Employment practices: monitoring at work draft guidance

12 October 2022

ico.
Information Commissioner's Office

Contents

About this guidance

This guidance discusses monitoring at work and data protection. It is primarily aimed at employers. The first part of this guidance explains your legal obligations if your organisation is considering or is already carrying out monitoring of workers. The second part addresses specific kinds of monitoring.

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.

This guidance provides clarity and practical advice to help employers who are monitoring workers to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The UK GDPR and the DPA 2018 do not prevent an employer from monitoring workers, but they must do any monitoring in a way which is compliant with data protection legislation. Public authorities and all bodies performing public functions should also consider the right to respect for a private and family life enshrined in Article 8 of the Human Rights Act 1998. 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 family and private life information are higher.

At a glance

- The UK GDPR and the DPA 2018 do not prevent monitoring. They set out a framework for the collection and use of personal data. You must balance the level of intrusion against the needs of the employer, workers and members of the public.
- Employers must make workers aware of the nature, extent and reasons for the monitoring unless exceptional circumstances mean that covert monitoring is necessary.
- Employers must be clear about their purpose for monitoring. They must not use the information collected for a new purpose unless it is compatible with the original purpose in most circumstances.
- Employers must carry out a data protection impact assessment (DPIA) for any monitoring that is likely to result in a high risk to the rights of workers and other people captured by the monitoring. Employers should keep this under review. Where a DPIA is not mandatory, employers should consider completing one anyway for good practice. The process helps you to make risk-based decisions and to meet your data protection obligations.

In detail

What do we mean by monitoring at work?

Workers largely recognise that employers carry out checks on the quality and the quantity of their work. Employers may also monitor workers to protect health and safety, or to meet regulatory obligations (for example, 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.

Sometimes monitoring goes beyond simply one person watching another. For example, you may record or automatically process personal data. You may also monitor calls or cameras. To comply with data protection law, you need to do this monitoring in a way that is lawful and fair to workers.

If excessive, monitoring has 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. It is not always easy to distinguish between workplace and private information, especially when workplaces are often homes too. 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. We cover this in our sections on special category data and monitoring emails and messages.

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.

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.

This list is not exhaustive. The purposes and technologies that employers use to monitor their workers have changed rapidly over time and will undoubtedly continue to evolve in sophistication. But the principles and rules of data protection remain a constant, which employers need to follow regardless of other developments.

Who is this guidance for?

This guidance is aimed at all organisations, both public and private sector that have employees, workers, contractors or volunteers. We use the term 'worker' throughout this guidance 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, regardless of the nature of the contract.

This guidance is not relevant to people recording information in a personal or household context unless there is professional or commercial activity. For example, the UK GDPR and this guidance covers using CCTV at home to monitor a nanny. It is also important to note that homeworking does not constitute personal or household processing, and so is also covered by this guidance.

This guidance is not relevant for law enforcement authorities who monitor workers for ongoing criminal investigations. These are subject to the separate law enforcement processing regime in Part 3 of the DPA. It is relevant to the Part 2 of the UK GDPR (non-law enforcement) processing carried out by such authorities. By this, we mean any monitoring carried out which is not for law enforcement purposes. For more information on which regime applies to you, see our guidance on which regime to use.

How do we lawfully monitor workers?

In detail

Can we monitor workers?

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

Any decision to monitor workers should involve a careful balancing between the business interests of an employer and the workforce's rights and freedoms in relation to their personal data.

If monitoring is done in a way which is unfair, this negatively impacts the trust between you and your workers. It also has an impact on their rights and freedoms under data protection. 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, the company rolls out device monitoring. This allows senior management to access automatic webcam pictures and check if workers are at work. This is likely to infringe data protection law.

They could achieve the same purpose by checking worker log-on times, giving 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 specific lawful basis. There are six to choose from. Monitoring workers often includes capturing sensitive data. This is called special category data in the UK GDPR. We define this later in the guidance. Because of the sensitivity, it requires extra protection. You must therefore identify a special category processing condition as well as a lawful basis. We explain this in our 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 must consider all the legal implications of any other relevant law.

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 special category condition.

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 should think about why you want to monitor

workers and consider which lawful basis best fits the circumstances. We have listed the 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 in identifying 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. There is no hierarchy in the order of the list in the UK GDPR. That said, some are likely to be more appropriate than others for employers and where we can we highlight this below.

Please also see our separate lawful basis guidance for more general information about the different bases available.

Sometimes, more than one basis applies. You should identify and document all of them from the start. Take care to try and get it right first time, as you should not swap later without good reason.

The six lawful bases are:

(a) 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. Workers must have the option to withdraw their consent without detriment. This should be as easy as when they first provided it. You also need to demonstrate how you managed this process of consent, most likely through record-keeping.

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

(b) Contract: the monitoring is necessary for a 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 it is the only way for an employer to fulfil their side of a contract, it is hard to envisage.

Monitoring is more often for internal business improvement purposes. It is likely that another lawful basis is more suitable for the monitoring of workers.

(c) 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. 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' hours. In this circumstance, legal obligation is appropriate. The logistics company documents the decision to rely on this lawful basis and signposts to the rules which apply. The company does not process more data than necessary to fulfil obligations under the rules on drivers' hours. They also do not use the data for any other purposes.

(d) Vital interests: the processing is necessary to protect someone's life.

This is for emergencies, where you need to process personal data to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions. The task or function must have a clear basis in law. 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.

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, then this basis may be appropriate. You should assess the specific monitoring activity in relation to the basis in law. You cannot rely on this basis if there is a less intrusive way to achieve the same purpose.

If monitoring is separate from your tasks as a public authority, then you should consider an alternative lawful basis.

