

About this guidance	2
Data protection and monitoring workers	3
What do we need to do if we use monitoring tools that use solely automated processes?	26
Specific data protection considerations for different ways or methods of monitoring workers	31
Can we use biometric data for time and attendance control and monitoring?	42
Checklists	49

About this guidance

This guidance discusses the monitoring of workers by employers, and how this interacts with data protection. It is primarily aimed at employers. The guidance aims to:

- help provide greater regulatory certainty;
- protect workers' data protection rights; and
- help employers to build trust with workers, customers and service users.

The guidance provides clarity and practical advice to help employers to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). It assumes some knowledge of data protection, but provides links to other pieces of key data protection guidance, if you want to find out more information.

We use the term 'worker' throughout this guidance only to refer to someone who performs work for an organisation. Business models have changed in the last decade, with the rise of the gig economy. This guidance captures these relationships too. It is aimed at all circumstances where there is an employment relationship or otherwise a relationship between an organisation and a person who performs work for the organisation, regardless of the nature of the contract.

To help you understand the law and good practice as clearly as possible, this guidance says what organisations must, should, and could do to comply.

Legislative requirements

Must refers to legislative requirements.

Good practice

Should does not refer to a legislative requirement, but what we expect you to do to comply effectively with the law. You should do this unless there is a good reason not to. If you choose to take a different approach, you must be able to demonstrate that this approach also complies with the law.

Could refers to an option or example that you could consider to help you to comply effectively. There are likely to be various other ways you could comply.

Data protection and monitoring workers

In detail

- What do we mean by monitoring workers?
- Can we monitor workers?
- How do we lawfully monitor workers?
- How do we identify a lawful basis?
- What if our monitoring involves special category data?
- What about criminal offence data?
- Are there other laws we should consider?
- How do we ensure our monitoring is fair?
- How do we ensure that we are transparent about monitoring?
- How do we demonstrate accountability?
- Do we need to do a data protection impact assessment (DPIA) before we start monitoring?
- Do we have to define our purpose for monitoring workers?
- Do we need to restrict the amount of information we collect when we monitor workers?
- How do we ensure accuracy?
- How long should we keep information obtained from monitoring workers?
- How do we ensure the security of personal information obtained from monitoring workers?
- What must we tell workers about our monitoring?
- Should we discuss the introduction of monitoring with our workers?
- Can we use covert monitoring?
- Can workers request access to their personal information obtained from monitoring?
- Can workers object to being monitored?
- What do we need to consider if we use a third-party provider or an application provided by a third party to carry out monitoring?
- What do we need to consider if we transfer personal information of workers outside the UK?
- Checklist

What do we mean by monitoring workers?

Workers largely recognise that employers carry out checks on the quality and quantity of their work. Employers may also monitor workers to protect health and safety, or to meet regulatory obligations (eg requirements in the financial services industry). Monitoring can also form part of the security measures an organisation has in place to protect personal information. Increasingly, employers are using data analytics to infer worker performance and wellbeing.

We use the term 'monitoring workers' to mean any form of monitoring of people who carry out work on

your behalf. This can include monitoring workers on particular work premises or elsewhere, and can include monitoring during or outside work hours. To comply with data protection law, you **must** do this monitoring in a way that is lawful and fair to workers.

This guidance is not relevant to people recording information in a personal or household context, unless there is professional or commercial activity. For example, you run a business from home. This guidance also covers you if you employ a visiting worker to your household, such as a nanny or gardener, and monitor their activity routinely, or on an ongoing basis. It is also important to note that homeworking does not constitute personal or household processing, and so is also covered by this guidance.

Excessive monitoring can have an adverse impact on the data protection rights and freedoms of workers. Excessive monitoring is likely to intrude into workers' private lives and undermine their privacy and mental wellbeing. It is not always easy to distinguish between workplace and private information, especially when workers are based at home. Some workers may also use personal devices for work. Monitoring communications between a worker and their union representative or capturing a worker's personal correspondence both give rise to significant concerns. (See the sections [What if our monitoring involves special category data?](#) and [Can we monitor emails and messages?](#).)

As an employer, there may be occasions when you need to consider sharing personal information you have obtained from monitoring your workers with a law enforcement authority. For example, you may discover suspected criminal activity by a worker, such as fraud or theft. This guidance does not apply to processing carried out for the purposes of law enforcement. Law enforcement authorities are subject to the separate law enforcement regime under Part 3 of the DPA 2018.

This guidance covers systematic monitoring, where an employer monitors all workers or groups of workers as a matter of course. For example, if you use software to monitor productivity. It also applies to occasional monitoring, where an employer introduces monitoring as a short-term response to a specific need. This includes installing a camera to detect suspected theft, or a software package created to monitor workers systematically, but where monitoring functions are not always active, for example taking random screenshots.

Monitoring technologies and purposes may include:

- camera surveillance including wearable cameras for the purpose of health and safety;
- webcams and screenshots;
- technologies for monitoring timekeeping or access control;
- keystroke monitoring to track, capture and log keyboard activity;
- productivity tools which log how workers spend their time;
- tracking internet activity and keystrokes;
- body worn devices to track the locations of workers; and
- hidden audio recording.

The technologies that employers use to monitor their workers have changed rapidly over time and will undoubtedly continue to evolve in sophistication. However, you **must** follow the data protection principles regardless of technological developments.

Further reading

- We have [produced separate guidance to help you if you need to share personal information with a law enforcement authority](#).

Can we monitor workers?

Data protection law does not prevent you from monitoring workers, but you **must** do so in a way which is compliant with data protection requirements. Article 8 of the Human Rights Act 1998 concerns the right to respect for a private and family life. This is increasingly important due to the rise of homeworking. Workers' expectation of privacy are likely to be significantly greater at home than in the workplace and the risks of capturing information about your workers' family and private lives (if you monitor them when they are working from home) are higher.

You can monitor workers if you do it in a way which is consistent with data protection law.

When deciding whether to monitor workers carefully balance your business interests as an employer and workers' rights and freedoms under data protection law.

If you carry out monitoring in a way which is unfair, this will impact on their rights and freedoms under data protection law. It will also negatively affect the trust between you and your workers, as well as potentially affecting their mental wellbeing. Just because a form of monitoring is available, does not mean it is the best way to achieve your aims. You **must** be clear about your purpose and select the least intrusive means to achieve it.

Example

After an employer discovers that a small number of remote workers started later than they recorded on their timesheets, it rolls out device monitoring. This allows senior management to access automatic webcam images and check if workers are at work.

This is likely to infringe data protection law because it is disproportionate, and there are less intrusive ways to check start times.

The employer can achieve the same purpose by checking the times workers log onto the computer system, and then give workers the opportunity to explain any discrepancies.

How do we lawfully monitor workers?

To lawfully collect and process information from monitoring workers, you **must** identify a lawful basis. There are six to choose from and you **must** identify at least one that is appropriate for the type of processing you intend to do.

Monitoring workers often includes capturing sensitive information. This is called 'special category data' in the UK GDPR. Because of its sensitivity, special category data requires extra protection. If the nature of your monitoring means that you will collect special category data, or are likely to, you **must** identify a

special category processing condition, as well as a lawful basis. (See the sections on [lawful basis](#) and [special category data](#).)

You **must** also ensure any monitoring is lawful in the general sense. If you are considering monitoring workers, you **should** consider all the legal implications of any other relevant laws.

Example

A bank monitors all transactions made by every worker to prevent and detect fraud. This does not involve processing special category data. The bank needs to identify a lawful basis, but not a condition for processing.

Example

A bank wishes to monitor all email traffic to address the risk of fraud and protect commercially sensitive information. As well as a lawful basis, the bank should identify a special category condition. This is because monitoring all email traffic could detect special category data, such as emails sent to union representatives or to occupational health personnel.

How do we identify a lawful basis?

How you decide which lawful basis applies depends on your specific purpose and the context of the monitoring. You **must** think about why you want to monitor workers. You **must** identify which lawful basis best fits the circumstances. We have listed the available lawful bases below, along with some guidance to help you identify the right basis for your circumstances. You can also use our [interactive guidance tool](#) to help you. Carrying out a data protection impact assessment (DPIA) may also help you to identify the most appropriate basis.

You **must not** adopt a one-size-fits-all approach. No one basis is always better, safer or more important than the others. However, some are likely to be more appropriate than others for employers. We highlight some of these below.

Sometimes, more than one basis might apply. You **should** identify all those that apply, and document them from the start. Try to get it right first time, as you **should not** change it later without good reason.

The six lawful bases are:

Consent

The worker gives consent for you to process their personal data for a specific purpose.

A person **must** freely give their consent for it to be valid. This means that consent is not usually appropriate in the employment context, due to the imbalance of power between you and your workers. Workers are likely to feel that they have no choice but to give you consent.

Consent **must** be unambiguous and include an affirmative action. You **must**:

- give workers the option to withdraw their consent without detriment;
- make this as easy as when they first provided it; and
- keep records of when and how you gained consent, and what exactly workers consented to.

Consent is only appropriate if circumstances mean workers have a genuine choice and control over the monitoring.

Contract

The monitoring is necessary for a contract (such as the employment contract) you have with the worker, or because they asked you to take specific steps before entering into a contract.

You **should only** use this lawful basis if it is necessary for your side of the contract as an employer. Whilst scenarios may exist where the use of employee monitoring is the only way for you to fulfil your side of a contract, these are hard to envisage.

As monitoring is more often for internal business improvement purposes, it's unlikely that it will be a suitable lawful basis for monitoring workers.

Example

An employer inserts a clause into its employment contracts to say that it employs video surveillance across its premises to monitor productivity and improve efficiency. This would not be sufficient justification to use this lawful basis for such monitoring as there are other less intrusive ways of improving productivity.

