

THE TRAKMY GUIDE · COMPLIANCE

Tracking employees

The complete compliance guide: GDPR, national data protection authorities, employment law and case law. Understand the framework, choose a legitimate purpose, inform and consult, set the right retention periods, answer employees' rights requests and secure the whole arrangement.

2 months

DEFAULT RETENTION

5

CONDITIONS OF LAWFULNESS

4%

OF GLOBAL TURNOVER, MAXIMUM FINE

01 Why this is sensitive

Freedoms, privacy, social dialogue

02 The legal framework

GDPR, employment law, criminal law, regulators

03 The 7 GDPR principles

What binds every arrangement

04 Legal basis & purposes

Legitimate interest, accepted uses

05 Subsidiarity & prohibitions

Working time as a last resort

06 Proportionality

Collect only what is necessary

07 Informing employees

What the information notice must contain

08 Consulting the works council

Before the installation decision

09 Document & secure

Register, DPIA, access rights

10 Retention periods

2 months, 1 year, 5 years

11 Employees' rights

Access, rectification, objection

12 Special cases

Company cars, autonomous and lone workers

13 Sectors & processing chain

Watch points by industry

14 Penalties & litigation

Regulator, criminal law, unlawful evidence

15 The approach, step by step

From framing to review

16 Compliance checklist

Validate before go-live

17 Balancing test & notice

Method and template

18 Pitfalls, audits, governance

Avoiding them and lasting

19 Worked cases & privacy

Three situations analysed

20 FAQ, glossary & sources

Going further

● EXECUTIVE SUMMARY

If you take away only this

STRAIGHT ANSWER

Three reference points to frame your project before going into the detail.

1 · Lawful, but tightly framed

An employer may fit tracking devices to its vehicles and tools, but never on an unrestricted basis: a determined purpose, proportionate implementation, fair information and consultation of employee representatives. Without these, the arrangement is unlawful and its data unusable.

2 · An ancillary tool, never a default

Regulators and case law impose a principle of subsidiarity: you resort to tracking only where the objective cannot be reached by a less intrusive means.

3 · Compliance protects the employer as much as the employee

A compliant arrangement is enforceable: its data can serve as evidence, the company is shielded from a penalty, and social dialogue stays calm.

"The right question is not only what the law allows, but what the business genuinely needs in order to reach its objective."

HOW TO READ THIS GUIDE

The **GDPR layer** in this guide applies across the European Union. The **employment-law layer** — works council consultation, working-time rules, case law — is **national**: the worked example throughout is **France**, whose rules are among the strictest in the EU. Most member states impose equivalent obligations through different mechanisms. Always have the national layer checked in each country where you deploy.

Why the subject is sensitive

STRAIGHT ANSWER

Tracking touches at once on the employer's managerial authority, on employees' private lives and on social dialogue. It is one of the subjects that generates the most complaints to data protection authorities.

To track an employee is to collect data about their movements, and therefore about part of their life. The subject sits at the crossroads of three logics that do not pull in the same direction: **managerial authority** (organising, securing, proving), **protection of private life** (bounding what is collected) and **social dialogue** (transparency and consultation). Ignore any one of them and the arrangement is open to challenge.

Year after year, tracking of employee vehicles ranks among the leading grounds of complaint to the French regulator (CNIL), alongside video surveillance – to the point that the CNIL created an **accelerated sanction procedure** for these cases. Other European authorities report comparable caseloads.

For the business, the stakes are twofold: a badly designed arrangement does not deliver the legal certainty it was meant to provide (the records will not stand as evidence) and exposes the company to a penalty. Properly framed, it secures assets, makes operations more dependable and renders its data genuinely enforceable.

THE STARTING INSTINCT

Write down the real need – what are you trying to protect, prove or optimise? It is that need, not the technology, that must determine the purpose and the extent of the arrangement.

The applicable texts

STRAIGHT ANSWER

No single text governs employee tracking: compliance results from reading the GDPR together with national employment law, criminal law and regulator guidance, supplemented by extensive case law.

Source	What it imposes	References
GDPR (EU-wide)	Purpose, minimisation, limited retention, information, security, accountability.	art. 5, 6, 13, 30, 35, 83
Employment law (national)	Proportionality, informing employees, works council consultation, working-time records.	FR: L.1121-1, L.1222-3/4, L.2312-38
Criminal law (national)	Penalties for processing carried out in breach of obligations.	FR: art. 226-16 et seq.
Regulator guidance (national)	Accepted purposes, reference retention periods, control arrangements.	FR: CNIL delib. 2015-165 (NS-51)
Case law (national)	Subsidiarity principle for monitoring working time.	FR: Cass. soc. 19/12/2018; CE 15/12/2017

An arrangement can be technically faultless and legally fragile: neglecting a single one of these requirements is enough for the whole thing to be called into question. Items marked national are shown with their French references as the worked example; verify the equivalent in each country of deployment.

