplified overview of the guidelines. For more comprehensive legal explanations and examples, please consult the full text of the guidelines.

Read the complete guidelines