AUTORITEIT
PERSOONSGEGEVENS

The works council privacy booklet

The role of the works council for privacy in the workplace

Table of contents

1. Introduction: privacy and the works council

Personnel files. Registration of absenteeism due to illness. Cameras in the workplace. Screening of personnel. Employers process a lot of personal data of their employees. Some of this processing can be very intrusive, which is why it is vital that employers take the privacy of their employees into account and that this is discussed within the organisation. Works councils play a crucial role in this. The works council is closely involved in agreements regarding the processing of personal data of personnel and in staff tracking systems.

The Works Councils Act (Dutch: WOR) stipulates that the employer must ask the works council to consent to regulations for which personal data of employees are processed. The employer must ask the works council for an opinion regarding (text from the act):

1. A regulation regarding the processing and protection of personal data of persons working in the company (regulated in Article 27, paragraph 1 under k. of the WOR).
2. Regulations regarding facilities that are aimed at or suitable for observing or monitoring the attendance, behaviour or performance of persons working in the company (or staff tracking systems; regulated in Article 27, paragraph 1, under l. of the WOR).

The works council is therefore partly responsible for the handling and protection of personal data in the workplace. To support works councils in the considerations they have to make, the Dutch Data Protection Authority (DPA) has developed this guide.[1]

It starts with a short questionnaire that helps you understand what exactly is meant by a 'regulation regarding the processing of personal data'. This is followed by an outline of the privacy rules from the General Data Protection Regulation (GDPR). Here you will also find examples and suggestions for questions that you as a works council can ask when you test a regulation or provision as referred to in the WOR against the GDPR.

Especially if an employer is considering using staff tracking systems, he must involve the works council. The guide therefore concludes with assessment questions specifically for this type of processing.

In this guide, we use the terms 'employer' and 'employee'. The term 'employer' is in line with Article 1, paragraph 1 under d. of the WOR, which defines 'entrepreneur' as: 'the natural person or legal entity that maintains an enterprise'. The term 'employee(s)' refers to the person or persons working in the enterprise within the meaning of Article 2 of the WOR ('employee(s)').

The WOR applies to both business and government.

To make the contents of this guide as understandable as possible, the green boxes include examples of an employer who wants to use GPS trackers. This example appears in various places in the guide to make the privacy rules in the GDPR more specific.

[1] This guide replaces the old guide 'Privacy: Checklist for the works council'

2. The right of consent of the works council

The WOR gives the works council the right to consent to a proposed decision on a regulation for the processing of personal data of employees. But what exactly are personal data? And what is processing? You need to know this to determine whether the right of consent applies. For the interpretation of the terms of 'personal data' and 'processing' we look at the GDPR.

Does it concern personal data?

Personal data within the meaning of the GDPR are any information relating to an identified or identifiable natural person (referred to as the 'data subject'). This can involve all kinds of information: not only obvious data such as someone's name, address and telephone number, but also about this person's characteristics, views or behaviour.

Examples of personal data are:

- name, address, citizen service number;
- a video recording of a person;
- data about a person's telephone or computer use;
- the registration number of a car.

Personal data only exist if the identity of the person to whom the information relates can also reasonably be determined. This can be done directly, but also indirectly: for example, when combining different data about a person can be used to determine who it is. The information must be identifiable. Whether data can be identifiable depends on what is reasonably within the capabilities of the enterprise. Or what the enterprise can find out with additional information.

Employer X wants more control over the use of the (company) cars in his fleet. His employers use these cars to visit customers. Employer X wants to have a GPS tracker installed in the cars. This way, employer X can find out which employee is nearest to a customer and plan the most ideal route for his cars during the day. Some employees also drive the company cars privately. Employer X therefore also wants to use the GPS tracker to distinguish between work and private kilometres in the kilometre records.

A GPS tracker collects location data. Employer X knows which GPS signal belongs to which car and which employee is the driver of this car. It is therefore clear that the location data are personal data.

