DIGITAL PROGRAMME

Guide
October 2026

DATA RIGHTS ARE WORKERS' RIGHTS

A GDPR GUIDE TO PUSH BACK ON WORKPLACE MONITORING



DEMOS HELSINKI

FEPS
FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES

Kalevi Sorsa Foundation · Friedrich Ebert Stiftung · ECLM · Handels · delta · PAM · SAK · DANSK METAL · HK · FH

TABLE OF CONTENTS

USEFUL TERMS TO KNOW **3**

TO THE READER **4**

1 STEP-BY-STEP INSTRUCTIONS FOR USING THE RIGHTS GRANTED BY THE GDPR IN EVERYDAY SITUATIONS 6

2 UNDERSTANDING ALGORITHMIC MANAGEMENT AT WORK AND ITS FOUNDATIONS IN DATA 16

3 YOUR BEST TOOL TO CHALLENGE ALGORITHMIC MANAGEMENT AT WORK: THE GDPR 21

ANNEX 1: A TEMPLATE FOR REQUESTING ACCESS TO ONE'S DATA FROM THE EMPLOYER **29**

ANNEX 2: OTHER LEGISLATIVE TOOLS TO STEER AND CHALLENGE ALGORITHMIC MANAGEMENT **31**

REFERENCES BY SECTION **34**

ABOUT FEPS AND PARTNERS **37**

Useful terms to know

Algorithm: a set of rules a computer follows to solve a problem.

Algorithmic management: when computer programs and software take on the role of a human boss, for example, to assign daily tasks or track worker performance, or even to decide who gets hired or fired. The algorithm executes these instructions through an automated or semi-automated process. (Managers decide on the deployment of these systems, but often don't fully understand the decision logic they follow.) It makes its decisions based on data collected from workers (such as the number of keystrokes or the tone of voice in customer calls, as in the example case of tracking worker performance).

Data: digitised information collected from workers. Under the GDPR, it is called "personal data".

Data controller: the individual, company or public authority that decides why and how personal data is collected.

Datafication: a process where workers' actions, behaviours and performance (like keystrokes, movement or tone of voice) are turned into quantifiable digital data that can be monitored and used to make management decisions.

Data Protection Authority (DPA): an independent public body that enforces privacy laws and protects personal data rights within its jurisdiction. It advises organisations on data processing rules, handles citizen complaints regarding data misuse and imposes penalties where necessary.

Data protection impact assessment (DPIA): a formal process required by the GDPR – the Data Controller needs to conduct to identify, assess, and minimise the impact on workers of projects that handle personal information and that present high risks for the rights and interests of these workers.

Data Protection Officer (DPO): an expert in the organisation who monitors personal data processing and ensures the organisation is compliant with privacy laws, such as the GDPR. Advises management on regulatory duties and DPIAs and informs employees of their rights.

Data rights: the concrete legal protections (often grounded in laws like the GDPR) that give workers influence over their information.

Collective data governance: because an individual worker cannot freely say "no" to being tracked by an employer without risking their job, unions must use collective data governance. This means that the union negotiates the rules on how data can be collected and used in the workplace, on behalf of the whole workforce.

GDPR (the General Data Protection Regulation): EU legislation that applies directly to all EU member states and members of the European Economic Area. It aims to protect people's personal data by regulating how data is processed by organisations.

Individual data governance: an approach that relies on single workers managing their own data rights, such as granting personal consent for an employer's data collection or requesting access to their personal files under privacy laws like the GDPR.

Participatory data stewardship: the responsible use, collection and management of data in a way that workers are informed about how their data is used and actively consulted and involved in the development of data governance in the workplace.

Register of processing activities (RPA): an organisation's detailed, internal document that describes how an organisation collects, uses and stores personal data.

To the reader

Dear reader,

"Algorithmic management", a process where computer programs and software take on the role of a human manager to, for example, assign daily tasks or track worker performance, has become increasingly common in the Nordics. According to a recent study, 75% of the 6,000 respondents surveyed from Denmark, Finland, Norway and Sweden reported that at least one algorithmic management tool is used in their workplace. If not followed closely and steered by union representatives, the deployment of algorithmic management systems can pose serious risks to workers' autonomy, privacy, health and wellbeing, and how the fruits of technological development are divided between workers and capital.

With this guide, we want to support you in negotiating and challenging the use of algorithmic management in your workplace. The guide is targeted at shop stewards across the Nordics, but other union representatives and workers will likely find it useful, too.

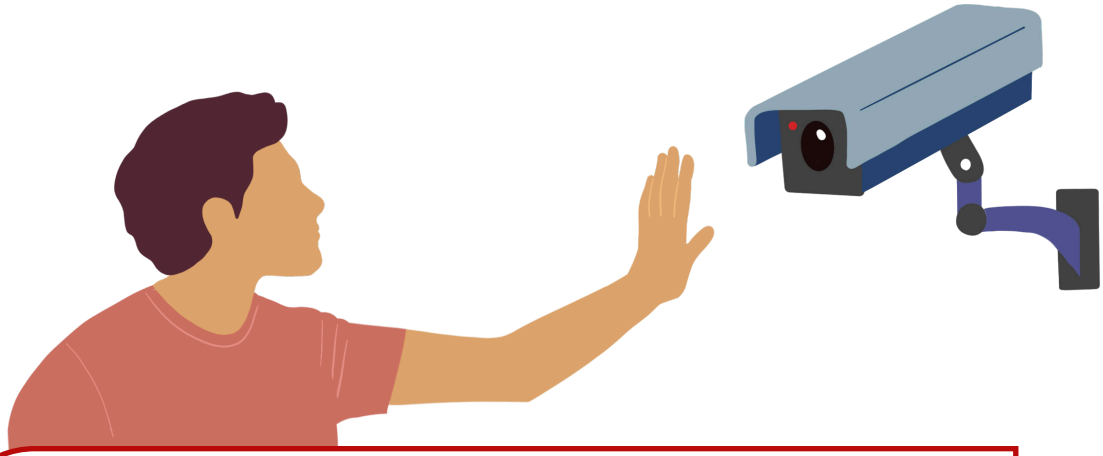
As algorithmic management runs entirely on data collected from workers, the guide focuses on how you can make use of an existing, powerful but underused tool available across the Nordics and the EU: the General Data Protection Regulation (GDPR). The GDPR regulates how workers' data is collected and processed by the employer and grants crucial legal rights for workers to defend themselves against harmful uses of worker data that algorithmic management systems are dependent on.

At this point, the whole topic can feel difficult to grasp, confusing and overly technical – you may not even know what systems are in place in your workplace; what data is collected; and whether it is harmful to you and your colleagues, and if so, what an individual union representative or worker can do about it.

This is a common feeling, but we want to reassure you: it is enough if you know the basic principles of how these systems operate and the most common ways they are used in workplaces; that you have legal rights granted by the GDPR; and that there are people who can help you and procedures you can follow when you want to engage more with these questions. All of this is presented in this guide.

In addition to doing literature reviews and desk research, we are grateful to the shop stewards in Finland and Sweden who volunteered to be interviewed to share their experiences of how algorithmic management is used in workplaces and what kind of support shop stewards would need to better negotiate it. The final guide was reviewed by the target users, shop stewards, to ensure it addresses real needs in the best possible way. We also want to thank data protection expert Anne-Christine Lacoste for her valuable remarks.

The guide was built by the independent think tank *Demos Helsinki*, commissioned by the *Foundation for Progressive Studies (FEPS)* as part of the *FEPS-Nordic Digital Programme*, a consortium of *Nordic trade unions* and think tanks including the *Kalevi Sorsa Foundation*, the *Swedish Union for Professionals (Akademikerförbundet SSR)*, the *Friedrich-Ebert-Stiftung (FES) Nordic Countries*, the *Economic Council of the Labour Movement (ECLM)*, the *Swedish Trade Union Confederation (LO Sweden)*, the *Swedish Commercial Employees' Union (Handels)*, *Delta Norway*, the *Central Organisation of Finnish Trade Unions (SAK)*, *Industrial Employees TP*, the *Danish Union of Metalworkers (Dansk Metal)*, *the Union of Commercial and Clerical Employees in Denmark (HK Denmark)*, and the *Danish Trade Union Confederation (Fagbevægelsens Hovedorganisation - FH)*. We want to thank the consortium and FEPS for their support and valuable comments throughout the process.