(f) 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. If you can reasonably achieve the same result in a less intrusive way, legitimate interests does not apply.

You should avoid using legitimate interests if you are monitoring in ways workers do not understand and would not reasonably expect, or if it is likely some workers would object if you explained it to them. The 'consulting workers' stage of the DPIA process may help you to assess this. Read our section on DPIAs for more information.

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 must assess each of the tests prior to processing and document the outcome so you can demonstrate that legitimate interests applies. You can do this by carrying out a legitimate interests assessment.

What if our monitoring involves special category data?

Special category data is personal data revealing or concerning information about:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where used for identification 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. For more information, read our core guidance on special category data. As well as identifying a lawful basis for monitoring workers, if you are capturing any of these types of data, you need to choose a special category condition.

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

If the planned monitoring captures this kind of data, 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 makes it likely (eg where monitoring may identify emails between a worker and a healthcare provider or a trade union rep). If this is the case, you should identify a condition to cover this.

When choosing a special category data condition, think about your purpose for monitoring, as this helps you identify the most appropriate condition. You must demonstrate that your purpose for monitoring outweighs the risk of inadvertently capturing special category data and the condition you choose should reflect this. Carrying out a data protection impact assessment (DPIA) helps you do both of these things. Read our section on DPIAs and our core DPIA guidance for further information about this.

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. 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 may wish to document a condition just in case, to minimise risks. However, you are not obliged to.

There are 10 conditions for processing special category data to choose from. 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 for more detail. You should also carry out a data protection impact assessment (DPIA) before you begin.

Below we discuss some of the special category conditions which may be relevant in a monitoring workers' context.

(a) Explicit consent

You may only rely on this condition if workers have control and choice over the monitoring. Explicit consent follows the same standard as lawful basis consent. Workers must affirm it in a clear statement (whether written or oral). To rely on this condition, workers must 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 carried out a DPIA and established the necessity and proportionality of this method. They offer a feasible alternative (PIN codes) to workers who withhold explicit consent. This does not negatively impact those workers.

The most likely conditions relevant to monitoring workers' context are:

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

This condition may be relevant where 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 need to identify the legal obligation or right in question, either by reference 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 can refer to a government website or to industry guidance that explains generally applicable employment obligations or rights.

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

Read our guidance on information about workers' health for more information about relying on this condition if you are collecting health data about workers. We will shortly be publishing draft guidance on this topic.

(g) Reasons of substantial public interest (with a basis in law)

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

This condition is often relevant for public authorities. It could be relevant for those with commercial, charitable or private interests. However, this only applies if you can demonstrate the wider substantial public benefit and basis in law and can identify a relevant substantial public interest condition.

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set

out in Part 2 of Schedule 1 of the DPA 2018. See our guidance on the substantial public interest conditions for more details.

Example

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

Further reading – ICO guidance

Special category data

What about criminal offence data?

Similar to special category data, the UK GDPR gives extra protection to the personal data of offenders or suspected offenders in the context of criminal activity, allegations, investigations or proceedings. If you are monitoring workers to detect criminal activity, you must identify a specific condition for processing in schedule 1 of the DPA 2018. For more information see our guidance on criminal offence data.

Are there other laws we should consider?

This guidance aims to help you comply with data protection obligations when monitoring workers. Other laws are relevant and we have listed examples below.

Human Rights Act 1998

The right to respect for private and family life is set out in Article 8 of the European Convention on Human Rights, incorporated into UK law through the Human Rights Act 1998. Workers are entitled to a reasonable expectation of privacy. This protects workers' privacy at work, balanced against business interests.

Equalities legislation

In England, Wales and Scotland, the Equality Act 2010 applies to a range of organisations, including:

- government departments;
- service providers;
- employers;

- education providers;
- transport providers;
- associations;
- membership bodies; and
- providers of public functions.

In Northern Ireland, public authorities have obligations under Section 75 of the Northern Ireland Act to ensure that equality of opportunity and good relations are central to policy making.

These laws are relevant as monitoring which does not comply with them is likely to infringe the 'fairness' principle of the UK GDPR.

Where monitoring is used to make decisions about workers, you need to ensure this does not result in discrimination.

Example

If you have an example, case study or scenario that you think would fit in this box, please send it to employmentguidance@ico.org.uk

Investigatory powers regulations

The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-Keeping Purposes) Regulations 2018 provide the legal basis under which an organisation may intercept communications for monitoring or record keeping purposes that are transmitted by a telecommunications system they control. Similar provisions are set out in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. These regulations authorise certain interceptions. Our guidance is in line with the provisions set out in these regulations.

This guidance is not intended to address covert surveillance activities carried out by public authorities governed by the Regulation of Investigatory Powers Act 2000 (RIPA), the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) and the Regulations of Investigatory Powers Act 2000 (Amendment) Order (Northern Ireland) 2002. This type of recording is covert and directed at a specific individual or individuals.

Further reading

- 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

What about fairness?

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.

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. The employer decides to install CCTV to monitor the door outside the changing room, to narrow the scope of any investigation of further thefts and to 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 door 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 worker performance. 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 inaccurate and unfair.

What about transparency?

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. You must tell workers about monitoring in a way that is accessible and easy to understand. Workers have the right to be informed about the collection and use of their information. We cover this in more detail in our section about privacy information.

Apart from in very exceptional circumstances where covert monitoring is justified, you must inform workers about any monitoring. Read our section on covert monitoring for more detail about this.

What about 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.

Make sure overall responsibility for monitoring workers rests at the highest senior management level. If you have a data protection officer (DPO), make sure they are closely involved in any plans to monitor workers.

Our accountability framework is a flexible tool to help you to plan and show your compliance.