Legal obligation

The processing is necessary for you to comply with the law.

You can rely on this lawful basis if you monitor workers to comply with a common law or statutory obligation. This does not apply to contractual obligations. In order to rely on this basis you **must** either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your obligation.

Example

A logistics company needs to monitor driving time, speed and distance to comply with the rules on drivers' working hours. Legal obligation is appropriate as a lawful basis. The logistics company documents the decision to rely on this lawful basis and signposts to the legislation which applies. The company does not process more information than necessary to fulfil obligations under the rules on drivers' hours. They also do not use the information for any other purposes.

Vital interests

The processing is necessary to protect someone's life.

This is for emergencies, where you need to process personal information to protect someone's life. This lawful basis is very limited in its scope and generally only applies to matters of life and death.

Example

A test pilot is monitored for several important factors, such as heart rate, blood pressure and brain activity. These factors may change in the demanding and dangerous job of test flights. These are vital to make sure the pilot is kept safe. On the other hand, an office worker would not expect to be monitored for these things, as there would be little in their job that would affect these factors. It is likely that another lawful basis for monitoring would be more suitable.

Public task

The processing is necessary for you to perform a task in the public interest or for your official functions.

You **must** have a clear basis in law for the task or function. This is most relevant to public authorities, but it can apply to any organisation that exercises official authority or carries out tasks in the public interest that have a clear basis in law. For example, a private organisation or charity working under contract to a public authority to help deliver one of their defined legal functions.

This basis may be appropriate if:

- you are a public authority or your organisation carries out tasks in the public interest; and
- you can demonstrate that monitoring workers is necessary to perform your tasks as set down in UK law.

You **should** assess the basis in law of the specific monitoring activity. You cannot rely on this basis if you could achieve the same purpose in a less intrusive way.

If monitoring is not necessary for you to perform your public task then you cannot rely upon this lawful basis.

Legitimate interests

The processing is necessary for your legitimate interests or those of a third party, unless the risks to the workers' rights overrides them.

This basis is the most flexible and could apply in a wide range of circumstances.

Legitimate interests may not be the most appropriate lawful basis if:

- you are monitoring in ways workers do not understand and would not reasonably expect; or
- it is likely some workers would object if you explained it to them.

You **could** use the DPIA process help you to assess this. (See the section on [DPIAs](#)).

Depending on the work they undertake, and the contexts they work in, workers can reasonably expect different levels of monitoring to fall within the legitimate interest definition

Example

A miner would reasonably expect to wear a tracking device within a mine. This would be due to the dangerous work they undertake, the risks involved in potential accidents and the need to keep track of their location within the mine.

However, an office worker would not reasonably expect to wear a tracking device in an office setting. There is far less risk working day-to-day in an office than a mine and office workers would not reasonably expect such a level of monitoring.

When deciding if the proposed monitoring is appropriate, you **must** balance your legitimate interests and the necessity of the monitoring against the interests, rights and freedoms of workers, considering the particular circumstances. This is different to the other lawful bases which presume that your interests and those of the worker are balanced.

You can break the key elements of the legitimate interests basis down into a three-part test:

- **Purpose test**– is there a legitimate interest behind the processing?
- **Necessity test**– is the processing necessary for that purpose?
- **Balancing test**– is the legitimate interest overridden by the person’s interests, rights or freedoms?

You **should** assess each of the tests before processing and document the outcome, so you can demonstrate that legitimate interests applies. You **should** do this by carrying out a legitimate interests assessment.

Further reading

- Please also see our separate [lawful basis guidance](#) [↗](#) for more general information about the different bases available.
- See also our [legitimate interest assessment](#) [↗](#), including a template you can use.

What if our monitoring involves special category data?

Special category data is personal information revealing or concerning:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where used for identification or authentication purposes);
- health or disability;
- sex life; or
- sexual orientation.

It needs more protection because it is sensitive and the risks of harm to the person from its inappropriate disclosure or use are likely to be higher.

When you are planning to carry out monitoring, you **should** consider whether you are going to capture any of the above types of information.

If the planned monitoring captures this type of information, you **must** have a special category condition, as well as a lawful basis, before you start the monitoring.

In certain circumstances, your planned monitoring may capture special category data incidentally. You may not plan to collect it, but the nature of the monitoring might make it likely (eg where monitoring may identify emails between a worker and a healthcare provider or a trade union representative). If this is the case, you **must** identify a condition for processing.

When choosing a condition for processing, think about your purpose for monitoring, as this helps you identify the most appropriate condition. In circumstances where you do not intend to capture special category data, but it's likely that you will do so, you **should** demonstrate that your purpose for monitoring outweighs the risk of inadvertently capturing special category data. The condition you choose **should** reflect this purpose. Carrying out a DPIA helps you do both of these things. (See the section on [DPIAs](#).)

If you process, or are likely to process special category data, it is possible that the information you gather may be protected by other laws as well. (See the section [Are there other laws we should consider?](#))

You **must** only keep the information which is relevant to your purpose for monitoring. This is particularly important because of the higher risks of collecting and using special category data. You **should** regularly review the information you are collecting and destroy what is not necessary.

If it's unlikely you'll capture any special category data, you **could** document a condition to minimise risks. However, you are not obliged to.

There are 10 conditions for processing special category data. Five of these require you to meet additional conditions and safeguards set out in Schedule 1 of the DPA 2018. (See [what are the conditions for processing](#)). You **should** also carry out a DPIA before you begin.

Further reading

Below, we discuss some of the conditions for processing special category data which may be relevant in the context of monitoring workers.

Explicit consent

You can only rely on this condition if workers have control and choice over the monitoring. Explicit consent is not specifically defined by the UK GDPR but is similar to the lawful basis of consent. If you want to rely on this condition, you **must** ensure that workers provide explicit consent in a clear statement (whether written or oral). Explicit consent cannot be implied. To rely on this condition, you **must** ensure workers have a genuine option, with no negative impact (either actual or perceived) for withholding explicit consent. This is unlikely in most employment circumstances. As with the lawful basis of consent, this is not usually appropriate in the employment context due to the imbalance of power between you and your workers. There may be some limited circumstances where it can apply.

Example

An employer wants to introduce an access control system which uses workers' biometric data to sign them into work devices. They have carried out a DPIA and established the necessity and proportionality of this method. They offer a feasible alternative (such as PIN codes) to workers who withhold explicit consent. This does not negatively impact those workers. Therefore they can rely on explicit consent as their condition for processing


In most scenarios, it is unlikely that workers will have full control or choice over the monitoring you're planning to use. This means you are unlikely to be able to rely on explicit consent.

Employment, social security and social protection (if authorised by law)

This condition may be relevant if you are monitoring to ensure the health, safety and welfare of workers. Your purpose **must** be to comply with employment law or social security and social protection law. You **must** identify the legal obligation or right in question, either by referring to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you **could** refer to a government website or to industry guidance that explains generally applicable employment obligations or rights.

This condition does not cover processing to meet purely contractual employment rights or obligations. If you are relying on this condition, you **must** also meet the associated condition set out in Part 1 of Schedule 1 of the DPA 2018. This condition requires you to have an appropriate policy document in place.

Further reading

- [Appropriate policy document](#) 

Substantial public interest (with a basis in law)




To rely on this condition, you **must** be clear that the monitoring is necessary in the public interest and with a basis in law. You **must** also justify the processing of special category data to achieve your purpose.

To meet this condition, you **must** demonstrate the wider substantial public benefit and basis in law for your processing. You **must** also identify a relevant substantial public interest condition as set out in Part 2 of Schedule 1 of the DPA 2018. You **must** also have an appropriate policy document in place for almost all of these conditions.

Example

A bank uses CCTV to detect and prevent crime. As footage may capture special category data about workers and customers, the bank relies on 'reasons of substantial public interest', and it meets the public interest condition 'preventing or detecting unlawful acts'.


Further reading

- [Special category data](#) 
- [Substantial public interest conditions](#) 
- [Appropriate policy document](#) 

What about criminal offence data?

Similar to special category data, data protection law gives extra protection to personal information about offenders or suspected offenders regarding criminal activity, allegations, investigations or proceedings. Article 10 of the UK GDPR restricts the processing of criminal offence data. You **must only** process criminal offence data if the processing is **either** under the control of [official authority](#) **or** authorised by domestic law (schedule 1 of the DPA 2018.) If you are monitoring workers to detect criminal activity, you **must** identify a specific condition for processing in schedule 1 of the DPA 2018.

Further reading

- [Criminal offence data](#) 

Are there other laws we should consider?

This guidance aims to help you comply with data protection obligations when monitoring workers. Any monitoring you undertake **must** be lawful and fair. There are other laws that you **should** also consider when monitoring workers, outside data protection. These include, but are not limited to, the Human Rights Act 1998, Equalities legislation and investigatory powers regulations.

Other sources

- [Human Rights Act 1998](#) 
- [Equality Act 2010](#) 
- [Section 75 Northern Ireland Act 1998](#) 
- [The Investigatory Powers \(Interception by Businesses etc. for Monitoring and Record-Keeping Purposes\) Regulations 2018](#) 
- [Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#) 
- [Equality and Human Rights Commission](#) 
- [IPCO – Investigatory Powers Commissioner's Office](#) 

How do we ensure our monitoring is fair?

Fairness is a key data protection concept. It means you **should** only monitor workers in ways they would reasonably expect and not in ways that cause unjustified adverse effects on them.

In some circumstances you **must** carry out a DPIA before carrying out monitoring. Even if you are not required to carry one out, you **should** still do so. The results of a DPIA will help you consider whether the planned use of monitoring is fair, for example by considering the risks of unjustified or adverse processing involved in installing CCTV systems in your business premises.