This guide is for you if...

Certain management actions represent major violations of rights, privacy or health, and you should draw firm boundaries against these kinds of practices. You will find practical guidance for how to do this in Chapter 1.

- **Stop automated dismissals:** human managers must always take final responsibility for disciplinary action, redundancy calculations or terminations.
- **Ban biometric surveillance:** reject tools that scan faces, analyse emotions or evaluate vocal stress. These are generally illegal, except where used for narrow medical or safety reasons.
- **Stop secret data repurposing:** data gathered for one explicit reason must never be secretly used against workers for another.
- **Protect union rights and private spaces:** enforce a strict ban on surveillance in rest areas or changing rooms. Prevent management from monitoring or identifying union communications or organising efforts.
- **Block discriminatory profiling:** refuse systems relying on biased data sources, like direct customer ratings for evaluating performance.
- **Prevent work intensification:** stop algorithms from pushing workers to maximum physical capacity without adequate rest. Secure a firm right to disconnect outside of working hours. Argue for evaluating work performance at the group level rather than the individual level.

1 STEP-BY-STEP INSTRUCTIONS FOR USING THE RIGHTS GRANTED BY THE GDPR IN EVERYDAY SITUATIONS

This chapter presents different problematic situations related to algorithmic management you may encounter in your workplace. It gives you guidance on how to proceed in each situation, lists good questions to ask your employer and tells you which GDPR articles you can reference to support your requests. The GDPR articles listed here point you to the right parts of the legislation. However, they can contain exceptions and nuances that cannot be explained here in detail, so always review the legislation itself before utilising the GDPR to back your claims. You can find access to the GDPR in the Further Reading section of this chapter.



Before taking action, always consult with your shop steward and union advisor on the best way to proceed.

I don't know what data my employer collects

Start here if you're not sure what digital tools are in use, what they track or where the data goes.

GDPR articles you can refer to: Articles 13-15, 24, 30 and 35.

What you will want to do:

- ☐ Ask the DPO if you can consult the RPA. This register should list the processing activities of the company and details of their legal basis, the duration of processing, the recipients of the data and so forth. The register should mention the existence of algorithmic management tools. The GDPR does not foresee an absolute right that would allow shop stewards to consult this register, but access may be granted on a case by case basis.
- ☐ Identify and document the digital tools used (e.g., automated recruitment systems, shift-planning applications, physical sensors and productivity trackers operating on the shop floor).
- ☐ Find out which external companies developed or currently supply these technological tools.
- ☐ Investigate how the employer collects, stores, analyses and eventually deletes or removes the information.
- ☐ Ask management to explain the conclusions they draw from this information and demand to know if they sell any data to external companies.

In almost all situations, employers are required to provide this information under the GDPR.

How to get started

Map your working day: Do this little exercise proposed by The Why Not Lab in their Workers' Data Rights Tool to get started.

To be totally sure you have a complete picture of this [how the employer processes your data and for what purposes], a good step is to map the digital tools you encounter during your workday from the moment you enter your workplace. Do you enter and exit work using an electronic key card (that's data!)? Do you use a computer (that's data!)? Do you have to input information onto a wearable device (that's data!)? Are there security cameras (that's data!)? Try to map you workday from the moment you enter or start work to the moment you leave or stop work. Remember to think about any devices or systems that you might take home with you that are owned by your workplace. Write down all of the digital systems you encounter and try to list what data they are collecting from you or the device you have to use.

Scrutinise the privacy policies: if management requires that workers use specific applications, shop stewards should look for or demand the privacy policies for those tools and read them carefully. These documents often reveal the exact data sources and categories of information extracted.

Ask for the DPIAs: the employer's DPIA must legally describe what data is being processed and for what purpose (read more about DPIAs in Chapter 3).

Ask the wider membership: survey members to collect observations from across the organisation. Workers in different departments may encounter different software.

Do a little research: search the internet for the names of the digital tools used in your workplace to see if experts or other trade unionists have already analysed these systems and published critical information about how they operate.

Submit formal data requests: if management is uncooperative, you can organise a group of colleagues to submit data subject access requests under GDPR Article 15. You will find instructions for how to do this below.

Good questions to ask the employer:

- ☐ Can I see the RPA?
- ☐ Can I see the organisation's DPIAs carried out for high-risk processing activities?
- ☐ Could you list every digital application currently affecting employee working conditions and explain the operational goal for each tool?
- ☐ Which external companies or internal teams built these applications, and who holds the ownership of the software?
- ☐ What specific categories of personal information go into these applications, and where does that data come from?
- ☐ Does the organisation transfer or sell any data containing worker performance metrics to external third parties?
- ☐ What algorithmic predictions or profiles does management generate about employees using this collected information?

A new tool is being introduced, and I want a say

Start here if management is about to deploy, or has just deployed, a new algorithmic system and you want to negotiate before it is rolled out.

GDPR articles you can refer to: Articles 5, 12-15 and 22.

General principles of good data governance to demand:

1) Demand transparency: employers must consult you *before* deploying algorithmic systems. Require the employer to explain what data is being collected and the logic with which the software makes decisions.

2) Enforce data minimisation: insist that management only gathers information that is necessary for specific tasks. Ask the employer to restrict access to the system to relevant personnel and delete the data after use.

3) Keep humans in command: ensure software only advises managers and does not make final decisions. Secure the right for workers to challenge machine-generated evaluations and request a review from a human supervisor. "because the algorithm said so" is not an acceptable excuse.

4) Secure participation: negotiate, for example, for a joint technology committee where union representatives can oversee system audits and data governance practices.

5) Protect against bias: require that management collaborates with the union to select external experts to conduct frequent reviews of automated systems to uncover possible discriminatory processing of data.

6) Protect sensitive data: restrict the use of identifiable and biometric information like facial recognition or collecting voiceprints to analyse workers' moods. Processing biometric data to identify a person is, in general, strictly prohibited, apart from a few, limited expectations.

7) Share the rewards: negotiate to distribute financial benefits of efficiency gains from digitalisation to workers through better pay, shorter working hours or more training opportunities.

What you will want to do:

- ☐ Identify the managers responsible for deploying the digital tools.
- ☐ Check current collective agreements and workplace policies for existing rules on data processing and monitoring.
- ☐ Establish strict red lines before entering negotiations.
- ☐ Contact your trade union for support and involve your organisation's health and safety representative(s).
- ☐ Ask union members about their concerns regarding algorithmic management.
- ☐ Think of how to demand a fair share of the financial rewards generated by the technology, such as through shorter working hours or higher pay. Talk about these with your union.

Good questions to ask employers:

- ☐ Which manager holds responsibility for this system, and can they explain it in plain language?
- ☐ What is the exact procedure for an employee to challenge an automated decision that negatively affects their work?
- ☐ How has management communicated this right of appeal to all staff members?

How to scrutinise and participate in a DPIA

Management is required to complete a formal DPIA before launching any digital tools that pose high risks to workers (in practice, this covers all algorithmic management systems). If one is done, you should intervene during this evaluation to establish clear boundaries and to verify that the employer has reduced all relevant risks.

GDPR articles you can refer to: Articles 35 and 15.

What you will want to do:

- ☐ Notify management of their legal duty to consult worker representatives throughout the evaluation process.
- ☐ Ask for a complete written copy of the evaluation to verify the operational and legal justifications for data collection, assess the necessity of the system and check whether identified risks are actively reduced.
- ☐ Require management to provide a written explanation dating back to the original procurement decision if they claim an assessment is unnecessary.
- ☐ Establish a schedule for reviewing the evaluation regularly, especially when the digital system receives software updates or new functions.

Good questions to ask the employer:

- ☐ Did management complete a formal DPIA before purchasing or deploying this system? Either at the workplace or company level? If not, why not?
- ☐ Can the union have full and unrestricted access to review the results of this assessment?
- ☐ What mechanisms will management use to guarantee that workers are involved in governing this technology on an ongoing basis?



Rasmus, Cashier at a supermarket

Intervening before a new system is installed to ensure its legitimate use

The scenario: Rasmus is a shop steward at a supermarket. The employer is about to install a point-of-sale transaction monitoring system – to monitor the flow and efficiency of queues – to optimise the number of staff during different opening hours. As each cashier is logged into the system with their personal key card, Rasmus realises that combining these two data sources can lead to the employer using the new system to monitor the pace of work of individual cashiers, with the risk of profiling some individuals as being less efficient than others and reducing their shifts.

