About this guidance

Our consultation on this draft guidance is open until 5 March 2024.

This guidance is aimed at employers who are keeping employment records. It will help them understand their data protection obligations under the UK GDPR and DPA 2018 (we refer to these as data protection law). Keeping records about workers is a necessary part of running an organisation. Data protection law applies whenever you process your workers' personal information. The law does not stop you from collecting, holding and using records about workers. It helps to strike a balance between your need to keep employment records and workers' right to private lives.

We have designed this guidance for you to read alongside our other published guidance on data protection and employment. In particular, our detailed guidance on information about workers' health, Employee monitoring, and Recruitment and selection.

We use the terms 'worker' or 'former worker' to mean all employment relationships, whether this includes employees, contractors, volunteers or gig and platform workers. This is for the purposes of this guidance only and not in an employment law or other legal context.

How should we use this guidance?

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

Legislative requirements

- **Must** refers to legislative requirements.

Good practice

- **Should** does not refer to a legislative requirement, but what we expect you to do to comply effectively with the law. You should do this unless there is a good reason not to. If you choose to take a different approach, you must be able to demonstrate that this approach also complies with the law.
- **Could** refers to an option or example that you could consider to help you to comply effectively. There are likely to be various other ways you could comply.

This approach only applies where indicated in our guidance. We will update other guidance in due course.

Collecting and keeping employment records

Our consultation on this draft guidance is open until 5 March 2024.

In detail

What kinds of records might we keep about our workers?

As an employer, there are many different kinds of records you may need to keep about your workers. For example:

- personnel files;
- sickness and injury records;
- disciplinary and grievance records;
- training records;
- appraisal or performance review records;
- payroll information;
- pension information;
- interview notes;
- emails;
- references; and
- equality and diversity information (eg information about ethnicity, religion, disability and sexual orientation).

The UK GDPR and the DPA 2018 (referred to here as data protection law) applies whenever you are

processing your workers' personal information. Data protection law sets out principles for collecting and using personal information. These do not stop you from keeping the records you need about your workers. But you **must** make sure that you use their information in line with the data protection principles. In particular, you **must** make sure that your use is:

- fair – you only use people's personal information in ways they could reasonably expect, and not in ways that have unjustified adverse effects on them;
- lawful – you have a lawful basis to use the information, and you don't do anything generally unlawful with it; and
- transparent – you are open, honest, and inform people about what you are doing with their information.

Before you collect and use any personal information about your workers, you **must** be clear about why you are doing so. You **must** also be satisfied that you have justified reasons for collecting it.

You **must** record your purposes and specify them in your privacy information.

You can only use the information collected for employment records for a new purpose if:

- this is compatible with your original purpose;
- you get specific consent from the worker; or
- you have a clear obligation or function set out in law.

Remember to consider your obligations under:

- employment law;
- health and safety law;
- any other legislation;
- any common law duties; and
- any relevant industry standards.

Further reading

Read our guidance on:

- Lawfulness, fairness and transparency
- The data protection principles
- Special category data
- Purpose limitation

How can we lawfully keep records of workers' personal information?

To lawfully keep records of your workers' personal information, you **must** first identify a lawful basis. There are six lawful bases for processing set out in Article 6 of the UK GDPR. Remember that:

- You **must** apply at least one of these whenever you are keeping records of your workers' personal

information.

- You **should not** see any one basis as always better, safer or more important than the others. There is no hierarchy in the order of the list in the UK GDPR.
- How you decide which lawful basis for keeping records applies depends on your specific purposes, and your relationship with the worker.
- You **must** think about why you want to keep records of the information and consider which lawful basis best fits the circumstances.
- You might consider that more than one basis applies, in which case you **must** identify and document all of them from the start.

You can use our interactive guidance tool to help you decide which lawful basis might apply.

You may need different lawful bases for different categories of information, or for information used for different purposes.

You may also need to keep records of special category information about your workers. This is information that is considered especially sensitive, and so is given a greater level of protection. The special categories are information about peoples':

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

There are rules that cover using special category information and you cannot keep records of this type of information unless you meet some additional requirements. This means that in addition to a lawful basis, you **must** also identify a special category condition (under Article 9 of the UK GDPR). You may also need to satisfy a condition in Schedule 1 of the DPA 2018.