As soon as data can be traced back to an employee, they tend to be personal data. An employee number in a company can be traced back to a person. An employee can also be traced with a personal login name.

The following do not qualify as personal data:

- data about telephone use within the organisation that cannot be traced back to individual employees;
- data aggregated into a set ("aggregated data") about the workforce of a business of reasonable size.

Note! In addition to 'ordinary' personal data, the GDPR also includes so-called special categories of personal data. These are personal data that are particularly sensitive by their nature. These personal data enjoy additional protection under the GDPR.

Special categories of personal data are, for example, data that reveal a person's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership. In addition, this may concern genetic data, biometric data (used to identify a person), data about a person's health or data about a person's sexual behaviour or sexual orientation.

Examples of special categories of personal data at work are:

- data about absenteeism due to illness;
- data about alcohol, medicine or drugs use;
- data about membership of a trade union or political party;
- an iris scan, fingerprint or facial scan (biometric data).

The processing of special categories of personal data is prohibited, unless the company can rely on a legal exception (as referred to in Article 9(2) GDPR).

The company cars of employer X are also used privately by some employees. These employees are concerned about what the GPS tracker records outside working hours. Sensitive private data can be derived from location data.

For example, when the employee visits a church or goes to a medical appointment using a company car. For example, special categories of personal data may (unintentionally) be collected from employees. Has employer X thought about the possibility of disabling the GPS tracker when an employee is having a break or uses the car in his own time?

Medical data are not only a special category of personal data, but also fall under medical confidentiality. It is therefore very important that the employer does not manage these data, but that, for example, the company doctor does.

Are personal data being processed?

The GDPR contains the broad concept of 'processing of personal data.' This is understood to mean: an operation (or a set of operations) on personal data (or a set of personal data), whether or not carried out via automated processes. For example, collecting, recording, organising, structuring, storing, updating or modifying, retrieving, consulting, using, forwarding, distributing, combining, blocking, erasing or destroying data.

The GPS tracker forwards the location data to employer X. He can not only follow the employees live, but can also look up which routes have been taken. Among other things, this constitutes collecting, recording, storing and using data: all processing of personal data.

Who is the controller?

As soon as personal data are processed somewhere, there is always a so-called controller. This is the person who decides whether personal data are processed, and if so, which data, for what purpose and how.

To determine who is the controller, not only the formal legal control is important, but also the actual influence that the employer exerts on the processing.

The WOR regulates what is meant by 'enterprise', 'entrepreneur' and 'director'. In general, the employer (the entrepreneur within the meaning of the WOR) is the controller when processing personnel data.

Employer X wants to use the GPS tracker to send employees to the nearest customer and to check the kilometre records. Employer X determines the purpose and means of processing the location data and is therefore the controller.

If the employer does not process personal data itself, but has the actual operations carried out by a specialist organisation, this organisation is a so-called processor. The controller also remains responsible for processing that is outsourced.

The GDPR requires that the controller and the processor make agreements about the processing. They do this in a processing agreement. This contains agreements about the precise assignment of the processing, what the processor may and may not do with the personal data and what safeguards are in place to protect data. The processor is not allowed to use the personal data for other or his own purposes.

The processor and the controller also agree that the processor will delete the personal data after the processing services have ended. Or that the personal data will be returned to the controller.

In practice, it can be difficult to determine whether an organisation is a processor or controller. A few examples of processors that your enterprise may use to process personal data of employees:

- Payroll administration companies: if the employer provides clear instructions on who should be paid, on what date and for how long the data should be kept, personal data are processed on behalf of the employer. As a processor, the payroll administration company is not allowed to use the personal data for its own purposes.
- IT service provider: if the employer engages an IT service provider to manage the organisation's IT systems, it is often inevitable that the IT service provider has systematic access to employees' personal data. Although access to these personal data is not the main purpose of the support services, the employer, as a controller, must make agreements with this processor.

