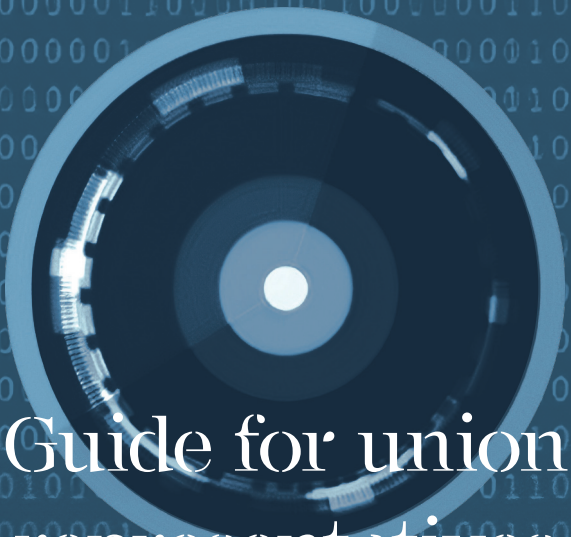


Guide for union representatives on surveillance and monitoring in the workplace

Monitoring undermines the trust between management and employees

Employee performance monitoring is spreading rapidly in these years. Sometimes with a specific purpose, other times because it is an automatic part of digital management systems and the software that companies use for data processing.

Monitoring challenges the trust-based relationship between employer and employee that characterises the Danish labour market. But it also interferes with the employee's rights to healthy and safe working conditions, protection of privacy and personal data, and to be notified of control measures. There is a fine line between practical and necessary monitoring and the feeling of being under surveillance.

As a union representative, you play an important role in ensuring trust and cooperation, which is why IDA has created this guide with suggestions on how to start a dialogue about monitoring in your workplace.

In the EU's European Company Survey[1], 22% of Danish companies surveyed said that they "monitor employee performance".

Who this guide is for

This guide is for you if you are a member of the works council, a union representative or a health and safety representative. It may also be relevant to you if, for example, you are a member of the information security committee or have a role where you are involved in making decisions about introducing or implementing IT systems that monitor employees.

What is employee monitoring?

Digital monitoring aims to collect information about our use of PCs and work phones, for example, to ensure that we as employees do not download harmful programs or use our work PC for illegal purposes. Another widespread practice is the recording of when employees arrive at and leave the office, as well as location data through GPS information. But work effort, language use and efficiency can also be recorded, and information about well-being, behaviour and mood can be made available to employers through dedicated monitoring systems.

Monitoring can extend beyond working hours, tracking things like employees' use of social media, sleep, exercise and health. Using the same PC and mobile phone for both work and personal purposes increases the ability for employers to track behaviour, habits, friends, and relationships.

Monitoring systems are increasingly integrating artificial intelligence and are used for hiring, profiling, and evaluating employees, predicting things like stress or the likelihood of resignation. They can also provide recommendations for salary or dismissal decisions.

Artificial intelligence software is often characterised, for example, by the collection of data from different types of sources and/or the use of machine learning. Machine learning is a function where an algorithm automatically incorporates new data in real-time and makes its own updates, recommendations or even decisions. Artificial intelligence can thus generate outputs that affect the actors and environments they interact with.[2]

Duties and rights

Employee monitoring cannot be introduced at workplaces in Denmark without discussions in the works council or with union representatives. This is because there are a number of requirements attached to the employer's management rights and thus to the introduction of employee monitoring. An essential requirement is that the monitoring does not have an invasive effect.

The protection against invasive control measures is also embedded in international conventions on human rights and labour rights and in the EU Charter of Fundamental Rights. Hence, the right to privacy also applies to the insight employers gain into employees' private sphere through surveillance systems.

GDPR also applies when we are at work. The personal data recorded about employees must be processed in a way that fulfils the requirements of personal data protection legislation. For example, if the workplace collects location data, it triggers an obligation for the employer to investigate what the consequences of the surveillance are for the affected employees and to test whether the measure is proportionate to the purpose.

Employee monitoring is also an issue for the health and safety organisation. Digital surveillance can affect both physical and mental health and must therefore be included in the employer's obligation to create a safe and healthy physical and psychosocial working environment that is in line with the technical developments in society.

The introduction of a monitoring system typically also needs to be assessed by the Data Protection Officer, the DPO.

Examples of protection against invasive control measures
In the state sector, the Circular on Agreement on Control Measures applies, which states that control measures must be objectively justified by operational reasons and have a reasonable purpose, and that they must not be invasive of employees or cause them any loss or significant inconvenience. For home workplaces, it states that control measures that violate privacy must not be introduced.