The action: as a shop steward, Rasmus uses his right to be consulted before changes in the workplace that affect workers. Rasmus organises a meeting with the manager responsible for the software. Given that the new system enables continuous monitoring of workers, he asks to see the results of the DPIA done for the system. He reminds the employer of GDPR Article 5 (the principle of purpose limitation), according to which data collected for one purpose cannot be used for another purpose. He also points out that employees should never be subject to decisions only made by a machine (GDPR Article 22).

The result: following Rasmus' request, the employer agrees to put the new system on hold until the issue has been properly negotiated. Ultimately, the employer agrees to write the outcome into a local collective agreement, which ensures the negotiation result is lasting and not dependent on the current manager.

Elena, Finance Sector Rep

Taking control of "sentiment" surveillance

The scenario: Elena represents workers in the finance sector. Management rolls out a digital application that prompts workers to log their mood every Friday. Workers feel pressured to constantly give positive responses out of fear of being flagged by HR as a problem.

The action: Elena uses the union's consultation rights on workplace health and safety to challenge the new tool. She argues the software constitutes a psychosocial hazard and invasive surveillance of workers' emotional states.

The result: Elena and the union negotiate to co-design the application questions, removing individually identifiable mood tracking and ensuring the tool focuses on systemic issues. Management anonymises the data and shares it with the union to help negotiate better workplace resources.





A worker has been penalised, warned or dismissed by an algorithm

Start here if a specific worker has already been affected by an automated decision, and you need to intervene now.

GDPR articles you can refer to: Articles 13-16 and 22.

What you will want to do:

- ☐ Ask the employer to explain the exact logic and parameters the software used to evaluate the worker.
- ☐ Check if a worker is subject to a solely automated decision, such as a computer-generated warning.
- ☐ Submit a formal request for human review.

Good question to ask employers:

- ☐ Is the worker subject to a solely automated decision, or did a human manager actively review and authorise this outcome?

If the decision stands or the process feels unfair

Move to Section 5 of this chapter to request the worker's full data file. Section 6 gives you instructions on how to escalate the issue to your organisation's DPO or your national DPA, if necessary.

Henrik, Transport Sector Union Rep
Challenging invasive biometric surveillance

The scenario: Henrik represents transport workers facing a new artificial intelligence (AI) camera system inside their truck cabins. The software scans drivers' faces to detect fatigue, which led to a driver receiving an automatic disciplinary warning for squinting into a bright sunrise. This surveillance left drivers feeling stressed and vulnerable.

The action: Henrik invoked the workers' right to object (Article 21) to this processing under the GDPR. He argued the system breached the purpose limitation principle, as it was designed for safety reasons and further used for disciplinary purposes, pointed out that it relied on invasive and flawed biometric profiling, and he demanded to see the DPIA. He pointed out that processing sensitive biometric information carries severe risks and requires worker consultation before deployment. He also pointed out that, under the EU AI Act, in-cabin driver-monitoring systems are likely classified as high risk and require formal risk management, logging and meaningful human oversight. Besides, under the new EU vehicle general safety regulation, systems identifying drivers are forbidden, and data must remain in a closed loop and be immediately deleted.

The result: management admitted they bypassed the risk assessment and omitted several data protection rules. They paused the system. Henrik negotiated a new boundary where cameras do not include any biometric features and data is only used for safety reasons and then deleted.

I suspect the system is biased

Start here if you're seeing a pattern, not just one bad decision and certain groups, shifts or departments seem to be consistently disadvantaged.

GDPR articles you can refer to: Articles 13-15, 22 and 35.

What you will want to do:

- ☐ Demand the employer discloses the training data used to build the system to determine if it relies on biased information.
- ☐ Reject the use of customer ratings as a direct performance metric, as this introduces external prejudices into the workplace.
- ☐ Propose that the algorithms undergo regular equality assessments and audits by independent, jointly chosen third parties.

Good questions to ask the employer:

- ☐ Have the algorithms undergone equality assessments?
- ☐ Will the organisation agree to conduct these by jointly chosen, independent third parties in the future?

I want to see what data is held on a specific worker

Start here if you need the worker's full data file, whether to support an appeal, verify a claim or simply understand what's being tracked.

GDPR articles you can refer to: Articles 15, 20 and 80.

➔ **Step 1: Secure a mandate from the employee**: these are individual legal rights. You must secure a signed written mandate from the worker authorising you or another union representative to represent them.

➔ **Step 2: Find the right recipient**: under the GDPR, the entity accountable for collecting your data, such as an enterprise, is called a "controller". You should direct your request directly to the controller.

- ☐ Check your organisation's Privacy Policy to find out who is the controller and their contact details. If your organisation has a DPO, they are usually a useful contact point for the controller. The Privacy Policy can often be found, for example, on the company's website or intranet.

➔ **Step 3: Determine the legal requests you want to refer to**:

- ☐ An Article 15 request is the main access tool. It aims to give you an overview of all your personal data. The employer must share all personal data they hold and explain the reasoning behind automated decisions.
- ☐ In addition, an Article 20 portability request is also useful if you specifically need the data delivered in a structured, machine-readable format.

➔ **Step 4: Write the request: you must clearly ask for the data processing details from the employer and attach the worker's permission.**

- ☐ State whether you want to review all your information or information from a specific time period, in what format you would like the information (e.g., in machine-readable format versus a PDF), your name and your contact information.
- ☐ In the request, ask the employer to confirm what categories of data they collect, who receives this information and the exact logic behind any automated evaluations.

In **Annex 1**, you can find an example template for writing your request.

➔ **Step 5: Submit, track and escalate**. You can escalate the issue if the employer ignores you or doesn't adhere to legal deadlines.

- The employer has a one-month deadline to deliver the response, although they can extend the deadline by two months if they need the time.
- Send a polite written reminder if management misses the deadline without a formal extension.
- File a free-of-charge complaint with your national DPA if the employer doesn't respond (see Section 6 of this chapter). If the employer refuses to provide your information, it must tell you the reasons for the refusal, which must always be based on law.

Management is ignoring us, or a red line has been crossed

Start here if a red line has been crossed or management ignores formal data requests, refuses to consult workers on new tools or deploys invasive surveillance. Contact the company's DPO first to seek an internal resolution. If the employer remains unresponsive, you can escalate the case to your national DPA.

GDPR articles you can refer to: Articles 38, 39, 77 and 80.

➔ **Step 1: Engage the DPO.** Organisations processing vast amounts of personal information must appoint an internal officer to monitor compliance. This official serves as your primary contact point to challenge questionable data practices internally.

- Find the contact details for the DPO within the company's Privacy Policy (which can be found on the company's website or intranet).
- Ask the DPO if they have reviewed the legality of newly proposed tracking systems or ask for the state of play of any ignored data access requests.
- Request a formal explanation detailing exactly how management plans to guarantee workers' data rights under new policies.
- If the employer claims no DPO is required, demand a written legal justification.

➔ **Step 2: Escalate to the DPA.** If internal discussions break down, you can take the dispute to the national authority.

- See the Info Box below to find your national authority's contact details and instructions for seeking their support.
- Note that the DPAs advise, or, in the case of Finland, request, you to contact the controller directly first before it will take a position on your case.
- Ask your union to officially represent the worker and make the complaint on their behalf. Note that you need a signed mandate for this. You can also make the complaint with the worker yourself.
- The authority should inform you about the process of the complaint within three months.
- Note that the DPA's decision can be subject to a judicial remedy if you consider it to be unsatisfactory. You also have the right to a judicial remedy, subject to national representation rules, independently of the DPA remedy.

Aisha, Call Centre Steward
Escalating to the DPA

The scenario: Aisha represents call centre workers. She suspects management uses new email-scanning software to track union members and identify organising efforts.

The action: Aisha coordinates several workers to submit formal GDPR data access requests. They demand to see what personal information the software flagged about them. They write a request consisting of all necessary information and requirements, pointing out the possible breach of the principle of secrecy of communications (ePrivacy directive) and the excessive impact on workers fundamental rights and freedoms (GDPR Article 6), and send the request to the organisation's DPO. When management ultimately refuses to provide the data, Aisha goes to the website of her national DPA to file a formal complaint. She has asked for additional support from her union's lawyers.