Further reading – ICO guidance

Accountability and governance

Accountability Framework

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 consult workers on your monitoring plans. This helps to shape your plans and to build trust with workers. 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 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 can use our screening checklists and read our detailed DPIA guidance to help you decide.

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

Further reading – ICO guidance

Data protection impact assessments

In detail – Data protection Impact Assessments

Data Protection Officers

It is good practice to carry out a DPIA even if there is no specific high risk. It is a flexible and scalable tool which assists your decision making. You should document any decision to proceed without carrying out a DPIA.

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 – ICO guidance

How do we do a DPIA?

Do we have to define our purpose for monitoring workers?

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

You should only change your purpose for monitoring if your new purpose is:

- compatible with your original purpose;
- related to a clear legal provision allowing the processing in the public interest;
- clearly in the worker's interest to do so; or
- related to activity that no employer could reasonably ignore.

The types of activity an employer could not reasonably ignore might include criminal activity at work, gross misconduct and health and safety breaches which jeopardise workers.

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. You should consider that workers base their expectations of privacy not only on policy but also on practice. 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.

Example

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

Systems can be set 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.

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

Yes. The data minimisation principle means you should not collect more data 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 is 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 worker monitoring regularly to prevent this. Similarly, you must not collect more 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 workspace 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 – ICO guidance

Guide to the UK GDPR – data minimisation

What about accuracy?

You should:

- take all reasonable steps to ensure the personal data you gather through monitoring workers is not incorrect or misleading as to any matter of fact; and
- provide workers with the opportunity to comment on the accuracy of any data gathered through monitoring. This particularly applies if the employer is using the data to make potentially adverse decisions about them, for example if they use monitoring data in performance reviews. Workers have the right to request that inaccurate data is corrected.

You should consider:

- Equipment or systems malfunction can cause information collected through monitoring to be misleading or inaccurate, for example 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.

Ensure that within or alongside disciplinary or grievance procedures and performance reviews or appraisals workers can see and, if necessary, explain or challenge the results of any monitoring.

Further reading – ICO guidance

Guide to the UK GDPR – accuracy

Guide to the UK GDPR – right to rectification

How long should we keep monitoring data?

You should not keep monitoring data for any longer than you need it. You should not keep any data gathered from monitoring workers for longer than is necessary for your particular purpose or purposes. You must 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 monitoring data just in case you find a purpose for it in the future. You should ensure you have a retention schedule in place and delete any monitoring data in line with your schedule. The UK GDPR does not specify retention periods, so you must justify why you need to keep the data.

Further reading – ICO guidance

Storage limitation

What about security?

Security is a key principle of the UK GDPR. You must have appropriate organisational and technical measures in place to protect any data collected 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 data to only those who need access. Take care to identify the most appropriate person or people to access the data collected. Ensure they are properly trained to handle monitoring information.

Sometimes another organisation processes monitoring data on your behalf, for example if you are using a third party. As a controller, you are responsible for compliance. This includes what the third party (the processor) does with the data.

The UK GDPR's security requirements also apply to any processor you use. See our section on third parties for more information. Similarly, if you are using commercially available monitoring tools, or the monitoring functionalities which are available on communication and collaboration tools, you still need to consider security and access to any data from the monitoring. You should not assume the tool has the appropriate level of protection built in. Read the section on commercially available tools for more information.

What should we tell workers about our monitoring?

You must make sure workers understand what data is being processed during monitoring. You also need to consider how and why you are going to use their personal data. You could set up a system to ensure workers remain aware that monitoring is being conducted. For example, via an intranet, or through signage in areas subject to video monitoring. You could seek assurance by collecting documentary proof when a worker has read any notices. You must regularly review any monitoring to ensure privacy information is kept up to date. Make sure you tell workers when changes are introduced.

Workers experiencing uncertainty as to whether they are being monitored, or the reason for the monitoring risks a chilling effect on the trust between workers and employers. This could have a negative impact on your business as well as infringing the data protection rights and freedoms of workers. Making sure workers understand any monitoring builds trust and ensures compliance with the right to be informed.

For a comprehensive list of information that should be provided, see our detailed guidance on the right to be informed.

Do we need to consult workers?

If you are planning to introduce monitoring, you should seek and document the views of workers or their representatives 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. Addressing any feedback or questions in advance helps to build good employment relationships and helps you to meet your obligations to protect workers' data protection rights and freedoms. Involving workers during the planning stages provides an opportunity to consider concerns early. This can potentially avoid complaints from workers if the monitoring is rolled out without telling them what they might reasonably expect or considering their potential concerns. You may do this as part of your DPIA. For more detail see our DPIA guidance on consulting individuals, our section on the right to object and our core guidance on the right to object.

Example

If you have an example, case study or scenario that you think would fit in this box, please send it to employmentguidance@ico.org.uk

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 would need to consider it as an option in most usual circumstances. There may, however, be exceptional circumstances where you would consider this. An example is where covert monitoring is necessary to enable the prevention or detection of suspected criminal activity or gross misconduct.

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

If you are considering monitoring workers covertly:

- This should only be authorised by the highest authority in your workplace.
- You must carry out a DPIA.
- You must 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.
- The covert monitoring must be strictly targeted at obtaining evidence within a set timeframe which should be limited to the shortest time possible.
- The covert monitoring must not continue after the investigation is complete.
- You must not use covert audio or video monitoring in areas where workers would reasonably expect to be private, such as toilets or changing rooms.
- You must 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 ensure there is a contract in place that requires them to only collect information in a way that satisfies your obligations under data protection legislation. See our guidance on controllers and processors for further detail.
- You must only use information gathering through covert monitoring for the purpose intended. Disregard and destroy any other information unless it reveals something that no employer could reasonably be expected to ignore where there is no other way to achieve this purpose.
- Limit the number of people involved in the investigation to only those who really need to be involved.
- Set clear rules limiting disclosure and access to the information collected.
- Remember workers' individual rights. For example, if a worker submits an access request, you may have to disclose the monitoring information. There are some exemptions, but these are not blanket. Requests must be dealt with on a case-by-case basis. Read our guidance on individual rights and subject access requests for further details.

