

Geolocation of vehicles provided to employees

So-called geolocation devices enable employers to know the geographical position, **at a given moment or continuously**, of their employees when they are on the move.

While these devices can improve the services provided by data controllers by enabling them to optimize fleet management and improve operational efficiency, they are **particularly intrusive** for employees.

Their use must therefore be strictly supervised to avoid any excesses on the part of employers.



For what purposes can an employer set up a geolocation system?

Personal data may be collected for **several purposes**, provided that these purposes are:

- **determined**;
- **explicit**;
- **legitimate**; and
- **not further processed** in a manner incompatible with these purposes

By virtue of this principle of **purpose limitation**, the APDP considers that the implementation of a geolocation system can meet the following objectives:

- **improving the production process**, either directly by better allocation of available resources (e.g. dispatching the nearest vehicle to carry out an activity such as an emergency intervention, breakdown service or pick-up), or indirectly by analyzing the journeys made after the event (e.g. analyzing the time needed to travel or carry out a task);
- contributing to **the safety of people, goods transported or the vehicle** for which the data controller is responsible (drivers of delivery vehicles, lone workers, transport of cash and valuables, etc.);

- **monitoring goods because of their special nature** (compliance with hygiene rules relating to the cold chain, for example);
- **monitoring and invoicing for the transport** of people or goods, or for services directly linked to the use of the vehicle (e.g. school buses, road cleaning, medical care, etc.);
- **monitoring employees' working hours when this cannot be done by other means;**
- **monitoring and establishing proof of the performance of a service** by the employee linked to the use of the vehicle.



The use of a geolocation device must not lead to **permanent and inappropriate monitoring** of the employee concerned, and the data collected may not be used, with certain exceptions, for disciplinary purposes.

The APDP therefore considers:

- with regard to business vehicles that may be used by employees **for private purposes**, the data controller must not collect information relating to the location of an employee **outside the latter's working hours**. In this context, it requires that employees have the option of deactivating the vehicle geolocation function at the end of their working hours;
- employees holding **elected office or trade union office** must not be geolocated when they are acting **in the exercise of their office**;
- the use of a geolocation system is not justified when an employee is **free to organize his or her movements** (medical sales representatives, sales reps, etc.).

What justification is needed for the implementation of a geolocation system?

To be lawful, automated processing of personal data must meet at least one of the requirements set out in Article 5 of Law no. 1.565 of December 3, 2024.

The APDP thus considers that the implementation of a geolocation system can be justified by:

- compliance with a **legal obligation** to which the controller or its representative is subject;
- the performance of a **contract**;
- the fulfilment of a **legitimate interest** pursued by the controller or a third party, **provided that this does not adversely affect the interests or fundamental rights and freedoms of the data subject**;
- a reason of **public interest** pursued by a legal person governed by public law or by a legal person governed by private law entrusted with a mission of general interest or a public service concession;
- the **consent** of the data subject.



In the case of data collected under an employment contract establishing a **relationship of subordination** between employer and employee, the apdp will very strictly assess any justification based on the consent of the data subject.



What information may be collected?

The data controller must ensure that the data collected are « *limited* » to achieving their objectives.

In order to comply with this principle, the personal data collected must be:

- **adequate** ;
- **relevant** ; and
- **limited** to what is necessary for the purposes of the processing.

The APDP therefore considers that only the following personal data may be collected by a geolocation device.

- employee identification: surname, first name, professional details, internal registration number, vehicle registration number;
- information relating to employee movements : location data from the use of a geolocation device, history of journeys made;
- additional information associated with the use of the vehicle : vehicle speed, number of kilometers travelled, length of time the vehicle is used, driving time, number of stops.

What about data on speed, driving time and breaks?

These data may be collected in the Principality, but not as part of processing linked to vehicle geolocation data, but rather as part of processing linked to the collection and archiving of **data from digital tachographs** installed in HGV vehicles. This processing is justified by a **legal obligation** to which the data controller is subject.

Article 1 of Ministerial Order no. 90-651 of December 28, 1990 on the use of speed control devices (tachographs) on motor vehicles states that « *All motor vehicles with a maximum authorized weight, with or without trailer, of more than 3.5 tons must be fitted with a speed control device known as a tachograph* ».

In addition, Article 2 of the aforementioned Ministerial Order stipulates that « *Tachographs must [...] enable the following to be recorded in addition to vehicle speed: - distance travelled; - driving time or other working time; - breaks in work and daily rest periods; - opening of the box containing the record sheet* ».

Finally, Regulation (EEC) no. 561/2006 of the European Parliament and of the Council of 15 March 2006 on the harmonization of certain social legislation relating to road transport « *lays down rules on driving times, breaks and rest periods for drivers engaged in the carriage of goods and passengers by road* ».

