



Check-list

Positioning Technology in Working Life

It has become more and more common for employers to use positioning systems of various kinds to check where their vehicles and employees are. When such systems are used, they usually make use of personal data that is regulated by the Swedish Personal Data Act (* see note on the next page).

A positioning system enables close monitoring of individuals and thus entails a risk of inappropriate invasion of privacy. The provisions of the Personal Data Act for protecting privacy have an important function here. This check list shows what requirements are imposed by the Personal Data Act.

Always assume the Personal Data Act applies

- Even if the positioning system rarely contains data that can be directly linked to the individual – for example, a person's name – there are often duty rosters or other ways of linking the vehicles in the system to particular individuals. An indirect link of this kind is enough for the Personal Data Act to apply.
- There are EU regulations for drivers' hours and rest periods as well as regulations on tachographs for hauliers. The Swedish Data Inspection Board does not in principle see any obstacle in the Personal Data Act to employers using positioning technology in order to meet the requirements of this legislation.



Data Inspection Board

Clarify who the controller of personal data is

The controller of personal data is normally the legal person who processes personal data within an operation (a company, an authority or an organisation) and who determines what data is to be processed and what it is to be used for. The data controller is obliged to ensure that no processing of data contravenes the Personal Data Act.

- Sometimes it can be difficult to determine who the data controller is. One example is when, on procuring contractors, municipalities require them to use positioning systems and supply data from these to the municipality. In these cases, the issue of where responsibility for personal data lies depends on the actual circumstances. Factors that play a part include what was agreed during negotiations and what options the contractors have for influencing how the positioning system is designed and used. It is important that in these cases, before the system is taken into use, the parties involved determine who will be the controller of personal data and that this is made clear to everyone affected.
- The positioning system is often purchased as a service from an external supplier. This may mean that this supplier processes personal data on behalf of the employer, for example if it is stored on the supplier's server. The employer must then, as data controller, draw up a written agreement – a so-called assistance agreement – with the supplier. The agreement must stipulate that the supplier may only process personal data in accordance with instructions from the employer and that the supplier is obliged to take suitable technical and organisational measures to protect the data. The assistance agreement may constitute part of another agreement with a personal data assistant, for example an assignment agreement.



Remember that employees are not normally able to consent

- Generally speaking, employers cannot rely on consent from employees to the processing of personal data that occurs when a positioning system is used. This is because employees often find themselves in a position of dependence upon their employers and are therefore unable to give the voluntary consent demanded by the Personal Data Act.
- If the employees are offered reasonable alternatives and are not subjected to any direct or indirect pressure to choose a system based on positioning technology, it may be permissible for the employer to process personal data supported by consent from the employees. One such example is driver's logbook management, where employees can choose between a manually completed driver's logbook and a system based on positioning technology.

* If a network provider is directly involved, for example, by offering positioning via the GSM network, the Swedish Electronic Communications Act (2003:389) also applies. PTS, the Swedish Post and Telecom Agency, performs inspections in accordance with this act. For further information on the Electronic Communications Act, please visit the PTS website: www.pts.se.

- Employers who want to use a positioning system must normally rely on a weighing up of interests. The employer's interest in carrying out the processing must then outweigh the employee's interest in protection from an invasion of privacy. In the overall assessment that must be performed in these cases, the following factors must be considered:
 - the purpose of the processing
 - how the data is handled and how the results are used
 - what information is given to the employees
 - whether the processing can be performed in a way that involves less invasion of privacy
 - what technical and administrative security is available for the data
 - the existence of collective agreements and the content of these and
 - whether the processing follows good practice for the labour market.

Detail the purpose of the processing

- Before a positioning system is taken into operation, it must have been clearly determined for what purposes the personal data is to be processed. These purposes should be set out in writing. It is, for example, usual for employers to cite security as their justification for using a positioning system. In that case it must be clearly stated whether it is for the sake of the staff's security or some other form of security. It must also be stated what checks on employees may be necessary.
- Data that has been collected for a particular purpose must not be used later for other, incompatible purposes. Data collected for security purposes, must not, for example, be used later to measure employees' performance.
- Data in the positioning system must have an actual significance for the purposes determined for the processing. Among other things, the employer must decide whether the purpose of the processing justifies its use at an individual level. If, for example, the purpose is to create statistics, it is enough to collect data in such a way that individuals are not identifiable.
- The purposes must be consistent with good practice. On the labour market this is something that is determined in discussions between different parties on the labour market. The parties need to consider to what extent it is permissible to monitor employees. For example, is it perhaps possible to switch the system off in the employee's leisure time?

Do not keep data any longer than is necessary

- It is the purpose of the processing that governs how long the data can be stored. Before the system is taken into operation, therefore, the employer must decide how long the data needs to be kept on the basis of the purposes decided upon. If, for example, the system is used for work management in real time, there is rarely any justification for keeping the data for anything other than a very short time.
- If the employer wishes to use the data for statistical purposes and therefore wishes to keep it for longer, it must be de-identified. Once data can no longer be linked to any particular individual, the Personal Data Act no longer applies.

Provide clear information for employees

- The employer must inform staff in advance if personal data will be processed in a positioning system, and must also ensure that there are functional procedures for this. The Swedish Data Inspection Board recommends actively passing the information on to the employees, both verbally and in writing, before starting to use the system. The information should also be easily accessible, for example on the intranet or in the personnel files.
- The information for the employees must be detailed yet clear. It must state who the controller of personal data is for this processing (normally the employer), the purpose of the processing, what categories of data will be collected, how long the data will be kept for and whether the data will be passed on to external parties (for example, a company dealing with the running of the system). Employees must also be informed of their right to know what data has been recorded on them (register abstract) and of the possibility of getting any errors rectified.

Protect personal data

- Access to data in the positioning system must be restricted by means of an access management system to ensure that it is only accessible to those who need it for work purposes. Access should be restricted by technical means as far as is practically possible in consideration of the activities being performed and the sensitivity of the personal data. There must be functional administrative procedures concerning how the system may be used. Log-in must be individual in order for it to be possible to follow up on incorrect or unauthorised access.
- There must be a log (i.e. a history of who has logged into the system and what they have done) and procedures for regular follow-up of the log, in order to be able to investigate incorrect use of, or unauthorised access to, personal data in the system. The log must be protected from unauthorised changes. Employees must be informed that logging and following up on logging takes place.
- When personal data from the positioning system is transferred via open networks, such as the internet, the data should be protected by means of encryption.

What the employer may do

It is normally **permissible** to use positioning technology if supported by a weighing up of interests in accordance with the Personal Data Act for the following purposes:

- logistics and distribution of resources
- security
- production of statistics and
- complaints management and customer service.

For the processing to be permitted it must, of course, take place in compliance with the Personal Data Act. The processing must, for example, be reasonably justified for the company's activities and must not be performed too comprehensively or obtrusively.

What the employer must not do

It is normally **not permissible** to use a positioning system if supported by a weighing up of interests in accordance with the Personal Data Act for the following purposes:

- Routine checks of time worked. This is only permitted in exceptional circumstances, where serious abuse of the employer's trust is actively suspected, for example, misuse of time reporting.

The Swedish Data Inspection Board

E-mail: datainspektionen@datainspektionen.se Website: www.datainspektionen.se
Phone 08-657 61 00. Address: Datainspektionen, Box 8114, 104 20 Stockholm.



Data Inspection Board