The seven GDPR principles

STRAIGHT ANSWER

Seven principles structure any processing. Each of them, on its own, can render an arrangement unlawful if it is not respected.

- ✓ **Lawfulness, fairness, transparency:** a legal basis, no concealed device, clear information.
- ✓ **Determined purpose:** a goal defined before collection, explicit and legitimate; no repurposing.
- ✓ **Minimisation:** only strictly necessary data, no more, and nothing collected "just in case".
- ✓ **Accuracy:** data accurate and up to date; errors corrected or erased.
- ✓ **Storage limitation:** kept for as long as useful, then deleted or anonymised.
- ✓ **Integrity and confidentiality:** protection against unauthorised access, loss and alteration.
- ✓ **Accountability:** the employer must be able to demonstrate compliance at any time.

THE OVERALL LOGIC

These principles converge on a single idea: a tracking arrangement must be targeted, transparent and limited. The broader, the more permanent and the more opaque it is, the further it moves from compliance.

Legitimate interest and accepted uses

STRAIGHT ANSWER

In an employment relationship the legal basis is almost always the employer's legitimate interest, not the employee's consent – which is not regarded as freely given within a relationship of subordination.

Relying on legitimate interest requires a **balancing test**: the company's interest must outweigh the employee's rights and freedoms. The greater the interference (permanent monitoring), the stronger and the more narrowly defined the interest invoked must be.

Asking an employee to "sign" an acceptance does not turn consent into a valid basis, and dispenses with neither the information obligation, nor the works council consultation, nor proportionality.

Purpose	Status	Concrete example
Security of property and people	Accepted	Recovering a stolen vehicle, protecting a lone worker.
Tracking and evidencing services	Accepted	Proving the time of a disputed call-out.
Route optimisation	Accepted	Reorganising rounds from historical journeys.
Allocating resources	Accepted	Sending the nearest team to an emergency.
Monitoring working time	Ancillary	Only where no other means of recording exists.

Working time as a last resort

STRAIGHT ANSWER

For monitoring working time, tracking is lawful only as a last resort (in France: Cass. soc. 19/12/2018; CE 15/12/2017). Several uses are prohibited outright.

The subsidiarity rule

If working time can be recorded another way (a clocking system, self-declaration, supervision by a manager), even less efficiently, tracking for that purpose is not justified. An **autonomous** employee cannot be tracked for that purpose alone.

Prohibited uses

- ✓ Permanent monitoring with no way of switching off during breaks.
- ✓ Tracking outside working time and on the unpaid home-to-work commute.
- ✓ Tracking autonomous employees in order to monitor their time.
- ✓ Tracking employee representatives in the exercise of their mandate.
- ✓ Monitoring speed while driving; disclosing the driver's name to the customer (save where indispensable).
- ✓ Repurposing (any use not declared).

REGULATOR REMINDER (CNIL, NOV. 2023)

Continuous recording with no ability to suspend the device during breaks is an excessive interference with freedoms. Switching off is not a convenience feature: it is a condition of lawfulness.

Proportionality and minimisation

STRAIGHT ANSWER

A compliant arrangement collects only what is necessary and gives the employee control over their private time. For a given objective, the arrangement must be the least intrusive possible.

Situation	Status	Condition / reason
Switch-off available outside working hours	Yes	A "privacy mode" button is mandatory.
Collection limited to working hours	Yes	Configuring the time windows is recommended.
Access restricted to authorised staff	Yes	Permissions managed by profile.
Tracking alone to monitor working time	Ancillary	Only where no other means exists.
Continuous 24/7 recording	Prohibited	Excessive interference with freedoms.
Tracking the home-to-work commute	Prohibited	This belongs to private life.

The employer retains the right to monitor the number and duration of switch-offs and to act on abuse: the control left to the employee is a balance, not a loss of oversight.

Informing employees

STRAIGHT ANSWER

No arrangement may go live without prior, individual information. It is an obligation — and the first lever of acceptability: an informed employee objects less.

The information notice must contain

- ✓ The precise purpose of the arrangement.
- ✓ The identity of the data controller.
- ✓ The legal basis (generally legitimate interest).
- ✓ The categories of data collected.
- ✓ The retention period and the recipients.
- ✓ The rights of access, rectification and objection, and how to exercise them.
- ✓ The ability to switch off outside working time.
- ✓ The DPO's contact details, where one is appointed.