(See the section [Do we need to do a data protection impact assessment \(DPIA\) before we start monitoring?](#))

Example

Workers report thefts from staff changing rooms. The employer considers installing CCTV in the changing rooms for the purpose of detecting and preventing thefts. The adverse effect of filming workers when they would reasonably expect privacy means this monitoring is unfair.

To help ensure fairness, the employer instead decides to install CCTV to monitor the door outside the changing room. This will narrow the scope of any investigation of further thefts and act as a deterrent. They also install signs to inform workers of its presence and the purpose of the camera. As this in itself poses a risk to the information rights and freedoms of workers, the operation of the CCTV is time limited to the duration of the investigation, and the company destroys any information not relevant to the investigation.

Example




An employer uses a software tool to monitor how long workers spend using a case management system. They use the monitoring reports to assess the performance of workers. The reports do not take into account the reasonable adjustments some workers have, which mean they work outside of the system for some tasks. Unless the employer takes into account the work done outside the system, the monitoring is unfair and inadequate.

How do we ensure we are transparent about monitoring?

Transparency is about being clear with workers about how and why you process their information. It is fundamentally linked to fairness. Building trust with your workers starts with transparency. Monitoring conducted without transparency is unfair and could negatively impact trust relationships. Workers have the right to be informed about the collection and use of their information, and you **must** tell workers about monitoring in a way that is accessible and easy to understand. (See the section about [privacy information](#).)

Apart from in very exceptional circumstances where covert monitoring is justified, you **must** inform workers about any monitoring. (See the section on [covert monitoring](#).)

Further reading




- [What is transparency?](#) 
- [Accountability framework - transparency](#) 
- [Right to be informed](#) 

How do we demonstrate accountability?

The principle of accountability makes you responsible for complying with the UK GDPR and says you **must** demonstrate your compliance. Putting in place appropriate policies, procedures and measures helps you demonstrate accountability. These **must** be proportionate to the risks, which vary depending on your type of worker monitoring, the level of intrusion and the technology you use.


You **should** make sure overall responsibility for monitoring workers rests at the highest senior management level. If you have a data protection officer (DPO), you **must** make sure they are closely involved in any plans to monitor workers. You **should** brief any workers involved in processes that are used for monitoring workers on data protection law and their roles within it.

Further reading

- [Accountability and governance](#) 
- Our [accountability framework](#)  is a flexible tool to help you plan and show your compliance. It can help in appropriately documenting your lawful basis for monitoring.
- [Data Protection Officers](#) 

Do we need to do a data protection impact assessment (DPIA) before we start monitoring?

DPIAs are an important accountability tool. Completing a DPIA helps you to identify and minimise the risks of any monitoring activity you might plan. The DPIA process includes a step where you can discuss your plans to introduce monitoring with workers. This helps to shape your plans and build trust with workers. When carrying out a DPIA you **should** also consider anyone else captured by your monitoring plans, such as customers, members of the public or household members, if your workers are based at home.

You **must** carry out a DPIA before undertaking any processing likely to cause high risk to workers' and other people's interests. You **should** use our [screening checklists](#)  and read our detailed DPIA guidance to help you decide.

Examples of high risk processing can include:

- processing biometric data of workers;
- keystroke monitoring of workers;
- monitoring that may result in financial loss (such as performance management); or
- using profiling or special category data to decide on access to services.

If you have a data protection officer (DPO), you **must** seek and record their independent advice on the outcome of the DPIA before making any final decisions.

If, following your DPIA, you decide to go ahead with your proposed monitoring, you **must** provide information about it to your workers before you begin monitoring.

You **should** carry out a DPIA even if there is no specific high risk as it is a flexible and scalable tool which can assist your decision-making. If you decide to proceed without carrying out a DPIA, you **should** document your decision.

If you have carried out a DPIA which identifies high risk that you cannot reduce, you **must** consult the ICO before going ahead with the monitoring.

Further reading

- For more information, see our guidance on [DPIAs](#) , especially the subsection [When do we need a](#)

- [Data Protection Officers \[↗\]\(#\)](#)

Do we have to define our purpose for monitoring workers?

Yes. Purpose limitation is a key principle of data protection law. You **must** be clear about the purpose for monitoring. For example, you may decide to monitor email traffic for security purposes, or use CCTV for site safety purposes. However, you **should not** monitor workers 'just in case'. You **must** document why you are monitoring workers and what you intend to do with the information you collect.

If the monitoring is to enforce your organisation's policies, make sure these are clearly set out. You **should** regularly bring the policies to the attention of workers. The policy or policies **should** also outline the nature, purpose and extent of any monitoring.

Example

An employer has acceptable usage rules for using the internet. They document these rules in a policy which is made known and accessible to all workers affected. Either in this policy, or linked from this policy, the employer sets out privacy information which explains:

- how they monitor these rules;
- how they use the information obtained from the monitoring; and
- the safeguards in place for the workers being monitored.

You **should** consider that workers base their expectations of privacy on practice, as well as policy. Excessive monitoring set out in a policy does not make it lawful, just because it is documented.

Example

An employer has a policy which imposes a ban on personal calls, but in practice, they overlook a limited number of personal calls. The employer cannot rely on the policy to justify carrying out monitoring.

You can set systems so that workers cannot access the internet or applications without accepting certain conditions. This can reduce the need for some types of monitoring.

Example

An employer minimises the risks of unacceptable usage by blocking some websites (personal email, social media sites and entertainment sites). This means they can minimise unacceptable usage rather than monitor for it.

You can only change your purpose for monitoring if:

- your new purpose is compatible with your original purpose;
- you get consent; or
- you have a clear obligation or function set out in law.

Do we need to restrict the amount of information we collect when we monitor workers?

Yes. The data minimisation principle means you **must not** collect more information than you need to achieve your purpose. It is closely linked to purpose limitation. Monitoring technologies and methods have the capability to gather wider categories and larger amounts of information than may be necessary to achieve your purpose. This risks 'function creep', where information is used for wider purposes than the original intention. This can happen gradually over time, so you **should** review how you monitor workers regularly to prevent this. Similarly, you **must not** collect more information than is necessary, just in case it might prove useful to you in the future.

Example

An employer collects office ethernet connection data to monitor the use of workspaces and ensure there is sufficient capacity for workers. They **should not** re-use this information for performance management purposes without identifying a new lawful basis and establishing the necessity and proportionality of this new purpose.

Further reading

- [Data minimisation](#) 

How do we ensure accuracy?

You **must**:

- take all reasonable steps to ensure the personal information you gather through monitoring workers is not incorrect or misleading as to any matter of fact;
- if necessary, keep personal information updated;
- take reasonable steps to correct or erase personal information as soon as possible if you discover that it is incorrect or misleading; and
- carefully consider any challenges by workers to the accuracy of any information you gathered through

monitoring.



This particularly applies if you are using the information to make potentially adverse decisions about workers. For example, if you use monitoring information in performance reviews.

You **should** consider the following points:

- Equipment or systems malfunction can cause information collected through monitoring to be misleading or inaccurate (eg a computer system resetting to the wrong time zone).
- Information can also be misinterpreted or even deliberately falsified.
- Data analytic tools can make incorrect inferences about workers.

You **should** ensure that workers can see and, if necessary, explain or challenge the results of any monitoring. You **should** do this within, or alongside, disciplinary or grievance procedures and performance reviews or appraisals.

Further reading

- [Accuracy](#) 
- [Right to rectification](#) 

How long should we keep information obtained from monitoring workers?

You **must not** keep personal information obtained from monitoring workers for any longer than is necessary for your particular purpose or purposes. You **should** base any retention period you set on business need. You **should** review it regularly, and take into account any professional guidelines or legal obligations. You **should not** retain information just in case you find a purpose for it in the future. You **must** ensure you have a retention schedule and delete any information you collect from monitoring workers in line with your schedule. The UK GDPR doesn't specify retention periods. However, you **should** be able to justify any retention periods that you set, and be able to link these to the reasons why you have obtained the information.

Further reading

- [Storage limitation](#) 

How do we ensure the security of personal information obtained from monitoring workers?

Security is a key principle of data protection law. You **must** have appropriate organisational and technical measures in place to protect any personal information you collect through monitoring.

You **should**:

- assess the data security risks of any monitoring and use this to decide the security measures you need to put in place; and

- restrict access to the information to only those who need access. Take care to identify the most appropriate person or people to access the information you collect. You **should** properly train them to handle information obtained from monitoring.

If you decide to outsource your monitoring activities to a data processor, you **should** remember that as the controller, you are responsible for compliance with data protection law. This includes what the processor does with the information.

Processors also have their own set of security obligations under data protection law. (See the section on [third parties](#).)

Similarly, if you are using commercially available monitoring tools, or the monitoring functionalities which are available on communication and collaboration tools – you are still responsible for compliance with data protection. In particular, you **should** still consider the security and access controls on any information you collect. You **should not** assume the tool has the appropriate level of protection built-in. (See the section on [commercially available tools](#).)

Further reading

- [Security](#)

What must we tell workers about our monitoring?

You **must** make sure workers are aware of how and what personal information you are collecting during any monitoring. You **could** set up a system to ensure workers remain aware that monitoring is taking place. For example, through your organisation's intranet or signage in areas subject to monitoring. You **should** regularly review your monitoring practices and you **must** keep privacy information up-to-date. You **must** also tell workers when you introduce changes.

It is unfair to workers if you are unclear on whether you are monitoring them. Not providing workers with clarity around monitoring risks damaging trust between you and your workers. Similarly, if you are monitoring workers, uncertainty over the reason for doing so can have a negative effect. This might adversely impact the work of your organisation, as well as infringing the data protection rights and freedoms of workers. Making sure workers understand any monitoring builds trust and ensures you comply with workers' right to be informed.