The result: the authority launches an investigation into the company's tracking practices, even though it has taken a year for the complaint to be taken up for processing. Finally, the system is ruled illegal. The employer faces substantial administrative fines and disables the software's keyword-tracking feature. They sign a collective agreement explicitly banning the surveillance of union communications.



Where you can lodge a complaint with your national DPA:

Datatilsynet in Denmark

Tietosuojavaltuutettu in Finland

Datatilsynet in Norway

Integritetsskyddsmyndigheten (IMY) in Sweden

Do you want to learn more about data protection and build networks with others in the field? These NGOs are a good place to start:

Danmarks DPO Forening (The Danish DPO Association): membership is open to individuals and companies working in the field.

Tietosuoja ry (Finnish Data Protection Association): membership is open to anyone interested in data protection or working with these issues.

Foreningen Personvernombudene (Norwegian Association of DPOs): membership is open to anyone who is registered as a DPO or has privacy advice as one of their primary tasks.

Forum for Dataskydd (The Forum for Data Protection): aimed at DPOs and anyone working with data protection issues at work.

Further reading

If you want to read more about how you can leverage existing tools and negotiate new ones to steer and challenge the use of algorithmic management in the workplace, these sources provide a solid foundation.

"General Data Protection Regulation (GDPR)". Intersoft Consulting. (n.d.). General Data Protection Regulation (GDPR). Retrieved 26 July 2026, from https://gdpr-info.eu/.

A user-friendly website to scroll through the GDPR and find desired articles quickly.

"Digital technology: Guide for union representatives". Prospect.

This guide offers practical tools for union representatives. It includes clear action checklists for scrutinising data protection assessments and negotiating technology agreements.

"Co-governance guide: A checklist to responsible use of algorithmic systems". Public Services International (PSI).

This resource features a 27-question checklist. You can ask these questions directly in meetings to require management to explain exactly how their digital tools operate.

"People-powered technology: Collective agreements and digital management systems". Trades Union Congress.

This manual details how to draw firm red lines, secure financial rewards, and establish technology committees through collective bargaining. It provides structural advice for setting up joint oversight.

2 UNDERSTANDING ALGORITHMIC MANAGEMENT AT WORK AND ITS FOUNDATIONS IN DATA

What is algorithmic management?

Algorithmic management refers to the use of algorithms, AI and digital technologies to perform managerial functions traditionally carried out by human managers and supervisors. In the context of a workplace, these computer-coded processes are used to direct, coordinate and control workers based on data collected from them. In practice, **employees rarely know why and how the algorithm made a decision. In addition, workers are rarely able to negotiate or contest these decisions with the employer.** This decreases workers' autonomy and puts workers in a significantly weaker position in relation to the employer.

How algorithmic management systems work in practice

1) Collect data
The system gathers information about workers and their tasks, such as location (GPS), time spent on a task or number of customers served.

2) Process the data
Software (an algorithm) analyses this data automatically, often in real time. It looks for patterns, such as who's fast and who's slow, or who's idle.

3) Make decisions
Based on that analysis, the system makes management decisions without a human manager directly deciding each time. This can be, for example, assigning the next task to the nearest or fastest available worker or proposing a route.

4) Give instructions
The system sends instructions back to the worker, such as "Go here next", "You have eight minutes left", "Your rating dropped", usually through an app.

5) Repeat and adjust
Every action the worker takes generates more data, which feeds back into the system, refining future assessments and decisions.



How is algorithmic management used in the workplace and what threats and opportunities does it pose for workers?

Algorithmic management has become very common in all workplaces across sectors. In a recent study, 75% of 6,000 employees surveyed in Finland, Denmark, Norway and Sweden reported that at least one algorithmic management tool is used in their workplace, especially in warehousing, customer service and retail (Finnish Institute of Occupational Health, 2025).

This includes, for example:

Workplace decision algorithms

These systems advise or replace human managers in day-to-day operational planning. Examples include predictive shift scheduling based on, for example, consumer footfall; the allocation of everyday tasks (such as routing drivers or directing warehouse picking); managing routine HR requests (like approving sick leave); and even algorithmically redesigning team structures based on skill assessments.

RISKS

Algorithmic management poses serious risks to worker health and wellbeing. By optimising day-to-day processes relentlessly for efficiency, algorithms eliminate the natural pauses workers need, leading to physical exhaustion, repetitive strain injuries and psychological stress, sometimes even requiring workers to formally request permission for toilet or meal breaks. When work is increasingly fragmented into machine-directed micro-tasks, it strips workers of autonomy and professional judgment. Algorithms also frequently lack real-world contextual awareness, such as road closures or bad weather conditions, leaving workers caught between following incorrect instructions and risking punishment for using their own judgment. Unlike human managers, algorithms are not capable of empathy or flexibility, and they do not take into account personal emergencies or other difficult circumstances.

OPPORTUNITIES

When workers and unions are involved in the design and deployment of these tools, they have the potential to improve working conditions. They can be used to generate initial shift suggestions that workers then collaboratively refine. If the software enables workers to swap shifts or request leave directly, it can reduce the dependence on managers and favouritism that can come with it. In warehouses and retail, algorithms can relieve workers of mentally taxing tracking tasks and suggest picking routes to reduce physical strain.

Performance management algorithms

This category includes tools used for the surveillance, monitoring and evaluation of workers. These algorithms can track physical location; monitor digital activity (such as keystrokes or active software); analyse the sentiment of employee emails; measure output against performance targets; and compile customer ratings to recommend, for example, disciplinary actions or bonuses.

RISKS

Algorithmic management raises serious concerns about privacy, fairness and worker dignity. Constant surveillance of location, keystrokes and even tone of voice creates an oppressive working environment, particularly for remote workers monitored in their own homes. In the most serious cases, AI tools have been used by employers to scan internal communications for union-related language and monitor organising activity, actively suppressing workers' rights to collective action. Systems that

continuously rank workers against each other generate chronic stress and job insecurity and harm workplace solidarity. Evaluation systems often prioritise easily measurable outputs like speed while ignoring tasks that are essential but less easily quantifiable. If customer ratings are incorporated into the automatic evaluation, it can enter racial and gender bias into performance assessments. The opacity of these systems makes it nearly impossible for workers to understand or challenge the automated decisions.



OPPORTUNITIES

If data-driven management tools are used carefully, they can have some benefits for the worker. Impartial performance data could help human managers give fairer, less biased feedback. The system can identify workers who are struggling and proactively offer them tailored arrangements. If monitoring is linked to a performance reward scheme, it can help employees to increase their pay. Monitoring technology can also serve a protective function, helping to shield frontline workers from customer aggression and other safety threats. However, these benefits are heavily dependent on how monitoring is designed and communicated. Workers should have a say in how these tools are being deployed, how employees are being monitored and for what purposes. The intensive and opaque monitoring deployed in workplaces quickly causes stress and exhaustion in workers.

Recruitment algorithms

These tools are used to automate hiring processes. This category includes algorithms that scan CVs to filter candidates, chatbots that guide applicants, tools for testing competencies, automated video interviews that analyse facial expressions or voices, and software that conducts background checks on candidates' social media histories.



RISKS

Algorithmic hiring tools carry significant risks of bias and discrimination. They are trained on historical data, reflecting past human prejudices, and can thus replicate and amplify those biases at scale. Amazon, for instance, stopped using an AI recruitment tool after it systematically downgraded women's applications. Automated systems that analyse facial expressions or vocal tones to assess traits like trustworthiness are widely criticised as pseudoscience. Automated social media background checks can penalise candidates for issues that are not related to their job performance, or lead to discrimination if the employer screens for and makes decisions to reject candidates based on information related to, for example, health or sexual orientation.



OPPORTUNITIES

If the systems are trained with properly audited and tested, unbiased data, algorithmic hiring tools have the potential to reduce discrimination by bypassing human unconscious bias and giving candidates from disadvantaged backgrounds a fairer chance. Text analysis software could scan job postings to remove "coded language" that might put applicants at a disadvantage based on gender or age.

Further reading

If you want to understand algorithmic management and its impacts better, here are a few good sources:

Briône, P. (2020) "Algorithmic management: A trade union guide". UNI Global Union Professionals & Managers.