Under the terms of Article 2, it applies regardless of the country in which the HGV is registered, as long as it is travelling within the territory of the European Community.



How long can data collected and processed by a geolocation system be kept?

The personal data collected **cannot be kept indefinitely** in a form that allows the data subjects to be identified.

The APDP therefore considers that, in view of the purposes authorized for the use of a geolocation device in a vehicle, a retention period of **two months** seems proportionate.

As an exception to this principle, it may accept that location data be stored for a period longer than two months if it considers this appropriate **in the light of the justification provided** by the data controller.

For example, such data may be kept for **one year** when they are used, in particular, to provide **proof of the work carried out** and when it is not possible to provide such proof by any other means.

Similarly, such data may be kept for **five years** when the geolocation system is used to **monitor the employee's working hours**.



Who can access the data from the geolocation system?

Access to geolocation data must be restricted to **only those people** who, as part of their job(s), can **legitimately be aware of them in view of the objectives of the system**.

In-house, this may include people responsible for coordinating, planning or monitoring journeys, people responsible for the security of people or goods being transported, or the service provider who has access to the data processing as part of the maintenance of the system.

With regard to the latter, the APDP points out that its access rights must be limited to what is **strictly necessary for the performance of its service provision contract**. In addition, the service provider is subject to the same security and confidentiality obligations as those imposed on the data controller.

In addition, only the necessary information must be communicated, as required.

Example : a customer will not need to know the driver's first and last name if they are just waiting to be picked up. Only the number plate and location data will be required.

The APDP also considers that the communication of data to the Police Department (Direction de la Sûreté Publique) may be justified for the purposes of a judicial investigation.

In this respect, it points out that in the event of transmission, the aforementioned department may only have access to the information within the strict framework of its legally conferred missions.



How to inform data subjects?

The data controller must take the **appropriate measures** to provide its employees with information on the use of their data collected by the geolocation system put in place and facilitate the exercise of their rights.

As a minimum, the employee **must** receive the following information:

- **the identity and contact details of the data controller**, and where applicable, its **representative** established in Monaco or, failing that, within a Member State of the European Union;
- the **purposes** and **legal basis** for the processing;
- the **legitimate interests pursued by the data controller** or a third party where legitimate interests is the legal basis;
- the **categories of personal data** concerned;
- the **period for which the data will be stored** or, where that is not possible, the criteria used to determine that period;
- where processing is based on **consent**, the right to withdraw consent **at any time**;
- the **recipients** or **categories** of recipients;
- the means of exercising **rights of access, opposition, rectification, deletion, limitation** or **portability**;
- the right to **lodge a complaint with the Autorité de Protection des Données Personnelles (APDP)** ;
- where applicable, the **contact details of the Data Protection Officer**.



What security measures should be put in place?

The APDP considers that the data controller must take **all necessary precautions to preserve the security of the data** being processed and prevent unauthorized employees from accessing them, in particular by implementing control and identification measures.

It therefore requests that an **authorization policy** be put in place and that individual access to geolocation data be granted by means of a strong, regularly renewed individual identifier and password, or by any other means of authentication.

The APDP also requests that **automated logging of access** to records be implemented.

Finally, it requires that **all data exchanges be secure**.

Position of the ECHR

In its **Florindo de Almeida Vasconcelos Gramaxo v. Portugal** judgment of December 13, 2022, the European Court of Human Rights (ECHR) held that Article 8 of the European Convention for the Protection of Human Rights is complied with when an employer uses data from a GPS device to dismiss an employee, provided that the employee was aware that the device had been installed.

In this case, the GPS had been installed by the employer in order to **monitor expenses** arising from the use of the vehicle, and the employee, who had been **informed** of the installation, indicated false mileage figures for his company car.

While the Court noted that the GPS tracking did not ultimately comply with national law and the authorization issued by Portugal's Data Protection Authority (CNPd), it nonetheless found that only the difference in mileage travelled had been used as the decisive criterion by the last national court to justify the dismissal, and not the fact that the employee was not working his eight-hour day. This meant that **there was less intrusion into the employee's private life**.

The Court also held that the intrusion was **strictly necessary to the legitimate interest pursued by the employer**, since there was no other, less intrusive means of checking the kilometres travelled on business and in private.

It also noted that only the relevant employees had access to the geolocation data and that the national body had carried out a **detailed balancing** of the respective interests.

In line with its case law established in **Bărbulescu v. Romania**, the Court based its assessment of the compliance of employee surveillance with Article 8 of the ECHR on six relevant criteria: information, scope, legitimacy, subsidiarity, consequence and safeguards.

[To find out more](#)