If the other organisation processes the personal data provided by the employer for its own, self-determined purposes, this organisation is also the controller and there is joint processing responsibility.

For more information, see the Processors file on the website of the Dutch Data Protection Authority (DPA).

Employer X is considering having the location data collected by the GPS tracker analysed by a specialist company, enabling employer X to deploy the fleet as efficiently as possible. Analysing location data is also processing personal data. Employer X is the controller for this processing operation too. The specialist company that is instructed to conduct the analysis is probably a processor.

Is the consent of the works council required?

If the employer intends to make arrangements for the processing of personnel data or a staff tracking system, the employer must submit this to the works council for consent. This also includes changing or withdrawing an existing regulation.

Regulations for processing personnel data exist in almost every organisation. For example, the works council has the right to consent to regulations regarding personnel files, absenteeism registration and payroll administration.

Staff tracking systems are also common. A staff tracking system is a system aimed at - or suitable for - observing employees or monitoring their attendance, behaviour or performance. If an employer does not use a certain system for this, but it could be possible, this system is also a staff tracking system. Staff tracking systems are therefore quite common in organisations.

For example, consider a system in which customer contacts are kept. Or systems in which files are stored and in which it is registered which employee consults a file at what time.

Employer X must submit the proposal to install a GPS tracker to collect and use location data of the cars used by employees to the works council for consent.

Observing and recording people and their behaviour is a hype in this age of digitalisation. The recording of human activities is also increasing rapidly within companies and organisations. Collected data can suddenly appear in assessment interviews or created files. It is important that the employer and employee communicate about this clearly. After all, good employment practices assume that the personal data of employees are handled with care. The works council can contribute to this: every reason to carefully apply the works council's right of consent.

As a works council, you may be able to invoke the right of legislative initiative under Article 23, paragraph 3, of the WOR if you believe that the employer is not taking the necessary action.

If you as a works council do not agree with the employer's proposed decision, the employer can ask the sub-district court judge for permission pursuant to Article 27, paragraph 4, WOR.

If you as a works council are unsure whether a regulation for the processing of personal data of employees is in place, ask the internal privacy officer for advice.

3. The General Data Protection Regulation

The legal framework for processing personal data is laid down in the General Data Protection Regulation (GDPR) and the GDPR Implementation Act (UAVG). The GDPR sets strict requirements for the processing of personal data. These requirements have been elaborated in a number of basic conditions. Are you, as a works council, aware of these important privacy rules?

Purpose limitation

According to the GDPR, personal data may only be collected for 'specified, explicit and legitimate purposes'. The data may not subsequently be further processed in a manner that is incompatible with those purposes. We call this 'purpose limitation'. Simply put: if you collect data for one purpose, you cannot simply use that data for another purpose as well.
Definitely not if this is a completely different purpose.

Facilities that register personal data can easily be used for multiple purposes. Examples include camera surveillance, for example. This can be used not only to secure employees and their belongings, but also to observe employees at work.

The employer (controller) must determine the purpose of the processing before starting processing personal data. It is important that he describes the purpose of the processing as accurately and completely as possible. Are there multiple objectives? Then the employer must mention this separately and test whether it is necessary to collect personal data for this purpose.

In the proposal for the GPS tracker policy that employer X submits to the works council, he explains that the location data are collected for two different purposes:

- to optimise the planning by sending employees to the nearest customers;
- by distinguishing between work and private kilometres in the kilometre records.

If at a later time, employer X decides that he also wants to use the location data for another purpose, it constitutes a change of the existing regulation. Employer X must test the new objective against the privacy rules and submit the change to the works council.

Lawfulness and fairness

Under the GDPR, personal data must be processed in a manner that is lawful, fair and transparent to data subjects.