The publication delves deeper into how algorithmic management is used in the workplace and the challenges and opportunities it creates.

Cox, T. and Oosterwijk (2024) "Algorithmic management in the workplace: Case studies on the impact of algorithmic technologies in seven sectors in the Nordics". Policy study. Foundation for European Progressive Studies, October.

The policy study presents the findings of case studies from across the Nordic countries on the impact of algorithmic management on worker rights and wellbeing, and on the balance of power between labour and capital.

Mikkonen, J., A. Pura, E. Välimäki, and R. Kull (2026). "AI, automation, and public authority - Beyond the hype of algorithmic decision-making in the Nordic Welfare State". Policy Study. Foundation for European Progressive Studies.

The policy study sheds light on the impact of algorithmic management and automated decision-making in the public sector with case studies from Finland, Norway and Sweden. It identifies organisational capability, professional discretion and judgment, legal interpretation, procurement, accountability, and public trust as the main challenges.

3 YOUR BEST TOOL TO CHALLENGE ALGORITHMIC MANAGEMENT AT WORK: THE GDPR

As described in the previous chapter, algorithmic management is a computer-coded process that relies on vast amounts of data to function. Hence, **having a full picture of employees' data that is collected and processed is the most effective way for workers and union representatives to intervene and shape the systems to benefit workers**. Leveraging the GDPR is a powerful tool for you to do this.

While this guide focuses on leveraging the GDPR, it is good to remember that other national and EU-level legislation, regulations and rights can also be used to challenge algorithmic management. Some of these are briefly presented later in this chapter.

There are many stages at which union representatives and workers can influence the design of algorithmic management tools. In worst-case scenarios, employers make significant decisions without even informing workers about what information the system uses. In slightly better cases, management at least informs employees about data collection. However, simply receiving information isn't enough: **as a shop steward, you should demand that workers are actively involved in how these digital systems are designed, deployed, and governed**. Figure 1, from the Ada Lovelace Institute's Participatory Data Stewardship Model, illustrates how people should be involved in the use, collection and management of data to preserve their rights.

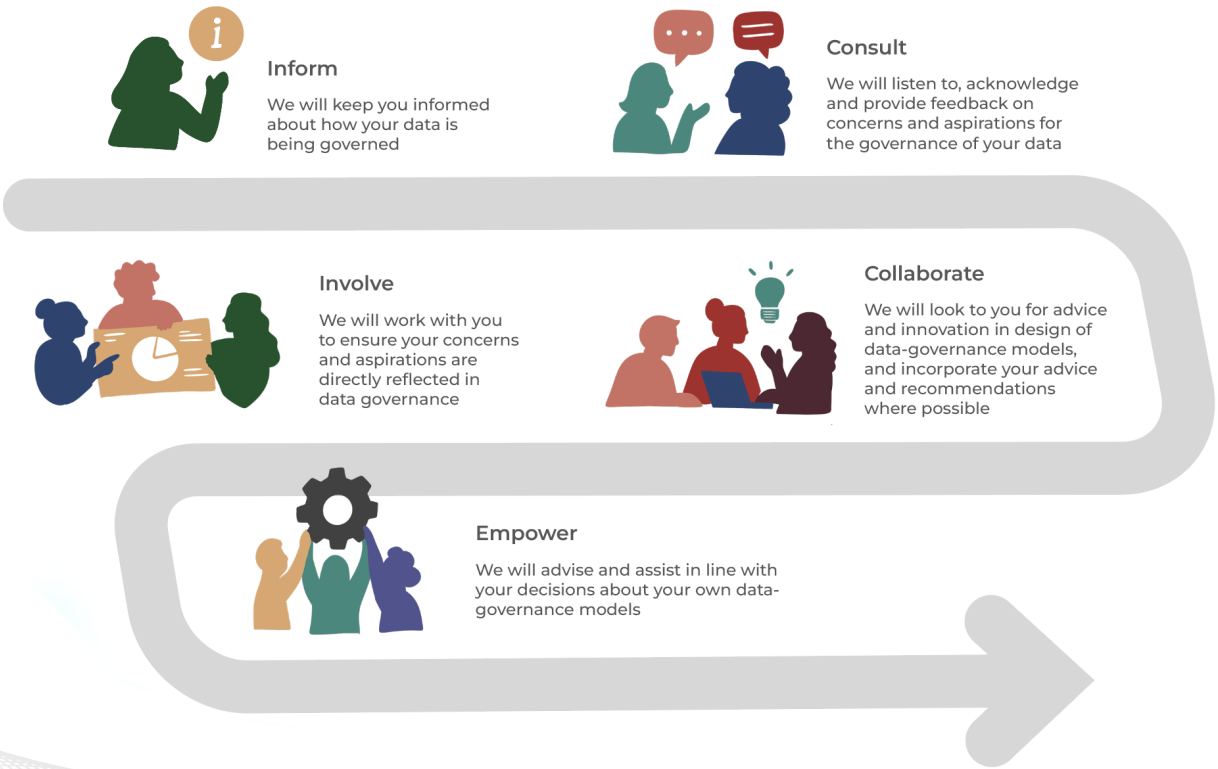


Figure 1. Ada Lovelace Institute's framework for participation in data stewardship.

To have more influence over data and algorithmic management, you must be informed about your legal rights. Personal data rights give you the legal hooks you need to challenge unfair automated decisions. While other legislation, such as general consultation and health and safety rules, remains important, **algorithmic systems depend entirely on information generated by workers**. **Using data rights as a legal lever gives you a cross-cutting tool to exert control over these technologies across any sector.**

The rest of this chapter explains what these legislative tools are and how you can use them to protect workers. The most important of them is the GDPR, which came into force in the EU in 2018. In Annex 2, you can find an overview of other legislative tools to steer the use of digital systems at work.

What are personal data rights?

Personal data rights are the concrete legal protections that give workers, and everyone else, control over how their personal information is collected and processed. In the EU, personal data is first and foremost protected by the GDPR.

What is the GDPR?

The GDPR is a comprehensive EU law that applies directly across all member states. It regulates the processing of "personal data", which means any information that identifies, or could be used to identify, a person. In the workplace context, this includes everything from names and contact details to performance metrics, location tracking and video surveillance. **Generally, you can begin with the assumption that all data collected from workers is covered by the GDPR. The GDPR foresees enhanced protection when processing is intrusive or relates to sensitive data.**

Because most algorithmic management tools rely entirely on personal data, the GDPR serves as the strongest legal tool you have to negotiate on algorithmic management.

Also keep in mind: privacy and data protection are fundamental human rights under EU law, not just ordinary rules. That gives them more weight than many other interests, like a company's business needs. Because of this, you can do more than just ask "did they technically follow the rules?" You can also ask whether the system should be considered legitimate at all, and how it affects workers' basic rights.

Next, we will cover the key rights provided under this regulation. Later in this chapter, we will present concrete instructions for using these rights.



You can access the full legal text of the GDPR through the official European Union source here. In the menu at the top of the page, you can choose to see it in Danish, Swedish or Finnish. For Norwegian data protection law, which incorporates the GDPR, click here.

KEY RIGHTS COVERED BY THE GDPR

1 Making the employer assess risks before the deployment of digital tools (impact assessments and data protection by design: Articles 35 and 25)

The law: employers must design systems to **collect only strictly necessary data** and conduct a formal **DPIA** before deploying high-risk technologies. Algorithmic management tools can be considered "high risk" because they usually meet a number of criteria listed in the GDPR: they generally involve new technological solutions, automated decision-making, monitoring, a combination of data sets and workers are in a dependent position in relation to employers. The aim of the DPIA is to identify, evaluate and mitigate possible risks posed by the new technology. During this evaluation process, the law requires that the employer seeks the views of affected workers or their trade union representatives, where appropriate, to identify and address potential harms.

The **privacy-by-design** principle reinforces this obligation. Before introducing new workplace monitoring or management technology, employers should build technical and organisational safeguards from the start. The measures must reflect the risks involved and may include processing less data, using pseudonymisation and limiting access. In short: privacy should not be an afterthought. It should be built in the design of workplace technologies from the beginning.

What this means in the workplace: for shop stewards, these rules provide a mechanism to intervene before software is deployed in the workplace. Shop stewards should always check whether a DPIA exists and ask to be consulted. You can find more information on participating in the assessment process in Chapter 1.