Form & evidence

Information is provided **before go-live**, in writing, to every employee concerned (an individual notice, a contract clause or a policy).

GOOD PRACTICE

Keep proof of delivery (signature, acknowledgement of receipt). In a dispute, it is for the employer to demonstrate that the employee was informed before go-live.

Consulting employee representatives

STRAIGHT ANSWER

The works council must be informed and consulted **before** the arrangement is put in place (in France, the CSE, art. L.2312-38). Skipping this undermines the whole project.

What to present to the works council

- ✓ The purpose pursued and the need that justifies it.
- ✓ The categories of employees concerned.
- ✓ The data collected and how often.
- ✓ The arrangements for switching off outside working hours.
- ✓ Retention periods and who is authorised to access the data.
- ✓ The safeguards (individual information, security, rights).

In the right order

Consultation takes place **before the decision** to install, on the basis of sufficient information. The minutes must be kept: they evidence the compliance of the process.

COMMON MISTAKE

Installing and then informing the works council "for form's sake" reverses the legal order. A late or purely formal consultation can be enough to have the arrangement set aside.

Employee representation bodies and their prerogatives differ across the EU (works council, union delegation, health and safety committee). Identify the competent body in each country.

Register, DPIA and data security

STRAIGHT ANSWER

The arrangement must be entered in the record of processing activities (art. 30), be the subject of a data protection impact assessment (DPIA, art. 35) where the risk is high, and be protected against unauthorised access.

Documenting

The **register** lists the purpose, the categories of data and of people, the recipients, the retention periods and the security measures — the first document requested in an audit. A **DPIA** is required for systematic monitoring of employees on a large scale: it describes the processing, assesses necessity and proportionality, and sets out the measures that reduce the risk.

Securing

- ✓ Access restricted to authorised staff only.
- ✓ Strong authentication (multi-factor recommended) for real-time tracking.
- ✓ Access logging: who consulted what, and when.
- ✓ Encryption in transit and at rest.
- ✓ Automatic deletion when the retention period expires.

GOLDEN RULE

The driver's name must not be disclosed to a customer or principal: that information is of no legitimate interest to them, save in a specific and indispensable case.

Retention periods

STRAIGHT ANSWER

Three periods frame retention: 2 months by default, 1 year for route optimisation or evidence, 5 years for working-time records alone. Keeping data too long is, in itself, a breach.

Use	Period	Concrete example
Day-to-day management	2 months	Routine fleet monitoring, with no particular justification.
Route optimisation	1 year	Journey history used to reorganise rounds.
Evidence of call-outs	1 year	Proving a visit to a customer where no other evidence exists.
Working-time records	5 years	Hours worked only.
Statistics	Beyond	Only after full anonymisation.

THE TAKEAWAY

Any period beyond two months must be justifiable by a precise purpose. Configure **automatic deletion** at expiry: it is the simplest safeguard. These reference periods come from French regulator guidance; other authorities publish comparable but not identical benchmarks.

Employees' rights

STRAIGHT ANSWER

Employees have rights that the employer must organise and answer within the deadlines. Failing to respond is a breach that attracts a penalty (the CNIL has fined €10,000 for it).

- ✓ **Right of access:** to obtain the data concerning them (e.g. their own vehicle's records).
- ✓ **Right of rectification:** to correct inaccurate data.
- ✓ **Right to object** on legitimate grounds relating to their particular situation.
- ✓ **Right to restriction** and right to be informed.

Answering well defuses litigation

Many complaints to regulators arise not from the arrangement itself but from the **absence of a reply** to a legitimate request. A prompt, complete and comprehensible answer often defuses the mistrust.

RECOMMENDED SET-UP

A point of contact (often the DPO), a documented procedure, a target of one month, and a record of every request and every reply.

Company cars, autonomous and lone workers

STRAIGHT ANSWER

Three common situations where the boundary between working life and private life has to be built into how the device is configured.

Company car

Used privately, it makes a **switch-off outside working hours** indispensable. The home-to-work commute is not, in principle, tracked (unless it is paid).

Autonomous & field-based employees

A direct consequence of subsidiarity: an employee who organises their own work cannot be tracked for the sole purpose of monitoring their time. The same applies to home working.

Lone workers

Protection (an automatic alert on a fall, a panic button, a location passed to the emergency services) is a **legitimate** purpose. The risk is use creep: a protective device must not then be used to monitor hours or productivity. Ideally, the location is only ever consulted when an alert is raised.

THE RIGHT INSTINCT

Document explicitly that the purpose is safety and that the data is not used to assess performance.