Lawfulness also means that you don't do anything with the personal information which is unlawful in a more general sense. This includes statute and common law obligations, whether criminal or civil. If keeping records would involve you committing a criminal offence, it will obviously be unlawful. However, keeping records may also be unlawful if, for example, it results in:

- a breach of a duty of confidence;
- your organisation exceeding its legal powers or exercising those powers improperly;
- an infringement of copyright;
- a breach of an enforceable contractual agreement;
- a breach of industry-specific legislation or regulations; or
- a breach of the Human Rights Act 1998.

You may need to take your own legal advice on other relevant legal requirements.

Further reading

Read our guidance on:

- Lawfulness, fairness and transparency
- Lawful basis for processing
- Special category data

Can we rely on a worker's consent?

You may be considering relying on a worker's consent to process the information in their employment records. Consent is one of the lawful bases for processing personal information. Explicit consent is one of the conditions that can be used to process special category information. However, consent provides certain challenges in an employment context.

The UK GDPR sets a high standard for consent, and people **must** have a genuine choice over how you use their information. Consent **must** be:

- freely given;
- specific;
- informed;
- unambiguous; and
- expressed by a clear affirmative action (ie using an opt-in).

It **must** be as easy for someone to withdraw their consent as it is to give it.

It may be difficult for you to rely on consent to keep records of personal information about your workers. This is because, as an employer, you will generally be in a position of power over your workers. They may fear adverse consequences and might feel they have no choice but to agree to you collecting and using their information. In such circumstances, consent is not considered freely given.

Explicit consent is not defined in the UK GDPR, but it is not likely to be very different from the usual high standard of consent. The key difference is that explicit consent **must** be expressly confirmed in a clear statement (whether oral or written), and not by inference from someone's actions.

You **should** avoid relying on consent unless you are confident you can demonstrate it is freely given. This means that you **must** give a worker the option to say 'no' without fear of a penalty being imposed and allow them to withdraw their consent at any time.

You **must not** rely on consent as a lawful basis if:

- the worker has no genuine choice over how you use their information; or
- you would still keep records of the information on a different lawful basis if the worker refused or withdrew consent.

If you think it will be difficult for you to show that consent has been freely given, you **should** consider relying on a different lawful basis, such as legitimate interests. See 'What lawful bases might apply when keeping employment records?' for more information.

However, this does not mean that, as an employer, you can never use consent as a lawful basis. Even where you are in a position of power, there may be situations where you **could** still show that consent is freely given.

There are also other considerations you **must** take into account if you want to rely on consent, such as recording and managing consent. Please see our separate guidance on consent for more information.

Further reading

Read our guidance on:

- Special category data
- Consent

What lawful bases might apply to employment records?

We've listed below the lawful bases which are most likely to be relevant in an employment records context, but other lawful bases may be available.

Remember, it is your responsibility to decide what lawful basis is most appropriate. If you can meet the criteria for a specific lawful basis, then you are likely to be able to rely on it.

Contract

This lawful basis applies where you need to keep employment records for a contract you have with the worker, or because they have asked you to take specific steps before entering into a contract. This is most likely to apply when you need to collect and use information about your workers under an employment contract.

You **must** only use the contract lawful basis once an employment offer of employment has been accepted, even if a contract has not yet been entered into. Acceptance of a conditional offer of employment shows an intention on both sides to enter into the contract. Until that stage, legitimate interest **could** be a more appropriate lawful basis.

This lawful basis only applies for contractual employment purposes rather than legal obligations under employment law.

Example

An organisation keeps records of their workers' names, addresses and salary information to meet their

contractual obligation to pay them for their work.

Legal obligation

You may be able to rely on this lawful basis where you need to use personal information kept in employment records to comply with a common law or statutory obligation (although this does not include contractual obligations).

Example

Employers have an obligation to share workers' names, addresses and salary details with HMRC for tax purposes.

Legitimate interests

This lawful basis may apply if keeping records of workers' personal information is necessary for your legitimate interests or the legitimate interests of a third party. This won't apply if there is a good reason to protect the worker's personal information which outweighs those legitimate interests. As part of this, you should carry out a legitimate interests assessment to determine if this is the case. For more information see our separate guidance which covers How can we apply legitimate interests in practice?

Example

An organisation requests references containing personal information about a job applicant from a previous employer. The organisation can rely on legitimate interests to collect and hold the information in this reference.