Together with AI regulation and labour law, these articles grant you the right to

- **Review risk assessments: demand to see the formal evaluation before any new tracking tool goes live. If a DPIA has not been conducted, ask for it.**
- **Demand written justification if no assessment is made: ask management to provide a formal written explanation if they plan to deploy a monitoring system without conducting a proper risk assessment first.**

2 Knowing what data your employer collects (transparency and information rights: Articles 12-14)

The law: the GDPR requires employers to be transparent about how they process your personal information. Under Articles 13 and 14, management must explain exactly **what data they collect, why they collect it, who receives it and how long they keep it**. This has to be done at the time the data is being collected. Article 12 states that the employer must actively assist workers in exercising their rights provided by the GDPR. **What this means in the workplace:** this provision allows shop stewards

to understand the basics of the technologies used at work. You should use this right to map all the systems your employer uses for algorithmic management. **Your employer cannot implement secret monitoring or evaluation metrics that impact working conditions.**

With these articles you can

- **Request to know what data is being collected and why, and what consequences the automated decisions might have if an employer uses a monitoring system or automated decision-making.**
- **Expect to be able to exercise your rights: your employer also cannot hide your rights in the small print or make it inappropriately complicated and exhausting to make requests.**

3 Reviewing workers' data files (right of access: Article 15)

The law: each worker has the right to know if their employer is processing their data and to receive a free copy of that information. This right also guarantees access to details about who receives the data and the logic behind any automated decisions that affect the worker.

What this means in the workplace: with this right, you can get comprehensive information on the algorithmic management tools used in your workplace and question their relevance and proportionality.

This article can be useful to

- **Support workers in disputes: you can help employees submit access requests to see what data the employer holds about them during performance reviews. You can find guidance on submitting these access requests in Chapter 1.**
- **Expose illegal profiling: you can coordinate access requests to find unlawful practices, such as secretly recording trade union membership or using hidden evaluation criteria.**

4 Correcting and deleting data (right to rectification and erasure: Articles 16 and 17)

The law: workers have the right to correct inaccurate personal information and request the deletion of data that is no longer necessary or was unlawfully collected. Employers must correct these errors or erase the unjustified files without undue delay.

What this means in the workplace: for shop stewards, these rights provide a mechanism to ensure algorithmic systems do not evaluate workers based on flawed or outdated records. Under this article, you can

- **Fix incorrect inputs: you can demand the correction of, for example, erroneous clock-in times or inaccurate performance figures before an automated system acts on them.**
- **Delete old records: you can demand that employers erase expired files, so they cannot dictate future employment decisions.**

5 Challenging machine-made decisions (right to object and human review: Articles 21 and 22)

The law: workers have the right to object to intrusive data collection, and the right not to have decisions made about them by a machine alone. If a computer program makes a significant choice about a worker, the worker has the right to demand human intervention, express their point of view and contest the machine-generated outcome.

What this means in the workplace: for shop stewards, these provisions establish a principle: **algorithms can advise, but human managers must decide**. Based on this right, you can, for example:

- **Contest invasive surveillance: use the right to object to demand the removal of continuous GPS tracking or biometric monitoring if the employer's business interest does not outweigh the worker's right to privacy.**

- **Stop automated dismissals: force management to guarantee a meaningful human review before any automated system makes a disciplinary warning, evaluates the employee's performance or proposes terminating their employment.**

6 Enforcing rights and escalating disputes (complaints and representation: Articles 77-80)

The law: employers must respect data rights. If they fail to comply, every worker has the right to lodge a formal complaint with their national DPA (read more on DPAs below). The authority must respond and inform the worker of the progress or outcome of the complaint within three months. Workers also have the right to take the employer or the authority to court. The law allows workers to mandate a trade union to lodge these complaints and exercise these legal remedies on their behalf. Some EU countries have also given unions the option to lodge complaints independently, without the mandate of a specific person. This can be the case, for instance, in Denmark, Norway and – to some extent – Sweden, under specific conditions, depending on labour law and collective agreements, in combination with data protection rules.

What this means in the workplace: for shop stewards, these rules provide an escalation path when management refuses to answer data requests or correct inaccurate information. Workers, or you as a shop steward, do not have to fight these battles alone. Under this article, you (as a union representative) can

- **Represent workers in formal disputes if you secure their written permission. You can find more information on escalating issues to national authorities in Chapter 1.**
- **Depending on specific conditions of national law, lodge complaints against the employer if you suspect data rights violations, even without a request from a specific employee.**

Data protection and privacy are fundamental rights

Under the Charter of Fundamental Rights of the European Union, privacy (respect for private and family life) and the protection of personal data are enshrined as fundamental rights. This means that these rights enjoy a higher status in the hierarchy of competing interests. Consequently, you can question the compliance of algorithmic management not just with the letter of the law, but its very legitimacy and its impact on workers' fundamental rights. Please note however that the Charter does not apply in Norway.

DPOs and DPAs at your service

There are colleagues and authorities to whom you can turn for support in securing your data rights.

The DPO is an official working inside your company to make sure management follows data rules. The DPO has a specific legal mandate to inform and advise the employer and workers about their data protection rights and obligations: their core tasks include monitoring the company's compliance with the law, raising awareness, training staff, and giving advice on and monitoring the fulfilment of DPIAs (DPIAs are discussed earlier in this chapter). They are also the formal contact point for the national DPA. The law (GDPR Article 37) requires that companies appoint this person, for instance, if they regularly and systematically monitor workers on a large scale as part of their core activities. Subject to the volume of data processed, the duration of monitoring and the necessity of monitoring for the activities of the company, algorithmic management will often require the designation of a DPO. They must work independently, so management cannot give them instructions on how to do their tasks,

and they also cannot be fired for doing their job. They must be provided with sufficient resources (like time and training) to perform their role. While their role does not extend to representing workers in dealings with their employer, you should consider the DPO an ally to shop stewards and build a strong relationship with them to check the legality of new tracking systems and review risk assessments.



If your employer claims they do not need a DPO, ask them to justify this decision in writing. In the absence of a DPO, you should direct your data requests and questions to the company's HR contact address and/or use your standard worker representation bodies to demand answers. If management still refuses to cooperate, you retain the right to escalate the issue directly to the national DPA. See Chapter 1 to find more information on how to do this in practice.

The DPA is an independent public body in your country, required by the GDPR (Articles 51-59), that enforces data protection law (see the list of and contact details for Nordic DPAs in Chapter 3). Think of them as the external police for data protection. If management ignores your requests or your internal talks fail, you can lodge a formal complaint with the DPA for free. They have the power to investigate the workplace, ban illegal tracking and issue fines to employers who break the rules. Go to Chapter 3 to read more on when and how to contact your national DPA.

EU law is changing: What to look for and how to keep up

Three important EU laws will come into force or be adopted in the autumn 2026 that may have an impact on the regulation of algorithmic management.

The Digital Omnibus is still a proposal at the negotiations stage, but it foresees some changes to the GDPR that may be relevant here:

- **A possible narrowing of the definition of personal data. This could place some pseudonymised workforce data outside of the scope of the GDPR.**
- **A limitation of the right of access when the request is considered abusive or when trade secrets or important economic harm is involved. This could make it harder for shop stewards to scrutinise the logic, input or operation of proprietary management systems.**
- **More harmonised requirements for DPIAs across the EU. This could make the assessment of high-risk algorithmic management more systematic for the benefit of workers.**

How to keep up: see here for details of the legislative process.

The AI Act has already entered into force but some provisions on high-risk AI systems will be applicable as of December 2027. Article 9 and Annex III of the Act will oblige employers to put in place a risk management system when they use AI for certain tasks in employment and worker management, for instance, targeted job advertising, analysis and filtering of applications, evaluation of candidates, and other employment/worker management use cases. In specific cases where the risks are particularly high, an assessment of the **impact on fundamental rights** shall also be performed, in conjunction with the DPIA.

How to keep up: see here for details on the content of the Act and here for the enforcement timeline.

Rules on platform work will enter into force on 2 December 2026. They aim to regulate the use of algorithms for HR management on digital labour platforms. Under these rules, employers will have to inform workers about algorithmic management, and these systems will need to be monitored by qualified staff, who enjoy special protection from adverse treatment. Human oversight will also be guaranteed for significant decisions, such as the suspension of accounts.