What about workers' right of access to their data?

The data collected through monitoring must be made available to workers if they make a subject access request unless an exemption applies. Technical means which gather large amounts of data, camera footage, and information containing the personal data of third parties could make this a challenge, especially if the systems used do not store information in a way that makes personal data readily retrievable. You should factor this into your planning or your DPIA, or both. For further detail, read our core Right of Access guidance. We will be publishing Employment Right of Access FAQs in due course.

Further reading – ICO guidance

Right of access

Can workers object to being monitored?

Yes, although this right is not absolute. 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 data through monitoring. The reasons should be based upon their particular situation.

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.

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 need to balance the worker's interests, rights and freedoms with your own legitimate interests. It is your responsibility to demonstrate that your legitimate grounds override those of the worker.

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

Undertaking your UK GDPR obligations before proceeding with any monitoring reduces the chances of workers raising objections. Carrying out a DPIA helps you to do this, particularly the 'consulting workers' stage. You must complete a DPIA where monitoring creates a high risk to worker's data protection rights and freedoms.

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

- manifestly unfounded; or
- excessive.

Example

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

In order to decide if a request is manifestly unfounded or excessive you must consider each request on a case-by-case basis. You should not have a blanket policy.

You must be able to demonstrate to the worker why you consider the request is manifestly unfounded or excessive and, if asked, explain your reasons to the ICO.

Further reading – ICO guidance

For more detail on what we mean by manifestly unfounded, see our core guidance on 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 your organisation uses a third-party to monitor workers or to process the data from monitoring workers, then that third party also has obligations under the UK GDPR. If you are using such a provider, and you as the employer determines the purposes and the manner of the processing, then it is likely the provider will be considered a processor under the UK GDPR, with your organisation being the controller. If the processor determines any purposes for the information, they may also be considered a controller.

As controller, you are ultimately responsible for the compliance of your processors as well as your own compliance. You are responsible for assessing

your processor is competent to process the personal data in line with the UK GDPR's requirements. You must ensure there is a UK GDPR compliant contract in place so both parties understand their responsibilities and liabilities. Putting in place a data sharing agreement will actively help both parties to understand the obligations and requirements. In the event of a UK GDPR infringement, you will not be liable if you can prove you are not in any way responsible for the infringement.

Example

A UK company outsources HR operations to a third-party service provider. The provider processes data about the UK company's workers. The provider is a processor. The UK company must ensure the provider is compliant.

You are responsible for data protection compliance if you are using a monitoring software package or gathering data from communication and collaboration tools or using an analytics application to conduct monitoring or to process data from monitoring workers. You must ensure the system or application is compliant with data protection law, and that any necessary contracts are in place, not your supplier.

Further reading – ICO guidance

Controllers and processors

What about international transfers?

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

The rules for international transfers apply if:

- you are agreeing to send personal data, 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 individual. This includes transfers to another company within the same corporate group.

However, if you are sending personal data 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 data outside your company or organisation.

Example

A UK company uses a centralised 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 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' data 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.

If you are sending monitoring data about workers overseas, you should read our core guidance about international transfers to find out more about adequacy regulations, appropriate safeguards and exceptions.

If you use a processor based outside the UK, the rules on international transfers apply. The UK GDPR restricts the transfer of personal data to countries outside the UK or to international organisations. Read our section on international transfers and our core international transfers guidance.

Example

A UK company uses a USA based application to monitor workers. The application provider hosts the data in the USA and is a processor. This counts as a restricted transfer, 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.

Further reading – ICO guidance

International transfers

International data transfer agreement and guidance

What about automated processes in monitoring tools?

At a glance

Monitoring tools have become increasingly sophisticated, with automated processes (sometimes known as 'people analytics') often used for data security purposes, managing performance, monitoring absence (including sickness and where a worker is away from their workstation). There are business benefits to people analytics. They can contribute to improving organisational performance and can demonstrate the impact of HR policies. Such tools have the capacity to collect and process large amounts of workers' data via monitoring in real time, which is then used to make predictions, inferences and decisions about workers on both an individual and a collective level. The UK GDPR has provisions on automated decision making and profiling. We cover them here in the context of monitoring workers.

In detail

What do we mean by automated decision making and profiling?

Automated decision making is a decision made by automated means without human involvement. Automated decision making often involves profiling too. This is where employers use worker's data from a number of sources in order to predict behaviour or make decisions about them.

Automated decision making and profiling pose risks to the data protection rights and freedoms of workers if used irresponsibly. Risks can include inaccuracy and discrimination.

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

The UK GDPR has rules (under Article 22) to protect workers if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

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

- necessary for the entry into or performance of a contract;
- authorised by law that applies to you 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 the individual's explicit consent. The UK GDPR says that consent must be a freely given, specific, informed and unambiguous affirmative indication. This is the most likely gateway for monitoring workers but may be difficult due to the power imbalance between workers and employers. You must offer an alternative to workers who do not want to give consent which does not detriment them.

Example

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 **will apply**.

Example

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 corroborated following a courier service's HR manager review of the vehicle's tracking device data showing that the vehicle only made a small proportion of journeys it was expected to make.

