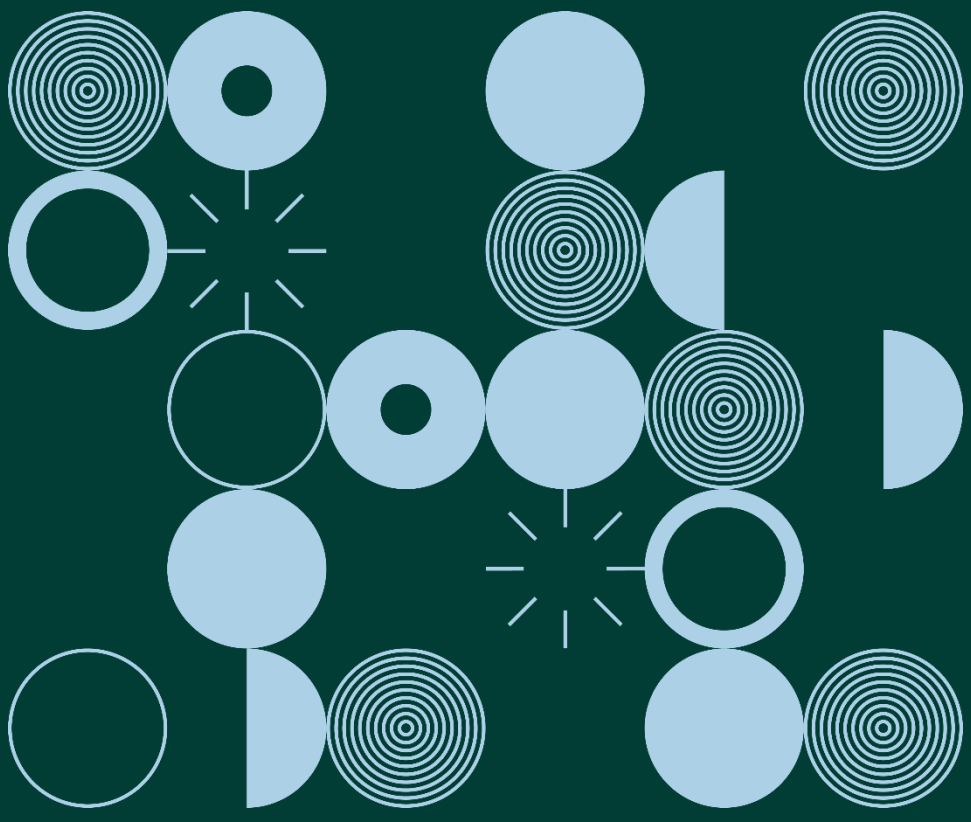
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance Note:

Employer Vehicle Tracking

May 2020



Contents

Employees are entitled to a reasonable expectation of privacy in the workplace as has been established by Article 8 of the European Convention of Human Rights and confirmed by recent case law in the European Court of Human Rights (ECHR).[1] The use of in-vehicle tracking by an employer ('the controller') carries a high risk of interfering with the privacy and data protection rights of the employee.

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 ('the Act') regulate how personal data may be processed. In the context of in-vehicle tracking, it's important to remember that location data qualifies as personal data under the GDPR any time it relates to an identifiable individual.

It is therefore important to note that an employer using vehicle tracking is not just collecting data about the vehicle but also the personal data of individual employee using that vehicle, such as location data or potentially even behavioural data about the employee. In order for in-vehicle tracking to be lawful under GDPR, strict requirements must be met by the employer.