Vital interests

In exceptional circumstances, you may be able to rely on the vital interests lawful basis to protect someone's life. This lawful basis is very limited in its scope and generally only applies to matters of life and death. For example, if there is a medical emergency and a worker's life is at immediate risk. It is important to note that you cannot rely on vital interests for health or other special category information if the person is capable of giving consent, even if they refuse their consent.

Further reading

Read our guidance on:

- A guide to lawful basis

- Contract
- Legal obligation
- Legitimate interests
- Vital interests

What conditions for keeping records of special category information might apply?

As explained above, if you are keeping records of special category information about your workers, in addition to identifying a lawful basis, you **must** also identify a special category condition.

There are 10 conditions for special category information. For five of these conditions, you **must** meet additional conditions and safeguards set out in Schedule 1 of the DPA 2018.

If you are relying on a Schedule 1 condition, many of these also require you to have an 'appropriate policy document' in place. This acts as part of the additional safeguards that are necessary for keeping records. See our separate guidance What is an appropriate policy document for more information. We have also produced an appropriate policy document template you can use.

Remember that you **must** determine your condition before you begin keeping records and you **must** document your decision, along with your lawful basis.

We've listed below the special category conditions which are most likely to be relevant in an employment records context:

Employment, social security and social protection law

To rely on this condition to keep employment records, you **must** be keeping records to comply with employment law, or social security and social protection law. You **should** identify the legal obligation or right, either by referring to the specific legal provision or by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you **could** refer to a government website or to industry guidance that explains generally applicable employment obligations or rights.

This condition does not cover any employment records you keep to meet purely contractual employment rights or obligations.

You **must** be able to justify why keeping records of this specific information is necessary, and a reasonable and proportionate way of meeting specific rights or obligations under employment, social security and social protection law. You **must not** obtain or use more information than you need.

If you are relying on this condition, you should also meet the associated condition set out in Part 1 of Schedule 1 of the DPA 2018. This condition also requires you to have an appropriate policy document in place.

Legal claims or judicial acts

You may be able to rely on this condition if using special category information is necessary to establish, exercise or defend legal claims. For example, if a worker is suing their employer.

You **must** be able to justify why keeping records of this specific information is 'necessary' to establish, exercise or defend the legal claim. You **must** only use this information if it is relevant and proportionate, and you **must not** obtain or use more information than you need.

You **must** only rely on the legal claims element of this condition, as the judicial acts element only applies to courts acting in their judicial capacity.

Substantial public interest

This condition allows you to keep records of special category information, if this is necessary for reasons of substantial public interest, as set out in UK law.

To rely upon this condition, you **must** meet one of the specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018. You **must** also have an appropriate policy document in place for almost all of these conditions.

The most likely substantial public interest conditions relevant for processing special category information about your workers are:

- statutory and government purposes;
- equality of opportunity or treatment;
- racial and ethnic diversity at senior levels;
- preventing or detecting unlawful acts;
- regulatory requirements;
- preventing fraud;
- safeguarding of children and of individuals at risk; and
- occupational pensions.

This list isn't exhaustive and if you intend to rely on any substantial interest conditions, you **should** look at the details of the specific conditions in the legislation to determine what condition is most appropriate to your purpose.

Vital interests

You may also find that vital interests might apply in some limited circumstances, similar to the vital interests lawful basis, discussed above.

Further reading

Read our guidance on:

- Lawfulness, fairness and transparency
- Special category data
- Substantial public interest conditions

How much personal information can we hold in our employment records?

The data minimisation principle says that you **must** make sure that the personal information you hold is adequate, relevant, and limited to what is necessary for your purposes. This links closely with the storage limitation principle where you **must** consider how long you need to keep the information and why. For more information see 'How long can we keep workers' personal information?'.

This means that you **must** identify the minimum amount of personal information you need to hold about your workers. You **must not** hold more information than that.

How much is adequate, relevant and necessary will depend on the context. It may also differ from one person to another. Therefore, to work out whether you are holding the right amount of personal information, you **should** first be clear about why you need it.

If you only need to hold particular information about certain workers, you **must** collect it just for those people. The information is likely to be excessive and irrelevant about other workers.

Example

An organisation holds information about employees' disabilities, so that they can make reasonable adjustments to enable them to carry out their roles. Information about disabilities is information about health, and so is special category information. The organisation ensures that it only holds information about disabilities for workers who need reasonable adjustments, as it would be unnecessary to hold this information about other workers.

You **should** periodically review your records to check that the personal information you hold about your workers is still relevant and adequate for your purposes, and delete anything you no longer need.