Where to find more information: see here for a briefing from the Council of the EU.

Further reading

If you want to read more about negotiating data rights and challenging automated systems, these resources provide the best practical advice.

Massé, E. and C. Tackett (2018) "A user guide to data protection in the European Union: Your rights and how to exercise them". Access Now, 2 July.

This guide explains the GDPR in simple terms. It provides clear instructions for submitting data access requests and outlines the steps to lodge a formal complaint with your national DPA.

"GDPR: How to make it work for unions". industriAll European Trade Union.

A concise but informative publication tailored for trade unionists, summarising key GDPR provisions and how they impact the workplace.

"Negotiating data rights: GDPR". The Why Not Lab.

An interactive, step-by-step online tool designed to help workers and union representatives map data collection and push for transparency.

ANNEX 1: A TEMPLATE FOR REQUESTING ACCESS TO ONE'S DATA FROM THE EMPLOYER

This is a general template for making GDPR requests, inspired by the German DPA's template. Access the original source here.

Request for information about my data pursuant to Art. 15 of the General Data Protection Regulation (GDPR)

Dear Sir or Madam,

In accordance with Art. 15 GDPR, I hereby request (free of charge) information as to whether you process personal data concerning me.

If this is the case, I request information about which personal data you process concerning me: I am particularly interested in the data you process about me in relation to [specify particular time periods or particular issues].

I request information about all data you process concerning me, including data observed, derived and inferred (e.g., name, address details, date of birth, scoring, profiling and evaluation data, non-textual data including location data, logs)

In addition, I would ask you to provide information on the following questions, for each category of data:

- **For what purpose or purposes do you process this data?**
- **Please inform me of the categories of personal data concerned.**
- **Have you disclosed this data to third parties, or do you plan to disclose it to third parties? If so, to whom and for what purpose?**
- **How long will you process my data?**
- **Where does this data originate from?**
- **Do you use my personal data for profiling or any other automated decision-making? If so, I request meaningful information about the logic involved, as well as the significance and envisaged consequences for me.**
- **Is data transferred to third countries? If so, I request information on which safeguards pursuant to Art. 46 GDPR are in place.**
- **Please provide me with a copy of my personal data.**

Optional:

Irrespective of the request for access set out above, I am exercising my right to data portability, as provided for in Article 20 of the GDPR. I therefore request that you provide me with the personal data concerning me that falls within the scope of Article 20, namely, the data that I have provided and which is processed by automated means on the basis of my consent or the performance of a contract. This request is to be understood as including, in accordance with the European interpretation of the right to data portability, data resulting from my use of your services or devices and which was recorded in the course of that use, even where such data was not actively entered or provided by me.

Please provide this information without undue delay, and at the latest within one month (Art. 12(3) GDPR).

Yours sincerely,

(Signature)

ANNEX 2: OTHER LEGISLATIVE TOOLS TO STEER AND CHALLENGE ALGORITHMIC MANAGEMENT

While the GDPR provides powerful tools, other legal tools can support shop stewards in steering and challenging digital management.

The legal tool	What is it?	How to use it?
Employment law and co-determination rights	The Nordic approach relies on the dual pillars of co-determination and comprehensive collective bargaining. Employers have a legal duty to inform, consult, and negotiate with trade unions/employees prior to deploying new technologies. In Norway and Finland, the law specifically requires employee engagement when monitoring technologies are implemented.	Rely on your existing collective bargaining structures and consultation rights to demand full software transparency. Apply specific provisions in national laws to insist on data limits.
Health and safety regulations and workplace surveillance	The European Framework Directive 89/391/EEC and national laws require employers to evaluate and reduce risks to worker wellbeing before they cause harm. Stress caused by algorithmic management can be considered such a risk.	Demand health risk assessments before management buys, develops or deploys new tracking software. Use these rules to set boundaries on surveillance, challenge unsafe work intensification, and negotiate the right to disconnect so workers are not monitored outside of working hours. If your organisation has an Occupational Health and Safety Representative, ask for their support.
Anti-discrimination legislation and algorithmic bias	Equality legislation allows you to challenge direct and indirect caused by algorithmic management. For example, a scheduling algorithm might discriminate against workers who are sick or caring for a child by penalising them for absences.	Require management to conduct Equality Impact Assessments before introducing new digital tools to avoid algorithmic bias. Monitor and document the outcomes of automated systems and gather evidence to expose bias.

The legal tool	What is it?	How to use it?
Sectoral regulations	Some industries already have specific rules about workplace technology.	Look at the strongest protections that already exist in other sectors (like the Platform Work Directive) and try to negotiate similar protections into your own workplace agreement, even if your sector isn't legally required to have them.
Standards	Employers often point to technical standards and certifications as proof that their systems follow AI laws. But having a certificate doesn't automatically mean the system is fair or safe for workers, it just means someone checked a box.	Don't just accept an employer's word (or their certificate) that a system is compliant.
Collective bargaining as a tool to set data governance standards	Collective bargaining is the best tool trade unions have for setting workplace rules and shared governance standards that stop management from rolling out digital systems on their own.	Review your current collective bargaining agreement to check for existing provisions on data use and monitoring. Discuss with your union on new clauses.
The European AI Act	The European AI Act classifies many AI systems used for worker management as high risk. This classification requires that employers ensure these systems include built-in human oversight, maintain automatic operating logs and undergo a formal risk management process. N.B! The entry into force of some provisions is being delayed to 2027–2028. Read more about the anticipated changes to the EU legislation earlier in this chapter.	Check if a system is high-risk, for example by asking the employer, DPO or a union lawyer. If so, demand its risk assessments, technical documentation, and operating logs to verify automated decisions and ensure genuine human oversight.

REFERENCES BY SECTION

Step-by-step instructions for using the rights granted by the GDPR in everyday situations

"A user guide to data protection in the European Union: Your rights and how to exercise them". Access Now,. July 2018.

Briône, P. (2020) "Algorithmic management: A trade union guide". UNI Global Union Professionals & Managers, 1 September.

Colclough, C. J. (n.d.) "The data lifecycle at work – ensuring collective data rights". The Why Not Lab.

Cox, T. and Oosterwijk (2024) "Algorithmic management in the workplace: Case studies on the impact of algorithmic technologies in seven sectors in the Nordics". Policy study. Foundation for European Progressive Studies, October.

Geyer, L. (2025) "Workshop: Use the GDPR to help workers and advance union goals". Presentation slides. Platforum Conference, Nicosia, 25-26 September.

"GDPR: How to make it work for unions: Toolbox for trade unionists". industriAll European Trade Union.

"Data protection officers". Office of the Data Protection Ombudsman.

"Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". OJ L 119/1, 27.4.2016.

"Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)". OJ L, 13.6.2024.

"Digital technology: Guide for union representatives". Prospect."A checklist to responsible use of algorithmic systems: Co-governance guide". Public Services International.

Reuter, P. (2018) "The General Data Protection Regulation (GDPR): An EPSU briefing". European Public Service Union.

"Negotiating data rights: GDPR". The Why Not Lab."When AI is the boss: An introduction for union reps". Trades Union Congress, December 2021.

"People-powered technology: Collective agreements and digital management systems". Trades Union Congress, August 2022.

"Top 10 principles for workers' data privacy and protection". UNI Global Union.

Wray, B. (2025) "Negotiating the algorithm: Trade union manual". European Trade Union Confederation, September.

Understanding algorithmic management at work and its foundations in data

"Din kollega har blivit en algoritm: Digitalisering, AI och automatisering ur ett fackligt perspektiv", 3rd ed. Akademikerförbundet SSR, April 2025.

Briône, P. (2020) "Algorithmic management: A trade union guide". UNI Global Union Professionals & Managers, 1 September.

Cox, T. and J. Anttila (2024) "Algorithmic management and workplace digitalisation in Finland: Insights from the transport and logistics and retail sectors". Policy study. Foundation for European Progressive Studies, September.

Cox, T. and G. R. Oosterwijk (2024) "Algorithmic management in the workplace: Case studies on the impact of algorithmic technologies in seven sectors in the Nordics". Policy study. Foundation for European Progressive Studies, October.

Håkansta, C., R. Lind, P. Strauss-Raats et al. (2024) "Algorithmic management: Experiences and responses: Explorative study of companies and trade unions in the Swedish warehousing, retail and transport industries". Policy study. Foundation for European Progressive Studies, December.