Personal data may only be processed for a good reason. The legal name for this is 'lawful'. The GDPR lists six reasons (legal bases) on the basis of which personal data may be lawfully processed. For example, the processing of personal data is necessary to perform a contract, to comply with a statutory obligation or to pursue a legitimate interest.

For example, an employer may have a legitimate interest in processing personal data of employees to increase corporate security. The employer must always explicitly weigh the privacy interests of the employees against his own interests as an employer. This weighing of interests must be valid, written down and communicated transparently with employees.

In the proposal, employer X explains that the company has a good reason to use a GPS tracker. But just stating this good reason is not enough.

Employer X must also determine whether the use of the GPS tracker is necessary to achieve its purposes. Has employer X considered whether it is also possible to plan an efficient route without using location data? And is there no other way to distinguish between work and private kilometres, without a GPS tracker? And does the employer's good reason outweigh the employee's breach of privacy?

Consent

One of the possible legal bases is the consent of the person concerned. But for most data processing at work, the employee's consent cannot and may not be used. Because employees are dependent on their employer, they usually cannot give their consent freely. So without feeling pressured and without fear of negative consequences. And consent that is not freely given is not valid according to the GDPR. Only in highly exceptional situations can employees freely consent to the processing of their personal data by the employer.

Special categories of personal data

In principle, it is prohibited to process special categories of personal data, unless a legal exception applies and the controller has a legal basis.

For more information about the principles, see the Are you allowed to process personal data? file on the website of the Dutch Data Protection Authority (DPA).

Correct and accurate

Personal data must be correct as much as possible and updated if necessary. The employer must take measures to ensure that the data are correct and accurate.

The employees of employer X each drive their own car from the fleet. But sometimes, a car is lost, for example, because it is at the dealer for maintenance. The employees then borrow another car. Employer X must ensure that the location data are not linked to the wrong employee. Incorrect data must be erased or corrected by Employer X.

Duty to provide information

Employees must be able to see who processes their data and for what purpose. The employer therefore has a duty to provide information. This means that the employer must inform employees what happens to their data before the employer actually processes those data.

For example, when a new employee is hired. The personnel officer must then provide information before the employee completes the necessary forms for personnel and payroll administration.

This also applies, for example, if an employee is given a lease car. The employee must then receive information in advance about the data processing when using a car: which data are recorded and for what purpose.

If the employer receives data not from the employees themselves but from another party, the employer has to inform the employee about this at the time the employer records the data.

Employer X must clearly inform the employees about his plan to use GPS trackers. And how this affects employees. How does the GPS tracker work? Why is location data collected?

Data minimisation

Personal data must be sufficient, relevant, and limited to what is necessary for the purposes for which they are processed. Simply put: you are not allowed to process more data than you really need. We call this data minimisation, or processing as little data as possible.

To assess whether this is the case, you as a works council can ask the following questions:

- Does the employer make sufficient use of the options to anonymise personal data?
- Does the employer have to collect data at an individual level or can he limit himself to data at the level of a department or the company as a whole (aggregated level)?
- Does the employer have to record data about all employees? Or can he limit himself to collecting information about employees in certain positions or in certain places?
- Can the employer limit himself to a sample or must the employer continuously record data?

Personal data may not be kept for longer than is necessary to achieve the purposes for which they were collected. So: data no longer needed? Delete them!

In his proposal to use GPS trackers, Employer X has explained that one of the purposes for collecting location data is to be able to send employees to the nearest new customer. To achieve this purpose, employer X needs insight into the employees' current locations. Once the location data are no longer up to date, they will no longer be used for this purpose. For the other purpose, keeping track of kilometre records, the location data themselves are not relevant: they are converted into the driven distance in kilometres.

The works council therefore critically questions employer X about what happens to the (old) location data. Are these erased immediately?

Security

Personal data must be processed in such a way that appropriate security is guaranteed. This must be done by taking appropriate technical or organisational measures. This means that the data must, among other things, be protected against unauthorised or unlawful processing and against intentional loss, destruction or damage.