See the section on [transparency and informing workers about monitoring workers](#).)

Further reading

- For more details on what information you **must** provide, see our guidance on [the right to be informed](#).

Should we discuss the introduction of monitoring with our workers?

If you are planning to introduce monitoring, you **should** seek and document the views of your workers or

their representatives (such as trade unions), unless there is a good reason not to. If you decide not to, you **should** record this decision along with a clear explanation. Seeking the views of workers as part of your planning process is a good way of being transparent and building trust with your workers. You can then address any feedback or questions in advance which helps you build good employment relationships and meet your obligations to protect workers' data protection rights and freedoms.

You **should** involve workers during the early planning stages. This can potentially avoid complaints from workers at a later stage, allows you to consider potential issues before they arise, and helps to build trust with workers. You **should** do this as part of your DPIA.

Further reading

- For more detail see our separate DPIA guidance [How do we do a DPIA?](#) ↗
- For more information on workers' right to object see the section [Can workers object to being monitored?](#) and our [guidance on the right to object.](#) ↗

Can we use covert monitoring?

Covert monitoring means carrying out monitoring in a way designed to ensure workers are unaware that it is taking place. It is unlikely that you will be able to justify covert monitoring in most usual circumstances. However, there may be exceptional circumstances where you might be able to justify this. For example, if covert monitoring is necessary to enable you to prevent or detect suspected criminal activity or gross misconduct.

You **should** outline in your organisational policies the types of behaviours that are not acceptable and the circumstances in which covert monitoring might take place.

If you are considering monitoring workers covertly, there are several factors to be aware of:

- Covert monitoring **should only** be authorised by senior management.
- You **must** carry out a DPIA.
- You **should** be satisfied that there are grounds for suspecting criminal activity (or an equivalent, such as gross misconduct) and that informing workers about the monitoring would prejudice its prevention or detection.
- You **should** strictly target the covert monitoring at obtaining evidence within a set timeframe, limited to the shortest time possible.
- You **should not** continue the covert monitoring after the investigation is complete.
- You **should not** use covert audio or video monitoring in areas where workers would reasonably expect to be private, such as toilets or changing rooms.
- In most circumstances, you **should not** use covert monitoring to capture communications that workers would reasonably expect to be private, such as personal emails.
- If you are considering using a private investigator to collect information on workers covertly, you **must** have a contract in place that requires them to only collect information in a way that satisfies your obligations under data protection law. See our [guidance on controllers and processors](#) ↗ for further details.

- You **must** only use information gathering through covert monitoring for the purpose intended. You **should** disregard and destroy any other information unless it reveals something that no employer could reasonably be expected to ignore and where there is no other way to achieve this purpose.
- You **should** limit the number of people involved in the investigation to only those who really need to be involved.
- You **should** set clear rules limiting disclosure and access to the information you collect.
- Remember workers' data protection rights. For example, if a worker submits a subject access request, you may have to disclose the personal information obtained from monitoring. You **should** deal with requests on a case-by-case basis.

Ultimately, you **should** balance the interests of the employer and the worker. However, you **should** be able to justify every decision you make to carry out any covert monitoring.

Further Reading

- Read our [guidance on individual rights](#) and our guidance on [the right of access](#) for further details.

Can workers request access to their personal information obtained from monitoring?

You **must** make the personal information you collect through monitoring available to workers if they make a subject access request (SAR), **unless** an exemption applies.

It may be challenging to respond to a SAR if the monitoring system you use collects large amounts of information, or contains the personal information of third parties. This is especially the case if the systems you use do not store information in a way that makes personal information readily retrievable. You **should** factor in how easy it is to retrieve information when considering what type of monitoring system you plan to introduce. You **should** do this in your DPIA.

Further reading

- [Right of access](#)
- [SARs Q and A for employers](#)

Can workers object to being monitored?

Yes, workers can object to you collecting and processing their personal information from monitoring in certain circumstances. Specifically, a worker can object where the lawful basis you are relying on is:

- public task (for the performance of a task carried out in the public interest or for the exercise of official authority vested in you); or
- legitimate interests.

The worker must give specific reasons why they are objecting to you collecting and processing personal information through monitoring. The reasons should be based on their particular situation.

However, this isn't an absolute right and you can refuse to comply with the objection if:

- you can demonstrate compelling legitimate interests for the processing, which override the interests, rights and freedoms of the worker; or
- the processing is for the establishment, exercise or defence of legal claims.

If you are deciding whether you have compelling legitimate interests which override the person's interests, you **should** consider the reasons why the worker has objected to the monitoring. If they object on the grounds that the monitoring is causing them substantial damage or distress, the grounds for their objection will have more weight. To decide, you **must** balance the worker's interests, rights and freedoms with your own legitimate interests. To continue with the monitoring, you **must** demonstrate that your legitimate grounds override those of the worker.

If you are satisfied you do not need to comply with the request, you **must** let the worker know. You **should** document and thoroughly explain your decision. You **must** inform them of their right to make a complaint to the ICO. You **must** also tell them of their ability to seek to enforce their rights through a judicial remedy.

You can also refuse to comply with an objection if it is:

- manifestly unfounded; or
- excessive.

Example


A worker sends different requests to you on a regular basis with the stated intention to cause disruption. This may be manifestly unfounded.

Further reading

- [The right to object](#) 

What do we need to consider if we use a third-party provider or an application provided by a third party to carry out monitoring?

If you decide to carry out monitoring of your workers, you **must** ensure that this is done fairly and lawfully. You are responsible for deciding how and why the monitoring takes place, including the use of any particular technology or service to do so.

You **should not** assume that packages you purchase are compliant with data protection law. Before you begin any monitoring activity, you **must** ensure the system or application is compliant with data protection law, and that you have any necessary contracts in place. A DPIA will help you consider the impact that processing activities may have on your workers. (See the [section on DPIAs](#).) If you or your provider are using automated decision-making techniques (AI) to process worker data, you **should** take additional considerations into account. (See our section on [automated decision-making](#) .)

If you use another organisation to carry out this monitoring on your behalf, and they only work to your written instruction, it is likely that they will be a processor.

Example

A company pays a third party to supply a system that provides salary and pension contributions and processes expenses. The payroll provider processes personal information about the company's workers and provides weekly reports to the company on the time worked by each staff member. The provider is a processor and the company is the controller. The company **must** ensure the payroll provider is compliant with data protection law.

You are responsible for making sure your processor is competent to process the personal information in compliance with data protection law. You **must** have a contract (or other legal act) in place so both parties understand their responsibilities and obligations.

You **must** make sure any third party provider you use processes personal information in compliance with data protection law. You **should not** assume that any third party software has been designed with data protection in mind.

If your monitoring involves AI and automated decision-making, or automated decision-making by itself, there are additional considerations that you or your provider **should** take into account. (See the section on [automated decision-making](#).)

A DPIA will help you to address these issues as well as considering the impact your monitoring may have on your workers. (See the [section on DPIAs](#).)

Further reading

- [Controllers and processors](#)
- [Contracts](#)
- [Data sharing agreements](#)
- [Contractual liability in data sharing agreements](#)

What do we need to consider if we transfer personal information of workers outside the UK?

Data protection law restricts the transfer of personal information to countries outside the UK or to international organisations. These restrictions apply to all transfers, no matter the size or how often you carry them out. We refer to these as restricted transfers.

The rules for international transfers apply if:

- you are agreeing to send personal information, or make it accessible, to a receiver which is located in a country outside the UK; and

- the receiver is legally distinct from you as it is a separate company, organisation or person. This includes transfers to another company within the same corporate group.

However, if you are sending personal information to someone employed by you, or by your company or organisation, this is not a restricted transfer. The transfer restrictions only apply if you are sending personal information outside your company or organisation.

If you are making a restricted transfer, you **must** make sure the transfer is covered by either:

- [adequacy regulations](#) – this is where another country has been assessed as providing 'adequate' data protection;
- [appropriate safeguards](#) – before you rely on one of these you **must** carry out a transfer risk assessment to be sure workers' information will have protection essentially equivalent to the UK data protection regime; or
- [an exception](#) – if you are making a restricted transfer that is not covered by UK adequacy regulations or an appropriate safeguard then you can only make the transfer if it is covered by an exception.

Example

A UK company uses an outsourced human resources service in India provided by its parent company. The UK company passes information about its workers to its parent company in connection with the HR service. This is a restricted transfer, so the UK company **must** ensure there are adequate safeguards in place.

If you use a processor based outside the UK, the rules on international transfers apply. Data protection law restricts the transfer of personal information to countries outside the UK or to international organisations.

Example

A UK company uses a USA based software application to monitor workers. The application provider hosts the personal information in the USA and is a processor. This is a restricted transfer, and the UK company **must** ensure it is covered by appropriate safeguards. The UK company **must** ensure the application provider provides all relevant information to ensure compliance with data protection law.


Further reading

If you are sending personal information about workers overseas, read our guidance on:

- [International transfers](#)
- [International data transfer agreement and guidance](#)

Checklist

- We have checked that the monitoring of workers is necessary for the purpose we have identified. We are satisfied there is no other reasonable and less intrusive way to achieve that purpose.
- We have considered whether we need to do a DPIA and either completed one or documented the reason we considered one wasn't required.
- When making our DPIA decision, we have considered seeking the views of workers and representatives and either done this or documented our decision not to.
- We have identified a lawful basis for monitoring workers.
- Where required, we have identified an appropriate special category condition for monitoring workers if we're likely to capture any special category data as part of our monitoring.
- We have documented what personal information we are processing when we monitor workers.
- Where required, we have an appropriate policy document in place.
- We have included specific information about monitoring workers in our privacy information so that workers are aware of any monitoring taking place. We have made sure that this information is readily accessible to workers.
- We have considered whether the risks associated with monitoring workers affects our other obligations around data minimisation, security, and appointing Data Protection Officers (DPOs) and representatives.
- We have considered data protection issues as part of the design and implementation of monitoring systems and practices, including where we use external suppliers for monitoring technology, and where we use the functionalities built into communication and collaboration work tools.
- Where necessary, we have considered the rules for international transfers.