Vehicle tracking should not be used for the general monitoring of staff. The legitimate aim of using such technology may be to track or monitor the location of the vehicles used in an employment context, but it is important to note that employers should not regard vehicle tracking as a method to track or monitor the behaviour or the whereabouts of drivers or other staff.[2]

[1] See *Bărbulescu v. Romania* (Application no. 61496/08) [2017] ECHR 742

[2] See also Opinion 13/2011 on Geolocation services on smart mobile devices, WP 185, 16 May 2011 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2011/wp185_en.pdf

Lawfulness of In-Vehicle Tracking

As a first step employers must be able to demonstrate a legal basis for implementing in-vehicle tracking. Article 6 GDPR prescribes that any processing of personal data is only lawful where it is grounded on a legal basis. It sets out what these potential legal bases are, namely: consent; contract; legal obligation; vital interests; public task; or legitimate interests. Further guidance on the legal bases for processing personal data can be found on the Data Protection Commission's (DPC) website.

In addition to a identifying a legal basis, the employer must ensure that any processing of their employees personal data complies with the principles of data protection laid out in Article 5 GDPR, namely: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability. Some of these principles are discussed further below, however further guidance on these principles of data protection can be found on the DPC website.

Examples of legal bases for in-vehicle tracking may include: compliance with a legal obligation (such as using a tachograph on a lorry) or an employer's legitimate interest in being able to locate the vehicle at any time. Critically, employee consent will only be considered an adequate legal basis in *exceptional* circumstances. This is because of the difficulty in obtaining 'freely given' consent required by Article 4(11) GDPR, given the nature and power imbalance inherent in the relationship between employee and employer.[3] It should be remembered that consent is also revocable at any time at the option of the employee, and they must not suffer a detriment if they do so.[4]

Many employers may seek to rely on Article 6(1)(f) GDPR as a legal basis for processing location data: the necessity to process vehicle location data as a legitimate interest of their business. Critically the processing must be strictly necessary and proportionate for the purpose of achieving that interest, and the legitimate interest being pursued must be balanced against the rights and freedoms of the employee, including their reasonable expectations of privacy.

The legitimate interests of the employer to process personal data that is necessary for the normal development of the employment relationship and the business operation justify certain limitations to the privacy of individuals at the workplace. However, these interests cannot take precedence over the principles of data protection, including the requirement for transparency, fair and lawful processing of data and the need to ensure that any encroachment on an employee's privacy is fair and proportionate.

[3] Article 4(11) GDPR and Recital 43 GDPR further explores the meaning of consent.
[4] See Recital 42 GDPR

Tracking data must be limited and restricted to the specific purpose identified, in line with the principles of 'purpose limitation' and 'data minimisation' (discussed below), so as not to violate the employee's data protection rights.

Article 21 GDPR provides a right for the employee to object to data processing carried out on the grounds of 'legitimate interests'. This would include the right to object to vehicle tracking carried out on those grounds. In the case of objection, the employer may only proceed with the vehicle tracking if it is necessary to achieve a *compelling* legitimate interest which overrides the interests, rights and freedoms of the employee.

Purpose Limitation and Data Minimisation

Closely related to the obligations regarding lawfulness, controllers must also ensure any data processing meets the obligations of purpose limitation and data minimisation, found in Article 5 GDPR.

An employer must ensure they have identified the specific purpose for the data processing at least at the time of collection of the personal data, and in the case of vehicle tracking the purpose should be identified before the purchase or implementation of technology which allows such tracking. This purpose must be explicit and legitimate. The data must not be used for other, further purposes that are incompatible with the original purpose used to justify the initial processing.

An example of further processing, which would be incompatible with the original purpose would be the monitoring and evaluation of employees, where the original purpose of collecting the data was for security in the case that a vehicle was stolen.

In conjunction with the principle of necessity (particularly important when demonstrating a legal basis which provides a grounds for processing) and the principle of data minimisation, employers should remember that vehicle tracking should not be used if the purpose cited could be achieved by less intrusive means. Further guidance on the principles of purpose limitation, data minimisation and further processing can be found here on the DPC website.