To determine the necessary level of security, the employer must carry out a risk analysis. The nature of the data and the circle of users are important during this analysis.

If as a works council, you want to assess whether the employer has insight into the risks entailed by a (proposed) regulation for processing personal data of employees, you can ask the following questions:

- What does the employer do to identify the risks in a timely manner?
- Are the risks periodically reassessed?
- Has a procedure been established to test whether the security measures are (still) effective?

See also *DPIA and prior consultation* (p. 12).

The employer must ensure that access to the personal data of data subjects is limited. This means, for example, that only authorised employees may have access to personnel files. The employer must think very carefully about security before he starts collecting personal data. The security of personal data within organisations must be a point of continuous attention.

In the GPS tracker proposal, employer X explains that all employees are given a login code that gives them access to the environment where the live locations of the cars are available.

The employees of employer X don't like the thought that their colleagues can continuously monitor them. When the works council points this out to employer X, it turns out he had not thought of that.

When answering the question of what an appropriate measure is, the employer must take the state of the art into account.

Some examples of security measures are:

- access security with multi-factor authentication (verifying user identity with at least two different types of authentication factors);
- registering who has had access to the data (logging);
- pseudonymisation of personal data.

As a works council, you can seek advice about this from the information security officer or data protection officer (DPO) of your organisation. You will also find more information about this on the website of the Dutch Data Protection Authority (DPA).

A data breach can occur even when appropriate security measures have been taken. This means that personal data have been accessed or that the data have been destroyed, altered or released without the intention of the employer or without this being permitted by law. The employer is obliged to keep a data breach register. If it is a serious data breach, the employer must report this data breach to the Dutch Data Protection Authority (DPA) and in some cases also to the data subjects.

For more information, see the subject on Security on the website of the Dutch Data Protection Authority (DPA).

Rights of data subjects

Employees have various privacy rights. This allows them to maintain control over their personal data. They have the right to access their personnel file, among other things. They can also request rectification, addition or deletion of their data. This allows them to defend themselves against incorrect or incomplete data in the file.

> The employees of employer X believe they must be able to regularly check the kilometre records that are kept by the GPS tracker. Are these records the same as the car's odometer? The works council therefore asks employer X how employees can access these data.

If the employer processes data on the basis of a legitimate interest, the employer must inform the employees of their right to object. Employees have the right to object to this processing if they believe their privacy interests outweigh the interests of the employer. For example, when there are special personal circumstances. The employer is then not allowed to process the data if the legitimate grounds put forward by the employer for the processing do not outweigh the interests of the employees. Or when it is not clear whether these grounds carry more weight.

Lastly, the employer must offer employees the opportunity to have their data transferred. This is called the right to data portability. It means employees can receive their personal data in a structured, common and machine-readable format. And then transfer these data to another organisation.

For more information, see the Rights of data subjects on the website of the Dutch DPA.

DPIA and prior consultation

Under the GDPR, a controller may be obliged to carry out a data protection impact assessment (DPIA) before he can start processing data. A DPIA is an instrument for identifying the privacy risks of a data processing operation in advance, so that measures can be taken to reduce these risks. A DPIA is required for data processing operations that will probably entail a high privacy risk for the data subjects.

The Dutch Data Protection Authority (DPA) has drawn up a (non-exhaustive) list of types of processing for which a DPIA is mandatory. The large-scale or systematic processing of personal data to monitor employee activities appears on this list. This therefore falls under the DPIA obligation. If a processing operation is not listed, the employer must decide for itself whether the data processing operation entails a high privacy risk. To this end, the employer can use the 9 criteria drawn up by the EU data protection agencies.

> In the GPS tracker proposal, employer X explains that he has carried out a DPIA and that he will take appropriate measures to mitigate all of the identified risks.
>
> The works council would like to know more about these risks and therefore asks whether employer X wants to share the DPIA with the works council.