You can also view and print off this checklist and all the checklists of this guidance on our [checklists page](#) .

What do we need to do if we use monitoring tools that use solely automated processes?

In detail

- [Why is this important?](#)
- [What do we mean by solely automated decision-making and profiling?](#)
- [What do we need to consider if we are planning to make solely automated decisions with legal or similar effect on workers?](#)
- [What should we tell workers about solely automated decision-making?](#)
- [What is the role of human oversight?](#)
- [Checklist](#)

Why is this important?

Tools for monitoring workers have become increasingly sophisticated, with automated processes (sometimes known as people analytics) often used for:

- security purposes;
- managing workers' performance; and
- monitoring sickness and attendance (including if a worker is away from their workstation).

There are business benefits to people analytics. They can contribute to improving organisational performance and can demonstrate compliance with HR policies. Such tools have the capacity to process large amounts of workers' information by monitoring in real time. This can be used to make predictions, inferences and decisions about workers on both an individual and a collective level. The UK GDPR has provisions on solely automated decision-making with legal or similarly significant effects, including profiling. We cover them here in the context of monitoring workers.

What do we mean by solely automated decision-making and profiling?

Solely automated decision-making is a decision made by automated means without any meaningful human involvement. Solely automated decision-making may involve profiling too. In a work context, this could be where employers use workers' information from a number of sources to make inferences about future behaviour or make decisions about them.

Solely automated decision-making and profiling could pose risks to the rights and freedoms of workers.

Further reading

- For more information on what we mean by Artificial Intelligence, see the section '[What do you mean by AI?](#)' [↗](#) from our guidance on AI and data protection.
- [What is an AI output or an AI-assisted decision?](#) [↗](#)

What do we need to consider if we are planning to make solely automated decisions with legal or similar effect on workers?

Article 22 of the UK GDPR restricts you from carrying out solely automated decision-making that has legal or similarly significant effects on people.

A legal effect is something that affects someone's legal rights (eg a right to work). Similarly significant effects are more difficult to define, but are likely to include decisions that:

- significantly affect someone's financial circumstance (eg increasing or decreasing a worker's pay based on their performance at work); or
- affect a worker's employment opportunities (eg dismissing someone).

You can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract with the person;
- authorised by law that applies to you (eg if you have a statutory or common law obligation to do something and automated decision-making is the most appropriate way to achieve your purpose); or
- based on a person's explicit consent.

You **must** also ensure that you do not disadvantage workers who ask for human intervention in decision-making compared to those who are subject to automated decision-making.

Example - where Article 22 applies

An organisation pays workers based entirely on automated monitoring of their productivity. This decision is solely automated and has a significant effect, since it affects how much a worker is paid. Therefore, the additional rules under Article 22 apply.

Example – where Article 22 doesn't apply

A courier service uses an automated vehicle tracking device to determine if its workers are making deliveries on time and to the correct address.

A worker is issued a warning about failing to make deliveries on time. The warning was based on

complaints received from customers about not receiving their orders. These complaints were checked by the courier service's HR manager who reviewed the vehicle's tracking device data. This showed that the vehicle only made a small proportion of journeys it was expected to make. The manager also discussed the issue with the worker to ask about the delays and complaints before deciding to issue the warning.

Therefore, additional rules under Article 22 do not apply as the courier service's HR manager took the decision to issue the warning after reviewing the information. This is the case even though the warning was issued on the basis of the information collected by the automated tracking device.

Further reading

- For more on issues encountered in AI decision-making, see our guidance: [How do we ensure fairness in AI?](#) ↗
- For a deeper look at Article 22 in general, see: [What is the impact of Article 22 of the UK GDPR on fairness?](#) ↗
- For further clarification on Article 22 and the use of automated decision-making, see: [What does the UK GDPR say about automated decision-making and profiling?](#) ↗
- For more on the use of a lawful basis and its implementation in AI, see: [How do we ensure lawfulness in AI?](#) ↗
- For more information on consent see our guidance on: [consent](#) ↗.

What should we tell workers about solely automated decision-making?

The right to be informed means you **must** tell workers whose information you are processing that you are doing so for solely automated decision-making. You **must** give them "meaningful information about the logic involved, as well as the significance and the envisaged consequences" of the processing for them. You **must** also tell them about this if they submit a SAR.

You **must**:

- give workers information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision where the processing falls under Article 22; and
- carry out regular checks to make sure your systems are working as intended.

Further reading

- [How do we ensure fairness in AI? ↗](#)
- [How do we ensure lawfulness in AI? ↗](#)
- [How do we ensure individual rights in our AI systems? ↗](#)

What is the role of human oversight?

When you use automated decision-making to make decisions with legal or similarly significant about workers, there is a risk that you might make them without appropriate human oversight. For example, you might reduce a worker's pay if an automated system identifies poor performance. This infringes Article 22 of the UK GDPR. You **should** ensure that people assigned to provide human oversight remain engaged, critical and able to challenge the system's outputs, wherever appropriate.

If you plan to use automated systems as a decision-supporting tool (which will therefore be outside the scope of Article 22), you **should** ensure that the people making the decision are:

- involved in checking the system's recommendation and **should not** just routinely apply the automated recommendation to workers;
- actively involved and not just a token gesture. They **should** have 'meaningful' influence on the decision, including the 'authority and competence' to go against the recommendation; and

'weighing-up' and 'interpreting' the recommendation, considering all available input information, and also taking into account additional factors.

Further reading

- [Rights related to automated decision-making including profiling ↗](#)
- [How do we ensure individual rights relating to solely automated decisions with legal or similar effect? ↗](#)
- [What is the role of human oversight? ↗](#)

Checklist

- If we use the personal information from monitoring workers for automated decision making (including profiling), we have checked that we comply with Article 22.
- We offer alternatives to workers who ask for human intervention in decision making.
- We do not disadvantage workers who ask for human intervention in decision making, compared to those who are subject to automated decision making.
- Where we use automation with human involvement, we ensure the involvement is meaningful.
- We carry out regular checks to make sure the systems are working as intended.

You can also view and print off this checklist and all the checklists of this guidance on our [checklists page](#)



Specific data protection considerations for different ways or methods of monitoring workers

In detail

- [What do we need to consider if we want to monitor workers remotely and when they are working from home?](#)
- [What if commercially available tools are part of our monitoring?](#)
- [Can we monitor telephone calls?](#)
- [Can we monitor emails and messages?](#)
- [Can we use video or audio surveillance to monitor workers?](#)
- [Can we monitor work vehicles?](#)
- [Can we use dashcams to monitor our workers?](#)
- [What if we supply a product or service to another organisation and they ask us to monitor our workers?](#)
- [Can we monitor time and restrict access?](#)
- [What if we are monitoring to prevent data loss or detect malicious traffic?](#)
- [Can we monitor device activity?](#)
- [Checklist](#)

What do we need to consider if we want to monitor workers remotely and when they are working from home?

The rise in remote and home working in recent years has led to an increase in monitoring workers remotely, in particular if they are working from home. This is because employers want to secure their systems and manage remote workers.

If you are monitoring workers remotely, you **should** keep in mind that workers' expectations of privacy are likely to be higher at home than in the workplace. The risks of capturing family and private life information are higher as you can inadvertently capture it. You **should** factor this risk into any type of monitoring of remote workers you intend to implement. You **should** do this as part of a DPIA. This is especially important if you are considering implementing any of the forms of monitoring discussed below.

What if commercially available tools are part of our monitoring?

You may choose commercially available tools or services to provide you with the capability to monitor your workers. For example, you may procure a tool that helps to monitor your workers, gathers information about them or helps to store the information (ie a cloud storage provider).

In most of these cases, you are the controller for this processing activity and the third party is a processor. This is because you are deciding the means and purposes of the processing.

As a controller, your data protection responsibilities state that you **must**:




- comply with the data protection principles;
- ensure that workers and other people who may be captured can exercise their rights regarding their personal information;
- choose an appropriate processor who will provide sufficient guarantees that they will implement appropriate technical and organisational measures to ensure their processing meets data protection requirements; and
- meet accountability obligations, such as carrying out DPIAs and adopting a 'data protection by design and default' approach.

You **must** determine the controller and processor relationships before you begin to process personal information or implement monitoring.

As part of the procurement process, you **must** make sure that the provider gives sufficient information about their tool or service so you can carry out your responsibilities. You **must** do this through a written contract or service agreement between the controller and processor.

In some cases, the third party you are procuring from may use personal information collected by you for their own purposes. In this case, it is likely that the third party would become a controller for this processing.

Further reading

- [Controllers and processors](#) 
- [Contracts and liabilities between controllers and processors](#) 
- [What does it mean if you are a controller?](#) 

Can we monitor telephone calls?

It is not usually proportionate to monitor or record the content of calls in all cases. You **could** monitor business calls if it is necessary to provide evidence of business transactions, or for training or quality control purposes.

Example

A customer service call centre monitors helpline calls for training and quality control purposes. Workers are made aware of this through a policy which is regularly brought to their attention. Customers are informed during calls and are signposted to detailed privacy information.

Example

A finance company is legally required by a regulator's rules to record calls. The company limits recording to strictly what is required by those rules.

You may have a business need to monitor usage, for example to detect calls to numbers you would not routinely expect workers to call. You **could** consider using itemised call records rather than recording call content. If the itemised call record alone is insufficient, you can assess whether you can use it to strictly limit and target any further monitoring. If you decide to change the way you monitor calls as a result of information you gather during call monitoring, you **should** revisit your DPIA and carefully consider the implications of increased levels of monitoring.