In this example, additional rules under Article 22 **will not apply** as, although the warning was issued on the basis of the data collected by the automated tracking device, the decision to issue the warning was taken by the courier service's HR manager following a review of the data.

What should we tell workers about automated decision making?

The right to be informed means you must tell workers whose data you are processing that you are doing so for 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 subject access request.

You should:

- 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.

What is the role of human oversight?

When automated decision making is used to inform legal or similarly significant decisions about workers, there is a risk that these decisions are made without appropriate human oversight. For example, whether they have financial circumstance altered based on their performance at work. 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 which are designed as decision-support tools, and therefore are outside the scope of Article 22, you must ensure:

- human reviewers are involved in checking the system's recommendation and should not just apply the automated recommendation to an individual in a routine fashion;
- reviewers' involvement is active and not just a token gesture. They should have actual 'meaningful' influence on the decision, including the 'authority and competence' to go against the recommendation; and
- reviewers 'weigh-up' and 'interpret' the recommendation, consider all available input data, and also take into account other 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?

How do we lawfully monitor workers?

Checklist

- ☐ We have checked that the monitoring of workers is necessary for the purpose we have identified and 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 the DPIA 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 undertaken 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 data we are processing when we monitor workers.
- ☐ Where required, we have an appropriate policy document in place.
- ☐ We included specific information about monitoring workers in our privacy information so that workers are aware of any monitoring taking place.
- ☐ If we use the data from monitoring workers for automated decision making (including profiling), we have checked we comply with Article 22.
- ☐ Where we use automation with human involvement, we ensure the involvement is meaningful.
- ☐ 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.

Specific data protection considerations for different types of workplace monitoring

At a glance

Our how do we lawfully monitor workers guidance took an approach led by the UK GDPR principles. Reading that guidance helps you to understand your data protection obligations, regardless of what monitoring you are considering. Building data protection into monitoring helps develop employment relationships that are based on trust when you are monitoring workers, as well as protecting the data protection rights and freedoms of your workers. The UK GDPR is flexible and applies to all situations where you are monitoring workers.

We have listened to stakeholders, and we understand many organisations found our previous employment practices guidance useful. This covered several commonly occurring scenarios. Advances in technology and working practices pose an increased risk to workers' data protections rights and freedoms, and so in the following sections, we have updated our previous scenario-based guidance on monitoring workers. We have also added some new situations. We will continue to add to this as our work progresses, so do keep checking back.

In detail

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 could procure a tool that helps to monitor your workers, gathers data about them or helps to store the data (ie a cloud storage provider).

In most cases where you are procuring tools or services from a third-party for the purposes of monitoring your workers, 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 UK GDPR responsibilities include:

- complying with the data protection principles;
- ensuring that workers and other individuals who may be captured can exercise their rights regarding their personal data;
- choosing an appropriate processor who will provide sufficient guarantees that they will implement appropriate technical and organisational measures to ensure their processing meets UK GDPR requirements; and
- meeting accountability obligations, such as carrying out data protection impact assessments and adopting a 'data protection by design and default' approach.

For a comprehensive list of your responsibilities, see our guidance on What does it mean if you are a controller?

As part of the procurement process, you need to make sure that the provider gives sufficient information about their tool or service so you can carry out your responsibilities. You can 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 data collected by you for their own purposes. In this case, it is likely that the third party would become a controller for this processing, and you would be a processor.

Further reading outside this guidance

Controllers and processors: in brief

Controllers and processors: in more detail

Contracts and liabilities between controllers and processors

Can we monitor telephone calls?

It would not usually be proportionate to monitor or record the content of calls in all cases. You may 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 house is legally required by FSA rules to record calls. They limit recording to strictly what is required by those rules.

If you have a business need to monitor usage, consider using itemised call records rather than call content. If the itemised call record alone is insufficient, assess whether it can be used to help ensure that any further monitoring is strictly limited and targeted.

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.

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. Workers should understand the purpose and extent of any monitoring.

Information from personal calls should not be used for monitoring. It may be used for billing or in exceptional circumstances, for example where there is criminal activity. Have a policy in place 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 the policy banning personal calls to justify carrying out monitoring.

Expectations of privacy are significantly higher at home or outside the workplace. You should factor this in to your DPIA.

Remember, 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. These people should be told that monitoring is taking place and why. A recorded message is best practice. Where this is not possible, instruct workers to inform callers that calls may be recorded and to explain the reason why. You may provide the rest of the privacy information (retention periods, individual rights available, any data sharing) by other means – for example, emailing the caller a copy of your privacy notice or providing a link to it on your website. Any information collected is likely to be personal data and could be subject to external access requests, make sure workers know call recordings may be released to members of the public if requested. Read our guidance on the right of access for information about handling access requests.

Can we monitor emails and messages?

As an employer you might consider monitoring emails and messages sent to and received by work accounts to protect corporate information, for data security (see our guidance on data loss prevention for more information on this), to identify suspicious activity, and enforce any acceptable usage policies you may have in place.

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. Make sure you inform workers of any monitoring.

If you are considering monitoring emails and messages, you should complete a DPIA as this 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 obligatory, this is good practice and will help you to assess risk and plan, then evidence, accountability.

It would be difficult to justify monitoring the content of emails and messages where monitoring network data would meet your purpose. In exceptional circumstances where content is accessed, you must notify workers in advance that content may be monitored in relevant policy documents. Accessing content will not be appropriate unless there is 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 the network data record be used to narrow the scope of the monitoring, for example to restrict the 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 secure lines of communication that will not be caught by monitoring? For example, for 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 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?