If the DPIA shows that the data processing operation poses a high risk, and the employer cannot find measures to mitigate this risk, the employer has to consult with the Dutch Data Protection Authority (DPA) before starting the processing operation. This is called prior consultation. The Dutch Data Protection Authority (DPA) will in that case provide advice

about how the employer can mitigate the risks of the intended processing. The Dutch Data Protection Authority (DPA) can also advise the employer to refrain from processing altogether.

If a DPIA is not mandatory, the Dutch Data Protection Authority (DPA) recommends carrying out a privacy risk assessment, as a form of sound management.

Accountability

The controller must be able to demonstrate that he complies with the GDPR obligations. This is called accountability. The GDPR lists a number of mandatory measures that the controller must take to comply with this accountability.

Some examples:

- keeping a processing register;
- carrying out a risk assessment (DPIA) (if necessary);
- keeping a data breach register.

In addition to these mandatory measures, there are other measures that can help the controller to demonstrate that he complies with the requirements of the GDPR. For example, by rendering account in the annual report or adhering to an approved code of conduct.

Data Protection Officer

The Data Protection Officer (DPO) is someone who supervises the application of and compliance with the GDPR within the organisation. The DPO provides advice and insight to the controller. There are three situations under the GDPR in which an organisation is obliged to appoint a DPO:

1. the organisation forms part of the government or is a public organisation;
2. the core activity of the organisation is to track individuals on a large scale or map their activities;
3. the organisation processes special personal data on a large scale.

If a DPO is not mandatory, the controller may choose to voluntarily appoint a DPO.

The employer must involve the DPO properly and in a timely manner in all matters relating to the protection of personal data. Have you, as a works council, ever spoken to the DPO about the processing of personnel data?

The works council has taken note of the DPIA for the use of the GPS tracker. The risk assessment of employer X has raised a couple of new questions and the works council is wondering what the DPO's opinion is. The DPO has issued advice in response to the DPIA. The works council requests the advice of the DPO and invites the DPO to provide an explanation during the next works council meeting.

Data traffic with countries outside the EU

Transferring personal data to a country outside the European Union (EU) is in principle only permitted if that country has an adequate level of data protection. This means: equivalent to the level of protection of the GDPR. If there is no adequate level of protection, transfer is only permitted on the basis of one of the statutory provisions of the GDPR.

Some examples of situations in which data are provided to countries outside the EU:

- the employer has outsourced salary payments to a payroll administration company (processor) outside the EU;
- the employer uses the services of a cloud provider to store data (including personal data), whereby the data are stored on servers in the United States.

It is important that you, as a works council, check whether the organisations with which the employer shares personal data of employees are located in the EU.

If the employer plans to use a processor outside the EU to process personal data of employees, then as a works council, you can ask the following questions:

- Is it necessary to use a processor outside the EU? Has the employer considered European processors for this processing operation?
- How is the protection of the employees' data guaranteed when their personal data are provided to the processor outside the EU?

Employer X is still considering asking a specialist company to analyse the location data that are collected by the GPS tracker. Because the location data are processed for a new purpose in this analysis, employer X makes a new proposal and submits it to the works council for approval.

The documents tell the works council that the processor that employer X chose to analyse the location data stores the data in a database outside the EU. The works council asks employer X why he chose this processor.

For more information, see Transfer within and outside the EU on the website of the Dutch Data Protection Authority (DPA).

4. Assessment questions for staff tracking systems

More and more employers want to monitor employees through staff tracking systems. For example, when employees work from home. This raises questions about the privacy of employees. What questions can you as a works council ask about this?

If you assess staff tracking systems, you can, pursuant to Article 27, paragraph 1, under l. of the WOR, verify the proposed regulation on the following points. Does the organisation have a Data Protection Officer (DPO)? They can assist you with advice.