Example

A recruitment agency suspects workers are sharing commercial secrets with a competitor. The employer uses itemised call records to narrow down those under suspicion and then uses these records to target any further monitoring accordingly.

You **must** make sure you inform workers of any call monitoring in your privacy information. You **should** also include this in any other relevant internal documents, such as your employment handbook, codes of conduct and guidance. You **should** ensure workers understand the purpose and extent of any monitoring.



You **should not** routinely monitor personal calls. You might want to use information about personal calls for billing or in exceptional circumstances (eg suspected criminal activity). You **should** have a policy for personal calls and make sure workers are aware of this.

Workers base their expectations of privacy on practice as well as policy. So if you tolerate a number of personal calls, you cannot rely on a policy banning them to justify carrying out this type of monitoring.

Don't forget that worker's expectations of privacy are significantly higher at home or outside the workplace. You **should** factor this in to your DPIA.


Monitoring calls also inevitably involves collecting information about people who make calls to, or receive calls from the organisation, as well as about workers themselves. You **must** tell these people that you are recording the call and why. A recorded message is good practice. Where this is not possible, you **must** instruct workers to inform callers that calls may be recorded and to explain the reason why. You can then provide the rest of the privacy information (eg retention periods, individual rights available, and details of any data sharing) by other means. For example, you **could** email the caller a copy of your privacy information or provide a link to it on your website. Any information you collect is likely to be personal information and you **could** disclose it in response to a SAR. You **should** make sure workers know that you may release call recordings to people, if requested.

Further reading

- [Right to be informed](#) 
- [Right of access](#) 

Can we monitor emails and messages?

As an employer you might consider monitoring emails and messages sent to and from work accounts. You may intend to:

- protect corporate information;
- use it for data security (see our [guidance on data loss prevention](#)  for more information);
- identify suspicious activity; or
- enforce any acceptable usage policies you may have.

By messages, we mean instant messages available on some applications and the chat functions in collaboration tools.

You **must** be clear about your purpose for monitoring emails and messages and make sure any monitoring is necessary and proportionate to your purpose. You **must** inform workers of the purpose of any monitoring.

If you are considering monitoring emails and messages, you **must** complete a DPIA. This is because it poses a high risk to workers' data protection rights and freedoms and is likely to capture special category data. You **should** complete a DPIA even where this is not a requirement, as this is good practice. A DPIA helps you to assess risk, plan properly and demonstrate accountability.

It would be difficult to justify monitoring the content of emails and messages if monitoring network data traffic would meet your purpose. You **must** notify workers in advance, such as in relevant policy documents, if you may monitor content in exceptional circumstances. You **must not** access content unless there you have a clear policy in place explaining the circumstances where such monitoring may take place.

Before monitoring emails and messages, you **should** consider the following questions:

- If network data monitoring alone is not sufficient, can you use the network data record to narrow the scope of the monitoring (eg to restrict your checking of email content to those sent to rival organisations)?
- What risk does any monitoring pose to the common law duty of confidence owed to workers or customers?
- Are there any lines of communication that you will not monitor (eg emails from workers to trade union representatives)?
- Have you banned personal use of the system? Even a ban would not entirely justify accessing the content of personal messages. You **should only** investigate workers who breach any ban by looking at network data first rather than content.
- Does your system enable workers to mark emails as personal or private?

Are systems for recording information about emails and messages reliable and accurate?

Can we use video or audio surveillance to monitor workers?

Using CCTV has been common in organisations for many years. However, the quality, technology and possibilities have improved over time. It is possible to accidentally capture special category data through CCTV.

For example, there are CCTV systems which:

- can capture both video and audio;
- use facial recognition; or
- work in conjunction with AI to assess productivity or undertake emotional analysis of the people being recorded.

Remember that when you are planning your monitoring, if you believe that it is likely that you will capture special category data, you **must** carry out a DPIA.

We have covered [call recording](#) above. However, many organisations also have video surveillance with audio capability, or have recording devices available in meeting rooms and many video conferencing apps also have the capability to record audio. Using audio recording, particularly where it is continuous, is considered more privacy intrusive than purely visual recording. You will therefore require a much greater justification if you use it. You **should** switch off by default any capability to record audio. You **should only** use it in exceptional circumstances, for example by a trigger switch. Continuous audio and video recording can be highly intrusive and you are unlikely to be able to justify it in most circumstances.

You **should** target any monitoring at areas of particular risk and confine it to areas where expectations of privacy are low. You are only likely to be justified in using continuous video or audio monitoring of workers in rare circumstances.

If you are considering using video or audio monitoring, you **must**:

- complete a DPIA, as this will help you assess whether the benefits justify the adverse impact;
- consider why this monitoring is necessary for the intended purpose as part of your DPIA;
- make sure you inform workers about the extent and nature of the monitoring, and why you are carrying it out; and
- ensure that you make anyone else caught by the monitoring, such as visitors or customers, aware of its operation and why you are carrying it out.

You **should** also consider the right of access. If a worker or any other person captured by the monitoring makes a SAR, you may need to be able to redact third parties from the footage.

You are unlikely to be able to justify covert monitoring in usual circumstances. (See the section on [covert monitoring](#).)

Using video technology with facial recognition technology comes with higher risks to data protection rights and freedoms than standard video technology. This is particularly the case if you use facial recognition to make inferences about a person's likely behaviour, emotional state or intentions. There are also concerns about the accuracy of facial recognition technologies, particularly for people from ethnic minority groups.

Facial recognition technology uses biometric data. Biometric data is unique to each person, it cannot be changed. Biometric data is special category data if you are using it to identify individual workers. If you are using facial recognition technology as part of your monitoring, then you are using [special category data](#) and **must** have an appropriate lawful basis and condition for processing.

If you are considering using facial recognition technologies, you **must** carry out a DPIA because they present a high risk.

Further reading

- Our [FRT and surveillance checklist](#) will help you identify and address risks around using facial recognition.
- If you are considering using FRT for time and attendance control, read the section on [the use of biometrics for time and attendance control](#).
- If you are using or are considering using dashcams, read the section on [dashcams](#) and read our guidance on [surveillance in vehicles](#).
- [Video surveillance \(including guidance for organisations using CCTV\)](#)
- [Guidance on AI and data protection](#)

Can we monitor work vehicles?

Yes. However, if you allow workers to use the work vehicle for private use, you will rarely be able to justify monitoring during private use

Example

An employer provides workers with company cars which they are allowed for private use. Company cars are tracked during working hours for business reasons. The employer uses a tracking system which the driver can disable so it does not monitor driver activity when they are not working.

You **must** inform workers and passengers of any vehicle monitoring.

Some employers are obligated by law to use tachographs in vehicles to record information about driving time, speed, and distance to ensure the rules on drivers' working hours are followed. In this scenario, you can rely on the lawful basis of legal obligation.

You may be using vehicle telematics (also known as 'black boxes') across your fleet for vehicle insurance policies. These use technology to track and record driver behaviour to calculate insurance premiums. Telematics data which records the activities of drivers is personal information and is subject to data protection law. If your insurer is handling driver information, they also have data protection obligations.

It is harder for you to justify driver monitoring, such as monitoring driver behaviour and driving style, or

using cameras or audio. This is due to the higher risk to worker's privacy and the privacy rights of any passengers. You **must** carry out a DPIA as this type of processing would be considered high risk. You **should** consider whether less intrusive methods could achieve your purpose and document this assessment as part of your DPIA.

If you are considering the use of any monitoring tool which uses analytics to make inferences, predictions, or decisions about drivers, you **must** carry out a DPIA as this presents a high risk.

Further reading

- Read our guidance on [controllers and processors](#)  for further information.

Can we use dashcams to monitor our workers?

Dashcams and other cameras can be an efficient way to protect drivers, passengers and assets, and can help to reduce insurance costs. However, images captured of any identifiable person is personal information and is therefore subject to data protection law.

Dashcams may be intrusive and can impact on the data protection rights and freedoms of workers and other people, especially if you use them in places that people would not reasonably expect. Outward facing cameras or dashcams can capture recordings of other motorists or pedestrians outside of the vehicle. Inward facing systems can capture the driver and any passengers within a vehicle. Dashcams with audio recording capabilities present higher risk, and so you **should** switch off any capability to record audio by default. You **should** only trigger audio recordings in exceptional circumstances.

Example

A taxi has outward and inward facing cameras for the safety of drivers and passengers. This is not continuous. The driver can disable this when they are off duty. The audio feature is switched off by default and only triggered in exceptional circumstances, such as if a passenger behaves in a threatening way.

Further reading

- If as an employer you are using, or considering using, dashcams on your vehicles, you **should** read our guidance on [surveillance in vehicles](#) for more detailed information.

What if we supply a product or service to another organisation and they ask us to monitor our workers?

You cannot justify monitoring workers solely because your customer makes it a condition of business.

As an employer, you **must** still comply with data protection law. You **must** be certain that any monitoring required by a customer is necessary and proportionate, and that you inform workers.



Ultimately the decision about whether the monitoring requested by the customer is appropriate rests with you.

Example

An insurance company wishes to monitor an organisation's workers to ensure they are billing correctly for workers' hours and services. They propose monitoring the workers' computer activity, with reports generated for individual workers. The insurance company would need to justify why this level of monitoring is necessary and consider lower risk alternatives, such as aggregated reports where individual workers are not identifiable.

The employer would need to consider their data protection obligations before the insurance company carried out any monitoring of their workers. If the employer is not confident the monitoring requested by the insurance company meets their obligations under data protection law, they should refuse the monitoring and discuss alternatives with the insurance company.