Checklist

- ☐ We are clear about our purpose and collect no more data 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 data 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 bring this to workers' attention regularly.
- ☐ We have informed workers of the nature, extent and justification for any monitoring.
- ☐ We have a retention policy in place. We bring this regularly to the attention of workers, who know what to do with messages that need to be retained for business reasons.

If you are considering monitoring or you are already monitoring online activity which is wider in scope than emails, read our guidance on monitoring device activity.

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

A customer for your products or services may ask you as their supplier to monitor your workers. For example, if you were a supplier for a defence establishment you may be asked to carry out ongoing security checks on those workers employed on the defence contract.

However, monitoring workers cannot be justified solely because your customer makes it a condition of business.

Example

An insurance company wishes to monitor the workers of a service provider to ensure the provider is 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 supplier would need to consider data protection obligations before any monitoring is imposed by the insurance company.

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 workers are informed.

To help you decide this, you could use an assessment your customer might have already undertaken for itself, but this would be a guide only and the decision ultimately rests with you.

Can we use video or audio to monitor workers?

Not all uses of video surveillance and monitoring will be in a work context. You will therefore find our guidance on video surveillance useful for different types of processing.

By audio monitoring we mean the recording of face-to-face conversations, rather than the monitoring of business calls. This is highly intrusive and unlikely to be justifiable in most circumstances. The use of audio recording, particularly where it is continuous, is considered more privacy intrusive than purely visual recording. Its use will therefore require a much greater justification and 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.

Any monitoring should be targeted at areas of particular risk and confined to areas where expectations of privacy are low. Continuous video or audio monitoring of workers is only likely to be justified in rare circumstances.

If you are considering using video or audio monitoring, you should:

- complete a DPIA. This will help you to assess whether the benefits justify the adverse impact;
- as part of your DPIA, consider why this monitoring is necessary for the intended purpose;
- make sure workers are informed about extent and nature of the monitoring, and why it is being carried out;
- ensure that anyone else caught by the monitoring, such as visitors or customers, are made aware of its operation and why it is being carried out; and
- consider the right of access. If a worker or any other individual captured by the monitoring makes an access request, you will need to be able to redact third parties from footage.

Covert monitoring is unlikely to be justified in usual circumstances. See our guidance on covert monitoring for more information.

The use of cameras which have facial recognition capabilities or can perform analytics (for example, to analyse facial expressions) come with higher risks to data protection rights and freedoms depending on the context and the purpose, for example, the use of this technology to unlock a phone where the user has the option of a password is lower risk than the use of it to monitor behaviour in a workspace.

Facial recognition is biometric data. This is unique to an individual, it cannot be changed, unlike a password. There is also the potential for bias and discrimination. Several technical studies have indicated facial recognition is less accurate for some groups. Error rates in facial recognition can vary depending on demographic characteristics such as age, sex, race and ethnicity.

If you are considering using these technologies, you must carry out a DPIA. In your DPIA you should explain the rationale for not choosing less intrusive means.

Our FRT and surveillance checklist will help you identify and address risks around the use of facial recognition. If you are considering using FRT for time and attendance control, read our section on the use of biometrics for time and attendance control.

If you are using or are considering using dashcams, read our dashcams section and our detailed guidance on surveillance in vehicles.

Can we monitor work vehicles?

This guidance covers work vehicles that can be used for personal use as well as vehicles such as lorries. When the private use of a work vehicle is allowed, monitoring during private use will rarely be justified.

Example

An employer provides workers with company cars which they are allowed private use of. 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 outside of work.

You must ensure workers and passengers are informed 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' hours are followed. In this scenario, you can rely on the lawful basis of legal obligation.

You may be using black boxes across your fleet (vehicle telematics) for vehicle insurance policies. This uses technology to track and record driver behaviour to calculate insurance premiums. Telematics data which records the activities of drivers is personal data and is subject to the UK GDPR. If your insurer is handling driver data, they also have obligations. Read our guidance on controllers and processors for further information.

Driver monitoring which is more intrusive than gathering data on time, speed, and distance, for example, monitoring driver behaviour, or the use of cameras or audio are harder to justify due to the higher risk to worker's privacy and the rights of any passengers. You should carry out a DPIA to assess the risks. 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. It is unlikely that the use of such technologies would be justifiable or proportionate.

What about dashcams?

Dashcams can be an efficient way to protect drivers, passengers and assets and can help to reduce insurance costs. However, you should keep in mind that images captured of any identifiable individual counts as personal data and is therefore subject to the UK GDPR and DPA 2018.

Dashcams may be intrusive and can impact on the data protection rights and freedoms of workers and other individuals, especially when used in places that people would not reasonably expect. In terms of outward facing cameras or dashcams, this can apply to other motorists or pedestrians being recorded outside of the vehicle, or for inward facing systems, drivers and passengers within a vehicle. Audio is higher risk, you should switch off any capability to record audio by default, it should only be triggered 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.

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.

Can we monitor information about workers from third party sources?

You need to take special care when considering making use of information about workers from third party sources such as credit reference information or social media sites. You should also be cautious about covert recordings made by workers. Recordings made on workers' or clients' own devices are likely to be a purely personal activity but if the recording is disclosed to you, then it is likely the UK GDPR will apply. This section also applies to information held by employers in a non-employment capacity, such as when a bank monitors its workers' bank accounts.

We will be producing guidance on vetting and verification as part of our recruitment practices project. This guidance discusses the monitoring of workers once they are employed.