The main agreement between the Confederation of Danish Employers (DA) and the Danish Trade Union Confederation (FH) specifies a number of requirements for the introduction of control measures in the labour market. According to this agreement, control measures can only be implemented if there is an operational purpose and must not be invasive to the employees. In addition, the employer has a duty to inform employees of new control measures no later than 6 weeks before they are implemented. The information is provided through the works council or union representatives, and otherwise directly to the employees.

Protection of privacy
The European Court of Human Rights and the European Court of Justice have ruled that employer surveillance of employees must be considered an interference with employees' right to privacy. Such interference must therefore be lawful, have a legal basis and be both necessary and proportionate to its purpose. If these requirements are not met, the interference will constitute a violation.

Protection of personal data
Under the GDPR, employers must inform employees that their data will be collected and processed as part of a surveillance measure. This entails a requirement for impact assessment and compliance with requirements for proportionality, data minimisation, lawful basis, and transparency in the use of the data. If cloud-based tools are used, it must also be analysed whether employee data is transferred to a country outside the EU.

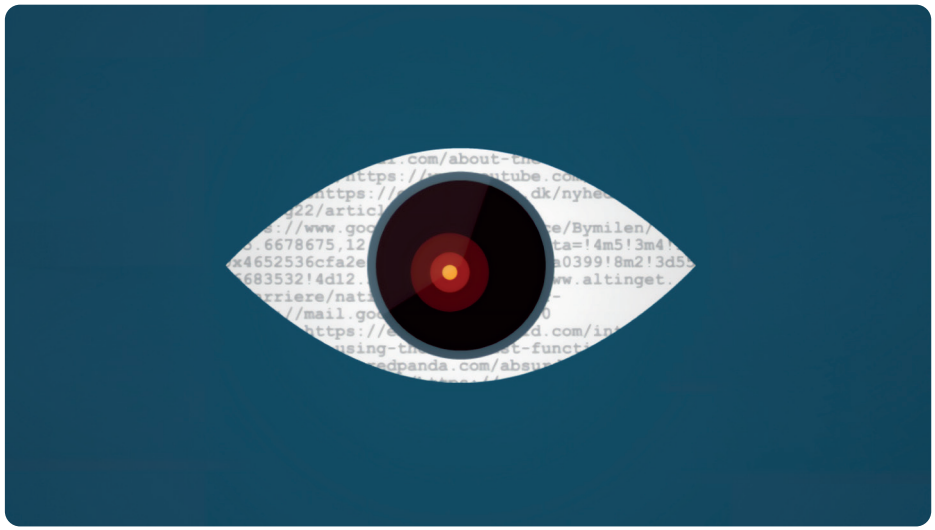
As an employee, you also have some specific rights to enable you to control your personal data. These include

- The right to be informed about the processing of your personal data
- The right to access information about yourself
- The right to have incorrect information rectified
- The right to have data erased
- The right to object
- The right not to be subject to automated decision-making and profiling

Health and safety
The Danish Working Environment Act requires the establishment of a health and safety organisation to create a framework for cooperation, contact and dialogue on health and safety between the employer and employees. The employer's obligations include, among other things, regularly conducting a workplace assessment (APV) and work environment discussion to examine whether the co-operation is healthy and safe. Intended and applied monitoring should therefore be included in the review of the working environment.

Particular issues to be aware of

Some systems go far beyond the boundaries of what we normally share with our workplace. One example we've come across is from a UK insurance company that gives employees bonuses if their sleep tracker shows they're getting enough sleep.[3] This type of system goes far beyond the realm of the workplace and challenges the employee's privacy, trust, adaptability and loyalty to the workplace.



Here are examples of areas where it's worth paying special attention:

- Workplace health: There is a difference between a voluntary programme, such as joining a running club, and health programmes that involve monitoring, where the workplace has access to your health data, such as how often you exercise, how many steps you take per day, etc.
- Monitoring via devices: Many workplaces provide mobile phones and PCs for employees, which can also be used for private purposes. If this is the case, there should be clear agreements about which of the collected data the workplace has access to. This could include, for example, where the employee spends their free time, website searches, social media activity or private correspondence.

HR tools

Many Danish workplaces have already implemented digital HR tools. It can therefore be a good idea to ask about the systems that are already in use. Our survey shows that employees who have had a dialogue with their manager about the IT systems in place are significantly more positive than those who know that data is being collected but have not had a dialogue with the employer[4].

Regardless of the reason for introducing employee monitoring, it is necessary for the workplace to think critically about the consequences of data collection for the individual employee, the work environment as a whole and the company's reputation. You should also not hesitate to make demands of the system provider, such as transparency. The employee should be able to find out how the algorithm arrived at a recommendation or decision: what values the algorithm is programmed to use in its calculations and how much weight they carry. A non-transparent wellbeing tool can quickly create distrust and make it harder for managers to exercise their right to manage and distribute work on a reasonable basis.