Further reading

- [Controllers and processors](#) 
- [Contracts and liabilities between controllers and processors](#) 

Can we monitor time and restrict access?

Many employers have measures in place to record and restrict access to work premises and equipment. Uses may include:

- controlling access to buildings or areas of buildings (eg server rooms);
- controlling access to IT and other systems (eg retail cashier systems, or online platforms which connect workers with clients);
- recording who is on site for fire safety purposes; or
- recording attendance for payroll purposes.

These measures can form an important part of your security measures and provide an audit trail. However, they may also pose a risk to workers' data protection rights and freedoms because of the level of knowledge and control they give you over workers' activities and movements.

You **must** be clear about your purpose for recording information about your workers' access and activities. You **must not** use the information for a different purpose unless:

- it is compatible with your original purpose;

- you obtain consent; or
- you have a legal obligation to do so.

Many employers use methods such as pin numbers and swipe cards to control access and record attendance. If you are using, or considering introducing, biometrics to control access, see the section on [biometrics and access and time data](#).

Example

An employer restricts access to a server room to certain workers for security purposes to protect equipment and information. They manage this by a swipe card access control system which records the entrance and exit times of the workers who have the right permissions to enter. This means if equipment is stolen or interfered with, or there is unauthorised access to information, records kept by the system enable them to identify workers who had access at the time.

The employer does not use information about workers' access and exit times for any other purposes (eg for performance evaluation).

Further reading

- [Purpose limitation](#)

What if we are monitoring to prevent data loss or detect malicious traffic?

You are likely to have a number of technical solutions in place to monitor and ensure the confidentiality, availability, and integrity of personal information. These can include solutions such as firewalls to monitor for, or to prevent, external threats, as well as internal monitoring, such as data loss prevention solutions.

You **should** consider the least invasive means possible when selecting solutions to protect against data loss or external threats. You **should** complete a DPIA. This will help you to assess the risk and identify if less intrusive methods might achieve your purpose.

Monitoring network traffic may be high risk, particularly if you carry out analysis of the data to make inferences about workers. (See the section on [automated tools](#).)

As an alternative to more detailed traffic monitoring, you **could** consider blocking suspicious incoming or outgoing traffic or redirecting the worker to a portal where they may ask for a review of the decision to block traffic.

Can we monitor device activity?

Developments in technology have led to an increase in the availability and affordability of monitoring tools with the capability to process large amounts of information. This can be particularly intrusive if workers are

using their own devices.

Some employers use certain tools to record workers' activities on a range of different devices – including those used by workers personally, such as laptops and handheld devices, as well as network devices, such as routers and firewalls.

This section focuses on the monitoring of devices that an employer may consider for:

- tracking workers' activity and productivity;
- ensuring policies and procedures are followed; and
- tracking visits to applications and websites.


This is not an exhaustive list. (See the section [What if we are monitoring to prevent data loss or detect malicious traffic?](#))

Device activity monitoring can include capturing workers':

- web browsing;
- emails and messages;
- documents;
- use of applications;
- screen captures;
- webcam captures; or
- keystroke monitoring (this is classed as behavioural biometric data where a worker is identifiable because of their unique manner and rhythm of typing).

Device activity monitoring is likely to capture excessive amounts of workers' personal information. This could potentially include special category data, such as emails about health conditions and emails to union representatives. You are particularly unlikely to be able to justify capturing webcam shots or footage.

If you are considering capturing the computer or device activity of workers, there are several factors to take into account:


- You **must** be clear about your purpose, and fully document your justification for carrying out device monitoring, including what consideration you gave to using less intrusive means. If you can achieve your aim in a less intrusive way, you **must** do so.
- You **must** identify a lawful basis and, where special category data is involved, identify a condition for processing.
- You **must** carry out a DPIA before undertaking any processing likely to cause high risk to workers' and other people's interests. You **could** use our [screening checklists](#)  and read our detailed DPIA guidance to help you decide if this is likely to be the case.
- Even where not mandated, you **should** carry out a DPIA as the process can assist with your risk assessment and planning.
- You **must** consider discussing the proposed device monitoring with workers or their representatives. A representative sample of workers involved in assessing the necessity of monitoring and the accessibility of any policies around this **should** guide your plans. Involving workers where risks may be high can help to address risks, concerns and help to build trust.

- You **must** inform workers about device monitoring, including how you are using it for making decisions which affect them.
- You **could** consider making aggregated analytics reports. These can identify trends without identifying individual workers.
- You **could** consider banning the private use of work devices and blocking problematic websites. However, remember that even with such a policy in place, it would be difficult to justify accessing a worker's personal communications.

You **should** ensure that when workers are using their own personal devices for work, you are not capturing their private use of their device.

Checklist

- We are clear about our purpose and collect no more personal information than we need to achieve it.
- We have carried out a DPIA that fully addresses our monitoring of emails and messages. It fully explores any impact on the rights and freedoms of workers and other individuals whose personal information may be captured by the monitoring.
- We distinguish between network data and content. We only access content in exceptional circumstances and we notify workers in advance.
- We have identified a lawful basis and a special category condition where appropriate.
- Where required, we have an Appropriate Policy Document in place.
- We have an acceptable usage policy in place, and we regularly bring this to workers' attention.
- We have informed workers of the nature, extent, and justification for any monitoring.
- We have a retention policy in place. We regularly bring this to the attention of workers, who know what to do with messages that need to be retained for business reasons.

You can also view and print off this checklist and all the checklists of this guidance on our [checklists page](#) .

Can we use biometric data for time and attendance control and monitoring?

In detail

- [What is biometric data?](#)
- [When might we use biometric data for time and attendance control and monitoring?](#)
- [What are access controls?](#)
- [How do we determine if using biometric data for access control is necessary and proportionate?](#)
- [What lawful basis and condition for processing can we rely on when using biometric data?](#)
- [Do we need to carry out a data protection impact assessment \(DPIA\)?](#)
- [What about accuracy, fairness and rights relating to automated decision-making?](#)
- [What do we need to tell workers about biometric data and access controls?](#)
- [Can workers object to the use of biometric data for access control?](#)
- [What about the security of biometric data?](#)
- [Checklist](#)

What is biometric data?

The UK GDPR defines biometric data as:



“Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person such as facial images or dactyloscopic [fingerprint] data.”

Biometric data is personal information that's unique to someone. It relates to their behaviour or biology, and is obtained using technology.

Biometric data includes:

- fingerprints;
- iris scanning;
- retinal analysis;
- facial recognition templates; and
- voice recognition templates.

Biometric data is unique in data protection law as its status can change depending on the purpose you use it for. When your purpose is unique identification (eg access control or timekeeping) further safeguards are

required. If you use biometric data to identify a specific person then it becomes [special category data](#).

When might we use biometric data for time and attendance control and monitoring?

Controlling and monitoring access for security or time recording is nothing new. Using swipe cards, PIN codes and passwords to control workers' access to buildings and IT systems is common.

However, the technologies and systems that are used to identify workers and enable access have developed, with biometric data increasingly part of the picture. Processing biometric data (eg using a worker's fingerprint) can be a convenient way to give workers access to their workplace. However, it does pose a risk to workers' data protection rights and freedoms. It can also undermine trust between workers and employers. Therefore you **should** consider whether there are any alternatives to using biometric data, in order to achieve your desired objectives.

The nature of biometric data means that it is more closely identified with a specific person. As such, the risks of harm in the event of inaccuracies or a security breach are much greater - as it is more difficult to rectify if inaccurate, and you cannot replace it in the event of a breach (unlike, for example, being able to reset a password). Therefore, you **must** consider whether you need extra security measures when collecting, using and storing biometric data.

What are access controls?

Access controls are for unique identification, where you process the information to identify specific people and then grant them access to specific resources during work time. This applies to both physical resources (eg access to a specific work area) and electronic resources (eg access to a specific piece of software).

You may also use information from access controls to record working hours.

Further reading

- For further information see our [guidance on biometric data](#).

How do we determine if using biometric data for access control is necessary and proportionate?

Start by following the steps you would take when you are deciding whether to introduce any other new monitoring technology, as set out above.

You **should** document your reasons for choosing to rely on biometric data, including any consideration of other less intrusive means and why you think they are inadequate. Remember, biometric methods of identification contain much larger amounts of sensitive information than methods such as swipe cards. You **should** be clear about your purpose and why using biometric data is necessary. If a reasonable alternative option to using biometric data is possible, you **should** be able to justify why you don't use this method. You **must** document all of this in your DPIA.

What lawful basis and condition for processing can we rely on when using biometric data?

Your lawful basis depends on your purpose for using biometric data to identify workers and the reason for your access control measures. (See the section on [lawful bases](#).)

If you use biometric data to uniquely identify someone, it is classed as special category data. So, if you are using biometric data for access control to identify workers, you **must** also identify a condition for processing. (See the section [What if our monitoring involves special category data?](#))

If you are relying on biometric data for workspace access, you **should** provide an alternative for those who do not want to use biometric access controls, such as swipe cards or pin numbers. You should not disadvantage workers who choose to use an alternative method. It is likely to be very hard to justify using biometric data for access control without providing an alternative for those who wish to opt out.

If you provide an alternative method for those who wish to opt out of the use of biometric data, and your workers are not disadvantaged for opting out, consent is the most likely lawful basis to apply to the use of biometric data for access control.

However, if there is no non-biometric alternative, then the consent basis will not be appropriate.

Remember that there are other lawful bases that you may be able to rely upon, if you can justify their use. Whichever basis and condition for processing you decide to use, you **must** document your reasons carefully in your DPIA.