Things to consider:

- Before undertaking any monitoring which uses information from an outside source, make sure your purpose (for example, suspicion of criminal activity) justifies the potential adverse impact. You should not search external sources for information about a worker without good reason.
- Provide workers with privacy information so they can understand what sources are to be used and why. For more details, read our guidance on What privacy information should we provide?
- Take particular care with information about workers that you have because of a non-employment relationship with them. For example because they are or have been your customers, clients, or suppliers, or you are connected on social media or an online professional networking site.
- Be cautious with information provided from a worker about another worker. Once information is disclosed to you as an employer, the information is no longer personal, and the UK GDPR may apply.
- Make sure workers carrying out monitoring which involves information from third parties are properly trained. Ensure there are measures in place to prevent the disclosure or inappropriate use of information obtained through such monitoring.
- You must only retain relevant information obtained through such monitoring. You may be able to simply record that a check has taken place and the result of this.

We will be producing guidance about social media and web-scraping in due course, as part of the forthcoming recruitment section of the employment practices guidance hub.

Further reading – ICO guidance

What information must we provide when we obtain personal data from another source?

Can we monitor time and attendance information?

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

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

- recording attendance for payroll purposes.

This can form an important part of an employer's security measures and audit trail but may also pose a risk to data protection rights and freedoms due to the level of knowledge and control over workers' activities and movements.

You must be clear about your purpose for recording access and time information. You must not use the information for a different purpose unless it is compatible with your original purpose.

If you are using, or considering introducing, biometrics to control access, read our guidance on biometrics and access and time data.

Further reading – ICO guidance

Purpose limitation

Example

An employer restricts access to a server room to certain workers for security purposes to protect equipment and information. This is managed 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 identification of workers who had access at the time.

The employer does not repurpose information about workers' access and exit times, for example, for performance evaluation.

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

Organisations are likely to have a number of technical solutions in place to monitor and ensure the confidentiality, availability, and integrity of personal data. 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 must consider the least invasive means possible when selecting solutions to protect against data loss or external threats. You should complete a data protection impact assessment (DPIA). A DPIA will help you to assess the risk and identify if less intrusive methods could achieve your purpose.

Monitoring network traffic, particularly if you carry out analysis of the data to make inferences about workers may be high risk. Our section on automated tools provides guidance on this.

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.

Checklist

Good practice suggestions:

- ☐ We limit the collection, storage, and processing of log data to what is necessary and proportionate.
- ☐ We offer unmonitored access for workers, for example, free Wi-Fi, or standalone devices (with confidentiality safeguards) to facilitate some private usage.
- ☐ We have measures in place to minimise interception which risks disproportionate intrusion (for example, visits to health-related websites).
- ☐ We document the monitoring in a policy which explains when and by whom information about suspicious activity can be accessed.
- ☐ We review our monitoring policy at regularly to assess whether the monitoring serves our purpose.
- ☐ We have considered trialling the monitoring with a representative group of workers to assess the necessity of the monitoring and the accessibility of the policy.

Can we monitor device activity?

Device monitoring is when tools are used to record workers' activity on devices. By devices we include those used personally by workers such as laptops and handheld devices and network devices such as routers and firewalls. This section focuses on the monitoring 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. Read our section on data loss prevention for guidance on monitoring to secure networks.

This guidance is for general processing regulated by the UK GDPR. If you are logging because of a law enforcement data protection audit obligation, you must

not use logging tools indiscriminately and collect more data than you need, this guidance may be useful to understand proportionality and necessity. You should also read our guidance on law enforcement processing.

Developments in technology have led to an increase in the availability and affordability of monitoring tools with the capability to process large amounts of data. This can be particularly intrusive where workers are using their own devices.

Device activity monitoring can include capturing workers':

- web browsing;
- emails and messages;
- documents;
- use of applications;
- screen captures; and
- webcam captures.

Keystroke monitoring 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 worker information and special category data, such as emails about health conditions and emails to union representatives. Capturing webcam shots or footage are particularly unlikely to be justifiable.

What do we need to consider when we monitor device activity?

If you are considering capturing the computer or device activity of workers, you should:

- Identify a lawful basis and a special category condition where appropriate.
- Be clear about your purpose, fully document your justification for carrying out device monitoring, including what consideration was given to using less intrusive means. If you can achieve your aim in a less intrusive way, you should opt for this.
- Carry out a DPIA. You are obliged to carry out a DPIA before undertaking any processing likely to cause high risk to workers' and other individuals' interests. You can use our screening checklists and read our detailed DPIA guidance to help you decide. Even where not mandated, a DPIA is good practice, the process with assist with your risk assessment and planning.
- Consider consulting 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 a trust-based relationship. The DPIA process includes a stage where workers are consulted.

- Ensure workers are informed about the monitoring, including how it is used for making decisions which affect them.
- Consider making aggregated analytics reports. Aggregated reports can be used to identify trends without identifying individual workers.
- Consider banning the private use of work devices and blocking problematic websites. However, you must keep in mind that even with such a policy in place, it would be difficult to justify accessing a worker's personal communications.

You must ensure private use is not captured where workers are using their own personal devices for work.

What about remote and home workers?

The rise in remote and home working in recent years has led to an increase in this type of monitoring as employers seek to secure their systems and manage remote workers.

If you are monitoring workers remotely, 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, so you should factor this risk into your planning.

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

At a glance

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

However, the technologies and systems used to identify workers and enable access have developed, with biometric data increasingly part of the picture. Whilst processing biometric data (for example, using a worker's fingerprint to provide access to work) can be a convenient way to give workers access to work, it does pose a risk to data protection rights and freedoms and the relationship of trust between workers and employers. The processing of employees' biometric data therefore requires careful consideration. You must also consider whether you need extra security measures when storing biometric data, as processing biometric data comes with a higher risk of harm as it cannot be reset in the event of a breach, unlike passwords.

In detail

What is biometric data?