Rather a joint agreement than individual consent

Who should have the dialogue can vary from workplace to workplace. It is not advisable for each employee to be asked to give consent. Consent is characterised by the ability to say no, and this is not necessarily a real option if the workplace or task performance is dependent on the system being used. Instead, you can work towards an agreement that when new systems are to be introduced that have consequences for employees, they must be submitted for consultation to the works council, also known as the MED committee. Here, employee representatives can take a position on the system and possibly propose changes to how the system is used, what data is collected and how long the information is stored. In workplaces where there are no union representatives, the health and safety representatives (AMRs) can be consulted.

How can you carry out the dialogue process?

It's important to start a good and constructive dialogue about how digital systems contribute to monitoring without becoming surveillance – Regardless of whether the purpose is better IT security, stress management or productivity improvements. The dialogue should be based on the purpose of the IT system. Some purposes are perfectly legitimate, such as requirements for high IT security. It could also be that the workplace asks employees to download an app to their work phone, for example, to keep track of how many hours they work if they have a maximum working time limit. One response to such initiatives can be to recommend that employees have their own PC and phone – and that the employer will, of course, provide a work phone if an app download is necessary.

TOOL:
Which questions should I ask?

Data collection is not necessarily visible to the person being monitored. Therefore, it can be difficult to know which questions to ask. We've compiled a list of questions that will often be relevant.

1. Are digital systems used to manage or recruit employees in this workplace?
2. Where are these systems used and which employees are affected by the system?
3. Have the affected employees been informed?
4. What is the purpose of the system?
5. How is it being used?
6. Can additional features be added to the system?
7. Who is responsible for using the system?
8. Who designed the system, who did we buy it from and who owns it?
9. What does the contract between developer, vendor and employer say about
   - access to and control of data and
   - how the system is monitored, maintained and possibly redesigned?
10. To what extent is artificial intelligence used in the system and for what purpose?
11. When is data deleted and do third parties have access to data?

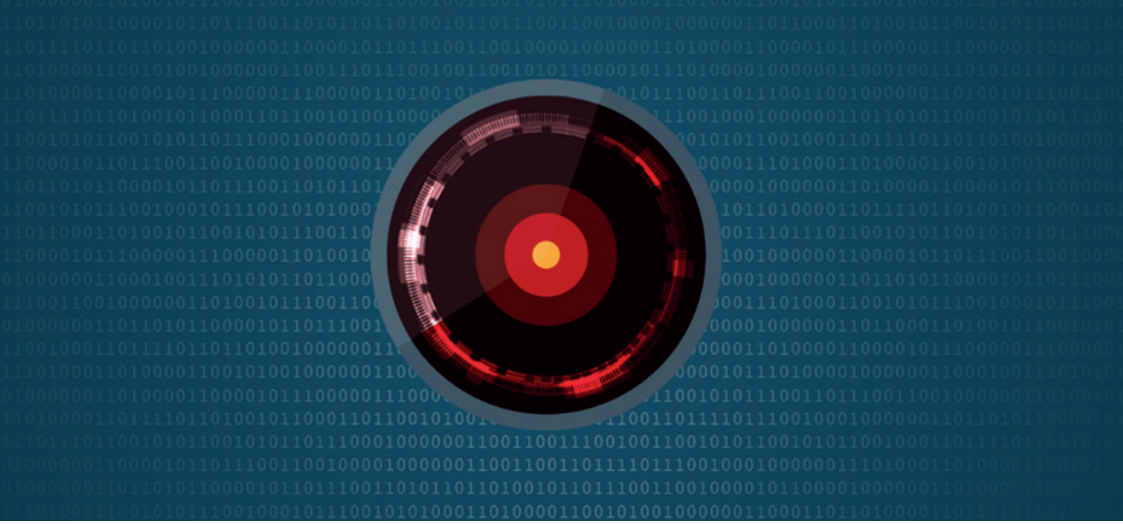
End notes

1 Use of data analytics for monitoring employee performance (Digitalisation) visualisation : European map by : Establishment Size, All, answer : Yes – European Company Survey – Data visualisation ECS2019 (europa.eu)

2 EU AI Act Proposal, article 3 (1).

3 https://ida.dk/raad-og-karriere/overvaagning-paa-job/kritik-af-overvaagningssoftware-vokser

4 https://ida.dk/om-ida/nyt-fra-ida/hver-femte-medarbejder-har-foelt-sig-overvaaget-paa-arbejdspladsen



Want to know more?

Find more information on workplace surveillance and employee rights on our website:
https://english.ida.dk/workplace-surveillance