Lahti, H. and T. Valtonen (2025). "Report: Algorithmic management is becoming more common in the Nordics — researchers warn about its impact on employee well-being". Finnish Institute of Occupational Health, 8 September.

Mikkonen, J., A. Pura, E. Välimäki et al. (2026) "AI, automation and public authority: Beyond the hype of algorithmic decision-making in the Nordic Welfare State". Policy study. Foundation for European Progressive Studies.

"When AI is the boss: An introduction for union reps". Trades Union Congress, December 2021.

Wray, B. (2025) "Negotiating the algorithm: Trade union manual". European Trade Union Confederation, September.

Your best tool to challenge algorithmic management at work: the GDPR

"A user guide to data protection in the European Union: Your rights and how to exercise them". Access Now, July 2018.

Aloisi, A. (2024) "Regulating algorithmic management at work in the European Union: Data protection, non-discrimination and collective rights". *International Journal of Comparative Labour Law and Industrial Relations*, 1(40): 37-70. DOI: 10.54648/ijcl2024001

Colclough, C. J. (n.d.) "The data lifecycle at work – ensuring collective data rights". The Why Not Lab.

Cox, T. and G. R. Oosterwijk (2024) "Algorithmic management in the workplace: Case studies on the impact of algorithmic technologies in seven sectors in the Nordics". Policy study. Foundation for European Progressive Studies, October.

"Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679". WP251rev.01. Article 29 Data Protection Working Party. European Commission, 6 February 2018.

Geyer, L. (2025) "Workshop: Use the GDPR to help workers and advance union goals". Presentation slides. Platforum Conference, Nicosia, 25-26 September.

"GDPR: How to make it work for unions: Toolbox for trade unionists". industriAll European Trade Union.

Kivikari, I. and O. Paasikivi (2025) "The Digital Omnibus - what the future looks like for data protection in the EU". Dittmar & Indrenius Attorneys Ltd., 11 February.

"Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". OJ L 119/1, 27.4.2016.

"Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)". OJ L, 13.6.2024.

Patel, A. (2021) "Participatory data stewardship: A framework for involving people in the use of data". Ada Lovelace Institute, 7 September.

"Digital technology: Guide for union representatives". Prospect.

Reuter, P. (2018) "The General Data Protection Regulation (GDPR): An EPSU briefing". European Public Service Union.

Silberman, M. S. and H. Johnston (2020) "Using GDPR to improve legal clarity and working conditions on digital labour platforms: Can a code of conduct as provided for by Article 40 of the General Data Protection Regulation (GDPR) help workers and socially responsible platforms?" *ETUI Research Paper – Working Paper 2020.05*. DOI: 10.2139/ssrn.3699338

"Negotiating data rights: GDPR". The Why Not Lab.

"When AI is the boss: An introduction for union reps". Trades Union Congress, December 2021.

Wray, B. (2025) "Negotiating the algorithm: Trade union manual". European Trade Union Confederation, September.

ABOUT FEPS AND PARTNERS

ABOUT THE FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES (FEPS)

FEPS is the European progressive political foundation and the think tank of the progressive political family at EU level. Our mission is to develop innovative research, policy advice, training and debates to inspire and inform progressive politics and policies across Europe.

FEPS
FOUNDATION FOR EUROPEAN
PROGRESSIVE STUDIES

Avenue des Arts 46
1000 Brussels, Belgium
info@feps-europe.eu
www.feps-europe.eu
@FEPS_Europe

ABOUT DEMOS HELSINKI

Demos Helsinki is an independent, globally operating not-for-profit think tank that drives societal change for fair, sustainable and joyful futures. We believe that this can only be achieved together, in collaboration with partners willing to push for change. We conduct interdisciplinary research, facilitate cross-sector collaboration, and support policymakers and organisations in developing evidence-based solutions to societal challenges.

DEMOS
HELSINKI

Mechelininkatu 3d
00100 Helsinki
info@demoshelsinki.fi
https://demoshelsinki.fi/
@demoshelsinki

ABOUT THE FEPS-NORDIC DIGITAL PROGRAMME

This guide is published as part of the FEPS-Nordic Digital Programme, a collaboration between FEPS and its members and trade unions from Denmark, Sweden, Norway and Finland.

The 2025-2026 programme has focused on the impact of AI on labour productivity and the public sector, as well as trade union capacity building in relation to algorithmic management and other aspects of workplace digitalisation.

Members of the FEPS-Nordic Digital Programme 2025-2026 Consortium are:

Kalevi
Sorsa
Foundation

Kalevi Sorsa Foundation
Siltasaarenkatu 18-20 C
00530 Helsinki (Finland)
https://www.sorsafoundation.fi/
@SorsaFoundation



Akademikerförbundet SSR
Box 128 00
112 96 Stockholm (Sweden)
https://akademssr.se/
@akademssr



Friedrich-Ebert-Stiftung Nordic Countries (FES)
Barnhusgatan 10
111 23 Stockholm (Sweden)
https://nordics.fes.de/
@FES_Nordics



The Economic Council of the Labour Movement (Arbejder-bevægelsens Erhvervsråd - AE)
Reventlowsgade 14
1651 Copenhagen (Denmark)
https://www.ae.dk
@tAEnketank



The Swedish Trade Union Confederation (Landsorganisationen i Sverige - LO Sweden)
Barnhusgatan 18
105 53 Stockholm (Sweden)
https://www.lo.se/
@LOSverige



The Swedish Union of Commercial Workers (Handelsanställdas Förbund - Handels)
Sveavägen 90
111 81 Stockholm (Sweden)
https://www.handels.se/
@handelsfacket



Delta
Pb. 9202, Grønland
0134 Oslo (Norway)
https://www.delta.no/
@deltaiys

Supporting unions of the FEPS-Nordic Digital Programme 2025-2026 are:

Service Union United (Palvelualojen ammattiliitto - PAM)
Siltasaarenkatu 18 A
00530 Helsinki (Finland)
https://www.pam.fi/
@pam.fi
The Central Organisation of Finnish Trade Unions (Suomen

Ammattiliittojen Keskusjärjestö - SAK)
Pitkäsillanranta 3
00531 Helsinki (Finland)
https://www.sak.fi/
@sak.fi

Industrial Employees (Teollisuuden Palkansaajat - TP)
John Stenbergin ranta 6
00530 Helsinki (Finland)
https://tpry.fi/
@TP_palkansaajat

Danish Union of Metalworkers (Dansk Metal)
Molestien 7
2450 Copenhagen (Denmark)
https://www.danskmetal.dk/
@danskmetal

Union of Commercial and Clerical Employees in Denmark (HK Danmark)
Weidekampsgade 8
2300 Copenhagen (Denmark)
https://www.hk.dk
@hkdanmark

Danish Trade Union Confederation (Fagbevægelsens Hovedorganisation - FH)
Islands Brugge 32D
2300 Copenhagen (Denmark)
https://fho.dk
@FH_danmark

ACTIVITY BACKGROUND

This guide is published as part of the FEPS-Nordic Digital Programme.

It reflects the opinions of the authors, not those of the European Parliament, FEPS, nor the participating member foundations and supporting unions of the FEPS-Nordic Digital Programme Consortium. The responsibility of FEPS is limited to the publication.

AI USE DISCLOSURE STATEMENT

This publication was written in accordance with FEPS guidelines on the responsible use of AI in research and writing activities. NotebookLM was used to support synthesising content across sources. Claude was used to help with text editing. Grammarly was used to notice grammatical errors and typos in the text. Accountability for all analysis, conclusions, and recommendations lies with the authors, who have written the text.

This guide is produced with the financial support of the European Parliament. It does not represent the views of the European Parliament.

Copyright © 2026 by the Foundation for European Progressive Studies and Demos Helsinki

Content editor: Anne-Christine Lacoste, STICS asbl

FEPS project coordinators: Monty Aal, Vanessa Zwisele

Language editor: Rosalyne Cowie

Layout: YESNOW

Cover image: YESNOW

ISBN: 978-2-39076-096-2

KBR deposit number: D/2026/15396./47

GUIDE PUBLISHED IN OCTOBER 2026 BY:

Copyright © 2026 by the Foundation for European Progressive Studies and Demos Helsinki



ISBN: 978-2-39076-096-2