Transparency and the Right to be Informed

Employers implementing in-vehicle tracking must also comply with their transparency obligations under the GDPR, and ensure they meet the employee's right to be informed.[5]

An employee must be informed of the existence of tracking and how it operates as well as being clearly informed of all the purposes for which their personal data is to be used, in advance of any such tracking being implemented. This means that the employer must clearly explain to the employee who is using the vehicle concerned what records are being created, why those records are necessary, what they will be used for, how long they will be kept for, who will have access to them and for what reason.

It is critical that employees are made fully aware of the extent of the use of the personal data collected through vehicle tracking. Under no circumstances should an employee be left in a situation in which they are unclear on what information is being collected or the purposes of that tracking. The data collected may not be used for any other purpose, unless that processing is compatible with the original purpose of collection.

An employee should receive prior notice and clear and comprehensive information about the type and purpose of the tracking. The Article 29 Working Party (WP29)[6] recommended that such information should be displayed prominently in every car, within eyesight of the driver.[7] While not compulsory, this may be considered good practice for compliance with transparency requirements.

Employers should devise and make available to drivers a policy on the use of vehicle tracking. In the context of the use of vehicle tracking devices, this document should also set out the employer's policy on the use of company vehicles for private use, if private use is permissible.

Data Protection Impact Assessments (DPIA)

A DPIA should be carried out by the employer where there is an intention to monitor vehicle location data. Article 35(1) GDPR states a DPIA must be carried out where a type of processing is '*likely to result in a high risk*' to the rights and freedoms of individuals.

[5] See Articles 5 and 12 GDPR, and in particular Articles 13 and 14 GDPR regarding a controller's transparency obligations.
[6] A working group consisting of the representative from each data protection authority in the EU, which has now been replaced by the European Data Protection Board (EDPB)
[7] WP29, *Opinion 2/2017 on data processing at work*, 8 June 2017.

When is a DPIA Needed?

Further, the WP29 published guidelines clarifying which types of processing are likely to result in a high risk for the purposes of the GDPR necessitating a DPIA. These guidelines were subsequently endorsed by the European Data Protection Board (EDPB), which replaced the Article 29 Working Party.[8] They recognised the following categories (among other categories cited) as being potentially high-risk data processing:

- ***Evaluation and scoring***: Including profiling and predicting, especially *"from aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements"* (see Recitals 71 and 91 GDPR).
- ***Systematic monitoring***
- ***Sensitive personal data:*** This may include location data depending on the circumstances.
- ***Innovation and technology:*** "*The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology, defined in "accordance with the achieved state of technological knowledge" (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms."*
- ***Data concerning vulnerable data subjects:*** vulnerable subjects expressly include *"employees"* due to a "*power imbalance*" inherent in the relationship meaning the employee is highly unlikely to be able to give free consent (see Recital 75 GDPR).

In most cases, a data controller can consider that processing meeting two of the above criteria would require a DPIA to be carried out. Further, the DPC has identified in accordance with Article 36(4) GDPR that *"systematically monitoring, tracking or observing individual's location or behaviour"* requires a mandatory DPIA. A guide to the types of Data Processing Operations which require a DPIA can be found on the DPC website.

Due to the nature of vehicle tracking and the fact that it will likely (at least indirectly) involve the collection of the personal data of the driver of the vehicle and the systematic tracking of their location, it is highly likely that DPIA will need to be done before implementing such technology.

How Should a DPIA Be Carried Out?

A DPIA should identify and mitigate the risks to an employee's rights and freedoms. A DPIA considering the proportionality of planned measures, and balancing the purpose

[8] Available at Guidelines on Data Protection Impact Assessment (DPIA)

of the measures with the reasonable privacy expectations of the employee should be conducted *prior* to implementing an in-vehicle tracking policy, and must be kept accurate and up-to-date.[9]

This is consistent with data protection by design and by default principles (see Article 24 GDPR and Recital 78 GDPR). Further guidance on carrying out a DPIA is available from the DPC website.