The UK GDPR defines biometric data as:

Quote

"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 includes:

- fingerprints;
- facial recognition templates; and
- voice recognition templates.

This is not an exhaustive list.

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

You should document the evidential basis for choosing to rely on biometric data, including any consideration of other less intrusive means and why they are inadequate. You must be clear about your purpose. If a reasonable alternative option to the use of biometric data is possible, you should be sure of your justification for not choosing this.

How do we identify a lawful basis, and a special category condition where needed?

There are six lawful bases to choose from. There is no hierarchy, and no one basis is better than the others. Your lawful basis will depend on your purpose for using biometric data to identify workers. Read our section on lawful bases for more information.

Biometric data constitutes special category data whenever it is processed "for the purpose of uniquely identifying a natural person". So, as well as choosing a lawful basis, you must identify a special category condition for processing when you are using biometric data for access control, as you will be identifying workers to do so. Read our section on special category conditions for monitoring workers for more information, and our core special category guidance. The UK GDPR has rules (under Article 22) to protect workers if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

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

- necessary for the entry into or performance of a contract;
- authorised by law that applies to you 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 the individual's explicit consent.

The UK GDPR says that consent must be a freely given, specific, informed and unambiguous affirmative indication. This is the most likely gateway for using biometric data for access control but it may be difficult to get true consent due to the power imbalance between workers and employers. You must offer an alternative to workers who do not want to give consent so they have free choice. The alternative must not be a detriment to workers choosing to use it, you must consider whether explicit consent can be genuine where a manual option takes longer.

If you are relying on facial recognition for workspace access, you would need an alternative for those who have not consented which does not involve the processing of their biometric data, such as a separate access for workers who have not consented. This should not disadvantage workers. For example, if those who choose not to use biometric data option need to walk further. Where a system scans all workers regardless of whether consent to process biometric data has been provided, this would involve the processing of biometric data of the workers who have not consented. This would be unlawful as there would be no lawful basis for processing the data of those who have not consented.

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 data is also used for payroll purposes. This system is using biometric data to identify individual workers so the employer needs a valid condition for processing special category data. 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 'explicit consent' as workers can give it freely and are able to withdraw it at any time.

Example

An employer rolls out new laptops to all workers. The devices have the option of facial recognition sign in. Workers who agree to using facial recognition provide 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.

If a reasonable alternative option to the use of biometric data is possible, you should be sure of your justification for not choosing this over the use of biometric data.

You should document your lawful basis and special category condition in your DPIA, including a rationale for the justification for using biometric data where a less intrusive option is available to workers.

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

Yes, you must carry out a DPIA whenever you process biometric data to uniquely identify an individual. This will assist you in assessing and documenting risk and any measures in place to reduce identified risks. The DPIA process also provides an opportunity to consult with workers and their representatives before any processing begins. This process can shape your planning and help you to address any privacy concerns that may be raised during the consultation. This will help build trust and reduce the risk of workers objecting after the system is rolled out.

What about accuracy and fairness?

When biometric data is used for matching to allow workers to access work or to pay them correctly, inaccuracy may have a particularly detrimental impact on workers. Be clear about the 'match rate' and the risk of false negatives. By this, we mean the statistical accuracy of your system. It is your responsibility as controller regardless of whether you have engaged another organisation to provide the system.

Example

If a building access system which uses fingerprints to allow workers onsite produces a false positive, then someone without permission to enter may access the site. If it produces a false negative, then a worker with permission will be barred from accessing site. As a site manager is always available and can give manual access to workers, the organisation chooses the higher risk of false negatives but minimises the risk of false positives to keep the building safe. The manager will mark any delays caused by false negatives on the system to ensure workers are not recorded as being late.

Numerous studies have shown facial recognition works with less precision for some demographic groups. To comply with the UK GDPR 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 that system is suitable for the groups and individuals you plan to use it for. If the system you use results in processing which causes bias or discrimination, you will infringe the UK GDPR principle of fairness.

Accuracy and match rates are also linked to workers' rights relating to automated decision-making and profiling.

Where access to work relies on authentication by an automatic process there is a risk of false negatives. Manual reviews must be available where an automatic process has resulted in a possible false negative. False negatives should be confirmed quickly with access given back to the worker as soon as possible. The request for manual reviews should not be to the detriment of workers. You should ensure both forms of authentication, biometric and the alternative, are offered on an equal basis, for example the processes take the same amount of time. This ensures that the explicit consent relied upon is freely given and decisions to provide consent are not made on the basis of speed.

Example

An app-based taxi company trials a facial recognition sign in process for drivers to access jobs via an app. They rely on explicit consent, offering those drivers who do not consent to the use of their biometric data a human review sign in option. Both forms of sign in take a similar length of time to complete. Where there is a false negative, either through the biometric login, or through the human review login, the time taken to resolve the issue follows the same process and neither option creates a disadvantage.

What about informing workers?

Make sure workers understand how the system works and what personal data is collected along with the nature and purposes of the monitoring. You should inform your workers through your privacy information, and you may want to provide information during staff meetings. You should cover this in the consultation stage of your DPIA, but then you should regularly bring the privacy information to workers' attention.

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 where 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.

Where consent is relied upon, workers can refuse and should be provided with an alternative which does not cause them detriment.

See our section on workers' right to object and our core UK GDPR right to object guidance for further details including when you can refuse an objection.

Further reading – ICO guidance

Automated decision making and profiling

Purpose limitation

Data protection impact assessments

What is biometric data?

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, it can't be changed. 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 such as encryption and organisational measures such as access restrictions.

Further reading – ICO guidance

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 consulted 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 data.

- ☐ We have considered accuracy and fairness and mitigated any identified risks.
- ☐ We have considered rights 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.