Sector specifics and the processing chain

STRAIGHT ANSWER

The principles are the same everywhere, but each sector has its traps – and outsourcing the arrangement does not outsource the responsibility.

Watch points by sector

- ✓ **Home care services:** evidencing the visit, protecting lone workers; no continuous tracking between calls.
- ✓ **Delivery / parcels:** proof of delivery and route optimisation are accepted; working time remains subject to subsidiarity.
- ✓ **Road haulage:** do not confuse this with the tachograph (its own regulation, EU-wide); tracking remains subject to general law.
- ✓ **Construction & plant:** often it is the equipment that needs tracking – fit the asset rather than the person.

Processors & agency workers

The company that determines the purposes and means is the **controller**. The provider that hosts or operates the platform is a **processor** (GDPR art. 28), governed by a contract (security, confidentiality). **Agency workers** enjoy the same protections; the split of roles between the agency and the user company must be clarified.

TO LOCK DOWN

An article 28-compliant contract, information given to every worker whatever their status, and a clear map of who does what with the data.

Penalties and litigation

STRAIGHT ANSWER

Failing to comply exposes the company to administrative, civil and criminal penalties – and deprives the employer of any evidence drawn from the arrangement.

€20,000

max fine (CNIL simplified procedure)

€20m / 4%

of global turnover (ordinary procedure)

5 years

+ €300,000 (criminal penalties, FR)

The French regulator operates a **simplified sanction procedure** (2022): a fine of up to €20,000, an injunction with a daily penalty (€100/day), or a formal warning. In November 2023 it issued ten decisions totalling €97,000, targeting vehicle tracking and video surveillance. Serious breaches fall under the GDPR ceilings, which apply across the EU: €20m or 4% of global turnover.

On the **criminal** side, French articles 226-16 et seq. carry up to 5 years' imprisonment and a €300,000 fine; most member states have equivalent offences. Before the **employment tribunal**, evidence obtained from an

unlawful arrangement is excluded from the proceedings: a disciplinary sanction founded on such data becomes ineffective.

THE DOUBLE PENALTY

A non-compliant arrangement stacks the risks: a fine, but also the loss of the very evidence it was meant to secure. The company invests in a tool that, on the day it needs it, is of no use before a court.

The approach, step by step

STRAIGHT ANSWER

A clear sequence avoids omissions. Each step conditions the next: take them in order.

- 1 Define and document the purpose**
A real need, a precise goal, as unintrusive as possible. Check that no less intrusive means would suffice.
- 2 Carry out the balancing test**
Document why the company's interest outweighs the interference with private life.
- 3 Design a proportionate arrangement**
Switch-off outside working hours, an appropriate frequency, restricted access, configured retention periods.
- 4 Inform and consult the works council**
Before the installation decision. Keep the minutes.
- 5 Inform every employee in writing**
An individual notice delivered before go-live, with proof of delivery.
- 6 Document, secure, organise rights**
Register and DPIA; permissions, access logging, automatic deletion; a point of contact for requests. Then review periodically.

Compliance checklist

STRAIGHT ANSWER

Before go-live, check at a glance that the essentials are covered. Every unticked box is an avoidable legal risk.

- ✓ The purpose is defined, documented and limited.
- ✓ No less intrusive means would have sufficed.
- ✓ The legal basis and the balancing test are documented.
- ✓ A privacy mode or switch-off exists.
- ✓ Employees have been informed individually, in writing.
- ✓ The works council was informed and consulted before installation.
- ✓ The processing is entered in the GDPR register.
- ✓ A DPIA has been carried out where the risk is high.
- ✓ Retention periods are configured and justified.
- ✓ Access to the data is restricted and logged.
- ✓ Rights of access, rectification and objection are organised.
- ✓ The data collected is reduced to the strict minimum.

THREE GOOD PRACTICES

Track the **asset** rather than the person wherever possible; favour **transparency**; **review regularly** your purposes, retention periods and access rights.

The balancing test and the information notice

STRAIGHT ANSWER

Founding an arrangement on legitimate interest requires a documented balancing test; every employee then receives a clear information notice.

The balancing test, in 3 stages

- ✓ **A legitimate interest?** A real, current and precise interest (e.g. securing vehicles exposed to theft).
- ✓ **Necessary?** No less intrusive means achieves the same objective.
- ✓ **In balance?** Weigh it against employees' rights and add safeguards (switch-off, restricted access, short retention).

Example: a delivery company adopts theft protection as its purpose, switches tracking off outside working hours, restricts access and retains data for 2 months – and rules out working-time monitoring, which is already covered another way.