Example

An employer introduces an electronic fingerprint scanning system for time and access control. Workers scan their fingerprint in order to access their workplace. The employer also uses the personal information for payroll purposes. Having carefully considered the available options during the DPIA process, the employer decides consent is the most appropriate lawful basis for their processing. This system uses biometric data to identify individual workers so the employer needs a valid condition for processing special category data in addition to a lawful basis.

The employer offers a swipe card option with no detriment to workers who do not wish to have their fingerprints scanned. This means the employer can consider relying on the explicit consent condition for processing the special category biometric data. This is because workers can give their consent freely and have the option to use a swipe card if they change their mind.

Example

An employer rolls out new laptops to all workers. The devices have the option of facial recognition sign in. Staff who have tested the system find the facial recognition feature very useful. The employer decides to use consent as their lawful basis.

Workers who agree to using facial recognition provide explicit consent on the understanding that the image created is only held on the device provided to them and is not stored elsewhere or used for any other purpose than device access. Workers who do not wish to use facial recognition to log on may use a password or a PIN instead. The facial recognition process does not initiate on the laptops of workers who have not given consent.

Do we need to carry out a data protection impact assessment?

Yes, you **must** carry out a DPIA whenever you intend to process biometric data to uniquely identify a worker. This is because processing biometric data is considered high risk. You **must** complete your DPIA before starting the processing. This will assist you in assessing and documenting risk and putting measures in place to reduce any identified risks. The DPIA process also allows you to discuss the proposed use of biometrics with workers and their representatives before you introduce it.

(See the section [Do we need to do a data protection impact assessment \(DPIA\) before we start monitoring?](#) )

What about accuracy, fairness and rights relating to automated decision making?

Any inaccuracies in biometric data that allow workers to access work or to pay them correctly are likely to have a detrimental impact on workers. When deciding whether to implement a new system, you **should** think carefully about the accuracy of the system and its ability to correctly identify people. As a data controller, it is your responsibility to ensure personal information stored on your system is accurate regardless of whether you have engaged another organisation to provide the system. You **should** make sure systems are in place to quickly correct any inaccurate information so it does not negatively impact workers.

There is a risk that facial recognition works with less precision for some demographic groups. To comply with the fairness principle, you **must** assess and mitigate the bias in your system. If you have engaged another organisation to provide the system, you **should** check it is suitable for the groups and people whose information it will capture. If the system you use results in processing which causes bias or discrimination, you are likely to breach the fairness principle.

Accuracy is linked to workers' rights about automated decision-making and profiling. If monitoring workers relies on authentication by solely automated decision-making, there is a risk that workers are incorrectly identified or not identified at all. You **must** ensure that manual reviews are therefore available if an automatic process has resulted in a possible access denial. You **must** give workers the option to ask for a review if they are unhappy with a decision made by solely automated processing. You **should** quickly identify issues with workers accessing systems or buildings and give back access to workers as soon as possible. You **should not** disadvantage workers who request manual reviews.

Example

Access to a building is controlled by facial recognition. A worker with full access permissions stands in

front of the camera but the door fails to open as the system has not recognised them. This means the worker cannot start work.

To mitigate this risk, the employer has also installed an intercom so the worker can quickly call a supervisor who can grant them entry and manually enter the time they arrived into the system.

If an alternative had not been in place, the worker could potentially have suffered negative consequences, such as loss of pay or disciplinary action. The intervention by the supervisor means that the worker experiences a minor inconvenience rather than a significant detriment as a result of the facial recognition access control system.

Further reading

- See also our guidance on video [surveillance](#).
- [How do we ensure fairness in AI?](#) [↗](#)

What do we need to tell workers about biometric data and access controls?

You **must** tell workers:

- how the system works;
- what personal information you are collecting;
- how you will use their information; and
- the nature and purposes of the monitoring.

You **must** inform your workers through your privacy information. You **could** also provide information on posters or during staff meetings. (See the section [What must we tell our workers about our monitoring?](#) [↗](#))

Further reading

- [Right to be informed](#) [↗](#)

Can workers object to the use of biometric data for access control?

A worker can object to the use of biometric data for time and attendance related purposes, if the lawful basis you are relying on is:

- public task (for the performance of a task carried out in the public interest);
- public task (for the exercise of official authority vested in you); or
- legitimate interests.

If you have used consent as your lawful basis, workers can withdraw their consent. If they do this, you **should** provide them with an alternative method of access, and make sure that this doesn't cause them

detriment.

Further reading

- See the section [Can workers object to being monitored?](#) and our guidance on [the right to object](#).

What about the security of biometric data?

You **must** have security measures in place which are appropriate to the risks of unauthorised access or disclosure of your workers' biometric data. Unlike a password or a phone number, biometric data is more permanent and can't be changed, in most cases. This makes the consequence of a breach more serious. You **should** consider whether you need to store a copy of the underlying image or whether it is sufficient to store the biometric template. In either case, you **should** consider security measures (eg encryption) and organisational measures (eg access restrictions).

If you are storing biometric templates, you **must** ensure that:

- you don't hold them for longer than is necessary;
- they remain accurate and you refresh them as often as considered necessary;
- you store them in a way which does not allow for reverse engineering into the original image or identity (ie the biometric templates are encrypted); and
- you don't store the biometric templates alongside other associated images or lists.


Further reading

- [Security](#)
- [Data protection by design and default](#)

Checklist

- We have documented our evidence base for relying on biometric data, including our consideration of why we are not using less intrusive means.
- We have identified a lawful basis and a special category condition where necessary.
- We have carried out a DPIA.
- We have discussed the proposed monitoring with workers during our DPIA.
- Where consent is relied on, we have put in place alternative methods for authentication or identification for workers who have not given their consent to the processing of their personal information.

- We have made manual reviews available for any workers having issues with access denial due to automatic errors.
- We have considered whether further security measures are required when processing biometric data.
- We have considered accuracy and fairness. We have mitigated any identified risks.
- We have considered the rights of individuals relating to automated decision-making.
- We have informed workers about the use of their biometric data for access control.
- We have considered workers' rights to object to the use of biometric data for access control.
- We have ensured there are appropriate organisational and technological measures to protect the security of any biometric data we process.

You can also view and print off this checklist and all the checklists of this guidance on our [checklists page](#) .

Checklists

These checklists provide an overview and quick guide to help you think about what you need to consider whenever you want to monitor your workers. Read the guidance if you want a fuller explanation and understanding of the issues.

These checklists are concerned with your data protection considerations only. They don't cover other separate legal obligations you may have as an employer, such as health and safety. You will need to obtain separate legal advice for any other such legal obligations.

Please note that these checklists are the same as the checklists at the bottom of each page of this guidance. We have presented them here to allow you to download them together.

Data protection and monitoring workers

- We have checked that the monitoring of workers is necessary for the purpose we have identified. We are satisfied there is no other reasonable and less intrusive way to achieve that purpose.
- We have considered whether we need to do a DPIA and either completed one or documented the reason we considered one wasn't required. -
- When making our DPIA decision, we have considered seeking the views of workers and representatives and either done this or documented our decision not to.
- We have identified a lawful basis for monitoring workers.
- Where required, we have identified an appropriate special category condition for monitoring workers if we're likely to capture any special category data as part of our monitoring.
- We have documented what personal information we are processing when we monitor workers.
- Where required, we have an appropriate policy document in place.
- We have included specific information about monitoring workers in our privacy information so that workers are aware of any monitoring taking place. We have made sure that this information is readily accessible to workers.
- We have considered whether the risks associated with monitoring workers affects our other obligations around data minimisation, security, and appointing Data Protection Officers (DPOs) and representatives.
- We have considered data protection issues as part of the design and implementation of monitoring systems and practices, including where we use external suppliers for monitoring technology, and where we use the functionalities built into communication and collaboration work tools.
- Where necessary, we have considered the rules for international transfers.

What do we need to do if we use monitoring tools that use solely automated processes?

- If we use the personal information from monitoring workers for automated decision making (including profiling), we have checked that we comply with Article 22.
- We offer alternatives to workers who ask for human intervention in decision making.
- We do not disadvantage workers who ask for human intervention in decision making, compared to those who are subject to automated decision making.
- Where we use automation with human involvement, we ensure the involvement is meaningful.

- We carry out regular checks to make sure the systems are working as intended.

Specific data protection considerations for different ways or methods of monitoring workers

- We are clear about our purpose and collect no more personal information than we need to achieve it.
- We have carried out a DPIA that fully addresses our monitoring of emails and messages. It fully explores any impact on the rights and freedoms of workers and other individuals whose personal information may be captured by the monitoring.
- We distinguish between network data and content. We only access content in exceptional circumstances and we notify workers in advance.
- We have identified a lawful basis and a special category condition where appropriate.
- Where required, we have an Appropriate Policy Document in place.
- We have an acceptable usage policy in place, and we regularly bring this to workers' attention.
- We have informed workers of the nature, extent, and justification for any monitoring.
- We have a retention policy in place. We regularly bring this to the attention of workers, who know what to do with messages that need to be retained for business reasons.

Can we use biometric data for time and attendance control and monitoring?

- We have documented our evidence base for relying on biometric data, including our consideration of why we are not using less intrusive means.
- We have identified a lawful basis and a special category condition where necessary.
- We have carried out a DPIA.
- We have discussed the proposed monitoring with workers during our DPIA.
- Where consent is relied on, we have put in place alternative methods for authentication or identification for workers who have not given their consent to the processing of their personal information.
- We have made manual reviews available for any workers having issues with access denial due to

automatic errors.

- We have considered whether further security measures are required when processing biometric data.
- We have considered accuracy and fairness. We have mitigated any identified risks.
- We have considered the rights of individuals relating to automated decision-making.
- We have informed workers about the use of their biometric data for access control.
- We have considered workers' rights to object to the use of biometric data for access control.
- We have ensured there are appropriate organisational and technological measures to protect the security of any biometric data we process.