1. **Does it concern a staff tracking system?**
As a works council, you have the right of consent if 'measures are aimed at or are suitable for monitoring or checking the attendance, behaviour or performance of persons working in the enterprise' (Article 27, paragraph 1, under l. of the WOR). In everyday language we call such 'measures' (or facilities) staff tracking systems. If there is a staff tracking system, you can assume that this also involves the processing of personal data.

   The design of a system often shows that it is aimed at tracking staff. The law adds a criterion that the consent of the works council is also required if a system is suitable for this. The possible effects of such a system must therefore be examined. Can staff be tracked, even if this is not (yet) done in practice? Then it still qualifies as a staff tracking system.

   Some examples of staff tracking systems are:

   - a system that registers attendance, time and access;
   - a track & trace system in cars and trucks, such as a GPS tracker, black box or on-board computer;
   - software that records keystrokes, email traffic and/or Internet use of employees, for example;
   - camera surveillance in the workplace;
   - wearables, such as a smartwatch;
   - a system that keeps track of contact with customers;
   - a system that supports the handling of work (workflow or case system);
   - a facility within a system that registers access to (sensitive) files by employees (logging);
   - a system that uses a pass or badge to register an employee's attendance and/or location within a building.

2. **Is it necessary to use a staff tracking system?**
The next question you as a works council should ask is whether the use of a staff tracking system is necessary within the enterprise. Only if the answer is yes, the method will be discussed.

As a works council, you can ask the following questions about the necessity for a staff tracking system:

- Why does the employer plan to use this facility? Or why is the facility used?
- Is there a legal or contractual obligation? If not, is there any other reason why it is necessary to implement or use the facility?
- If there is no external necessity, can the employer demonstrate that he has a legitimate reason (legitimate interest) to use the facility?
- How do the interests of the employer relate to the interests of the employees?
    - How invasive is the observation?
    - Are the interests of employees at risk?
    - Is it possible to achieve the purpose envisaged by the employer in a way that is less intrusive for the employees?

Using a staff tracking system is always an invasion of employee privacy. This is not to be taken lightly. What is important is whether the facility is reasonable in relation to the intended purpose. And whether the employer can also use less invasive means.

The facility can be so intrusive that you as a works council - based on the interests of the employees and in view of the purpose - do not want to consent to the regulation. Or only under conditions. Such conditions for the use of the facility can be included in the regulation.

If the employer plans to process personal data on a large scale and/or to systematically monitor activities of employees, the employer must first carry out a DPIA.

3. **Are employees informed of the observation in advance?**
In particular, employees must receive information about:

- the purpose of the observation;
- the timing and use of the data collected;
- retention periods.

In any case, employees must be informed of this at the time the system is introduced. This can be done, for example, with rules of conduct or a protocol.

Questions that are important in this case include:

- How are the personal data used?
- What are the possible consequences of this for employees?
- Who has access to the personal data that are processed?
- How is unauthorised access checked?

Structural covert observation is not permitted. Occasionally, covert monitoring may be justified, provided strict (additional) conditions are met. There must be reasonable suspicion about one or more employees that justifies the use of such an invasive check. This requires that other resources have been exhausted and that a substantial interest of the company is at stake. Employees must know that a staff tracking system may be used covertly in exceptional situations. The covert monitoring of employees is subject to carrying out a DPIA.

Questions you as a works council can ask about covert monitoring:

- Is the organisation aware of what behaviour is not tolerated and have employees been warned about this?
- Has the employer tried in any other way to prevent or detect the harmful behaviour?
- Is it sufficiently guaranteed that the facility will not be used rashly?

4. Is the personnel assessment based solely on the data collected with staff tracking systems?

It is important that data are not simply recorded in the personnel administration. And that staff assessments do not take place solely on this basis. Furthermore, employees must be given the opportunity to respond to the results shortly after the observation by the staff tracking system. Their views on this must be attached to the results.

Want to know more? Also view the information on the website of the Dutch DPA DPA and/or the website of your sector or trade association.