The information notice, section by section

- ✓ Subject and purpose.
- ✓ Controller and DPO.
- ✓ Data and frequency.
- ✓ Legal basis (legitimate interest).
- ✓ Recipients.
- ✓ Retention periods.
- ✓ Switch-off outside working time.
- ✓ Rights and how to exercise them.
- ✓ The right to complain to the supervisory authority.

ADVICE

A short notice in plain language is worth more than an unreadable legal document.

Pitfalls, regulatory audits and governance

STRAIGHT ANSWER

Most breaches come down to a handful of recurring mistakes. A compliance file kept up to date and clear governance avoid most of the risk.

Common mistakes

- ✓ Recording continuously with no switch-off during breaks.
- ✓ Installing before consulting the works council.
- ✓ Informing too late or incompletely.
- ✓ Retaining beyond the justified period.
- ✓ Reusing the data for an unplanned purpose.
- ✓ Tracking autonomous employees for working-time purposes.
- ✓ Failing to answer an access request within the deadline.

Keep an audit file ready

- ✓ The processing record entry; a dated balancing test; a DPIA where applicable.
- ✓ The information notice and proof of delivery; the works council minutes.
- ✓ The retention configuration and evidence of deletion; the list of authorised users and access logs; replies to requests.

GOVERNANCE THAT LASTS

A named owner (the DPO), a periodic review of purposes, retention and access, and training for managers: compliance is maintained over time.

Three cases analysed – and why location is sensitive

STRAIGHT ANSWER

Each case is resolved with the same grid: what purpose, what least intrusive means, what safeguards.

- ✓ **A construction SME:** separate vehicles driven by employees (purpose, information, works council, switch-off) from equipment not attached to a person (track the asset: theft protection, allocation).
- ✓ **Home care services:** evidence of visits and lone-worker safety are legitimate; no continuous tracking between visits; working time recorded another way.
- ✓ **Haulage:** recording tools are already available → tracking is not justified for working time, but is relevant for vehicle security.

Location and private life

A location trail does not only say where a vehicle is: cross-referenced over time, it reveals habits and the places a person visits (home, a place of worship, a union office, a healthcare facility), and therefore highly personal information. It is this capacity for **inference** that makes the data sensitive – and justifies how strict the framework is.

WORTH KEEPING IN MIND

The question is not only "am I allowed to?" but "do I need to?". Data you do not collect is data you do not have to protect, justify or delete.

FAQ, glossary & sources

Frequently asked questions

Do we need each employee's agreement?

No: consent is not the basis relied on (it is not freely given in an employment relationship). Prior information, however, is mandatory.

Can we track 24/7?

No: continuous recording with no switch-off during breaks is an excessive interference, and is regularly penalised.

Can we monitor working time?

Only on an ancillary basis, and only where no other means exists. Ruled out for autonomous employees (FR: Cass. soc. 19/12/2018).

Do we still have to notify the regulator?

No: since the GDPR, prior notification has disappeared, replaced by accountability (register, DPIA, documentation).

What about an employee's own car?

Strongly discouraged (private sphere). Prefer a company vehicle or a dedicated device, with collection limited to working time.

Glossary

- ✓ **DPIA**: data protection impact assessment (GDPR art. 35).
- ✓ **Legal basis**: the ground for the processing (here, legitimate interest).
- ✓ **Works council**: the body consulted before any means of monitoring activity (in France, the CSE).
- ✓ **Minimisation**: collecting only what is strictly necessary.
- ✓ **Balancing test**: does the company's interest outweigh employees' rights?
- ✓ **Subsidiarity**: tracking for working time only as a last resort.

SOURCES & DISCLAIMER

GDPR (art. 5, 6, 13, 28, 30, 35, 83) — *EU-wide*. French national layer, given as the worked example: CNIL (practical guidance, delib. 2015-165, statement Nov. 2023); Cass. soc. 19/12/2018 no. 17-14.631; CE 15/12/2017 no. 403776; Code du travail (L.1121-1, L.1222-3/4, L.2312-38); Code pénal (226-16 et seq.). **General legal information current in 2026, not personalised advice**: employment law and employee-representation rules differ in every member state. For a specific situation, and for every country of deployment, consult your DPO or a qualified lawyer.

TAKE THE NEXT STEP

A compliant arrangement, by design

TRAKmy builds tracking solutions designed for compliance: switch-off outside working hours, fine-grained access control, configurable retention periods, data hosted in Europe. Let us talk about your project.

[Request a quote](#)

TRAKmy · La Station · 22 rue Pradier · 30000 Nîmes · France

contact@trakmy.fr · +33 4 30 00 57 25 · trakmy.fr

Data hosted in Europe · General legal information, not personalised advice