DPIAs must contain:

a) a description of the processing operation along with the purpose of the processing and, where applicable, the legitimate interest for the processing;

b) an assessment of the necessity and proportionality of the processing in relation to the purpose;

c) an assessment of the risks to the rights and freedoms of the data subjects; and

d) the measures to be taken to mitigate the risks.

Of note the WP29 opinion endorsed by the EDPB stated the following, regarding the ongoing obligation to ensure a DPIA is up to date and remains relevant:

> *The DPIA is an on-going process, especially where a processing operation is dynamic and subject to ongoing change. Carrying out a DPIA is a continual process, not a one-time exercise.*[10]

Practical Compliance Steps for Employers

The following are some practical tips for employers who may be considering or have implemented vehicle tracking, to ensure it is done in a limited, proportionate, and lawful manner:

☐ ***Limit the time and/or location when tracking takes place***

It is unlikely that tracking a work vehicle (and particularly a privately owned vehicle being used for work purposes) outside work hours would be lawful, proportionate or necessary within the meaning of the GDPR.

Cases involving the theft of a company vehicle could be an example of a limited circumstance where it may be necessary to access tracking data in order to locate the

[9] See Articles 35(1) and 35(10) GDPR and Recitals 90 and 93 GDPR.
[10] WP29, *Opinion 2017 on guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679,* 4 April 2017.

vehicle, but the proportionality and necessity of the measure would need to be assessed and demonstrated, meeting a high threshold for such an intrusive measure.

Employers should consider accessing the location data only in an emergency situation, such as by activating the visibility of the location by accessing the data already stored by the system only when the vehicle leaves a predefined region. This limited access to location data could be a step towards mitigating a potential infringement of the employee's data protection and privacy rights, and ensuring processing is done in a manner which is proportionate and necessary.

- ☐ ***Take extra care when implementing new technologies, particularly where employees may not expect or be aware of them***

As already noted, new technologies that are more covert in nature carry a high burden for transparency and are considered more high-risk. This is because novel forms of data processing may not be reasonably expected or anticipated by the employee. An employer must ensure that only data which is strictly necessary for the purpose identified (and no other purpose) is processed and the employee is informed of the existence and purpose of tracking in accordance with the employer's full transparency obligations.

It is recommended that employers devise and make available to employees a policy on the use of tracking devices. This document should also set out the employer's policy on the use of company vehicles for private use or private vehicle for company use.

The WP29 stated the following, highlighting the importance of transparency and proportionality, particularly where relying on legitimate interests to justify the processing of personal data:

> *If there are no limits to the processing, and if not transparent, there is a high risk that the legitimate interest of the employers in the improvement of efficiency and the protection of company assets turns into unjustifiable and intrusive monitoring.*[11]

- ☐ ***Implement opt-out measures such as the ability to switch tracking off easily***

In circumstances where a work vehicle is also used for private use outside of working hours**,** the employer must be particularly vigilant in ensuring compliance with GDPR. An 'opt-out' measure must be provided, such as allowing for the tracking to be turned off or disabled with a 'privacy switch', particularly if a privately owned vehicle is used for work purposes.

Employers should also ensure that all drivers are given training on the operation of the opt-out measures. This includes making all new employees aware of the existence of tracking devices and training them in the operation of the privacy switch.

[11] WP29, *Opinion 2/2017 on data processing at work*, 8 June 2017.

- ☐ ***Avoid intrusion into an employee's personal life and limit tracking to what is strictly necessary***

The EDPB, in its recent guidelines on processing personal data in the context of connected vehicles and mobility related applications (1/2020), noted geolocation data as being *"particularly revealing of the life habits of data subjects"*, and high risk in nature where the line between home and work life is increasingly blurred, stating that *"the data controller shall be particularly vigilant not to collect if location data except if doing so is absolutely necessary for the purpose of processing."*

It is unlikely that the tracking of an employee's personal vehicle would ever be lawful outside of work hours as it would amount to a grave interference with the right to privacy and the data protection rights of the employee in the absence of a compelling legal basis grounded in Article 6 GDPR.