Further reading

Read our guidance on:

- Data minimisation
- Right to rectification
- Right to erasure

How do we keep workers' personal information in our records accurate and up-to-date?

The accuracy principle says that you **must** take all reasonable steps to keep any personal information you hold about your workers accurate and up-to-date.

In practice, this means that you **should**:

- take reasonable steps to ensure the accuracy of any personal information;
- make sure that is clear where you have obtained personal information from;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to periodically check and update the information.

If you are collecting personal information directly from your workers, it is your responsibility to make sure it is correct. You **should** take particular care if the information might have serious implications for the worker if it was recorded inaccurately (eg information that is used to calculate a worker's salary).

The more important it is that the personal information is accurate, the greater the effort you **should** put into ensuring its accuracy. So if you are using the information to make decisions that might significantly affect the worker concerned or others, you **should** put more effort into ensuring accuracy. This may mean you have to get independent confirmation that the information is accurate. For example, you may need to check the precise details of the education, qualifications and work experience of job applicants, if it is essential for a particular role.

A record of an opinion is not necessarily inaccurate personal information just because the person disagrees with it, or it is later proved to be wrong. For example, an opinion expressed in a performance review that someone is underperforming is not necessarily inaccurate, just because the worker disagrees with it. Opinions are, by their very nature, subjective and not intended to record matters of fact. However, in order to be accurate, your records **should** make clear that it is an opinion, and, where appropriate, whose opinion it is.

If someone challenges the accuracy of an opinion, you **could** add a note recording the challenge and the reasons behind it. If it becomes clear that an opinion was based on inaccurate personal information, you **should** also record this fact in order to ensure your records are not misleading.

Remember that workers have the right to have inaccurate personal information corrected. This is known as the right to rectification.

Further reading

Read our guidance on:

- Accuracy
- Right to rectification

How long can we keep records of our workers' personal information?

The storage limitation principle says that you **must not** keep personal information for longer than you need it. Making sure that you erase or anonymise personal information when you no longer need it will also reduce the risk that it becomes irrelevant, excessive, inaccurate or out-of-date.

Therefore, you need to consider how long you need to keep workers' personal information, as well as the information of former workers, and be able to justify doing so. This depends on your purposes for holding the information.

Data protection law does not set specific time limits for how long you can keep personal information of your workers. This is up to you, and will depend on how long you need the information for your particular purposes.

You **must** consider any legal or regulatory requirements and seek advice on compliance, if necessary. There are various legal requirements and professional guidelines about keeping certain kinds of records, such as information on aspects of taxation, or health and safety. Certain legislation may require you to keep the information for a specified period. If you keep workers' personal information to comply with a requirement like this, you will not be considered to have kept the information for longer than necessary.

You **must** make sure that you only retain records that you still need. Once you no longer need the information, you **should** erase it, or, where possible, anonymise it. For example, after the employment relationship and all your legal obligations to retain the information have ended. This links to the accuracy and data minimisation principles. If you hold on to information for longer than you need it, you are holding on to more information than you need, and it is more likely to become inaccurate over time.

You **should** set up a retention policy or schedule that lists:

- the types of record or information you hold;
- what you use it for; and
- how long you intend to keep it.

They help you establish and document standard retention periods for different categories of personal information.

You **should not** take a 'one-size-fits-all' approach to retention of workers' personal information. While you may need to hold on to some types of information about previous workers, you may be able to delete other information as soon as the employment relationship ends.

Different categories of personal information will need different retention periods. This will depend on your purpose for holding the information. You may also have other legal or regulatory obligations to retain some records, such as about income tax, or certain aspects of health and safety. You **should** know what these other obligations are, and factor them in to your retention schedules.

Where possible, you **could** set up automated systems to help with this process that flag when information you are holding is due to be reviewed or deleted.

Further reading

Read our guidance on:

- Storage limitation
- Documentation requirements
- Right to erasure

How do we keep our records about workers' personal information secure?

The security principle says that you **must** have appropriate security measures in place to prevent the personal information you hold about workers being accidentally or deliberately compromised.

You **must** choose a level of security appropriate to the nature of the information you are protecting and the level of harm that might result from misuse or loss.

You **must** make sure that the employment records you hold:

- can only be accessed, altered, disclosed or deleted by those who are authorised to do so (and that those people only act within the scope of the authority you give them). For example, ensuring that access to employment records systems is limited to HR staff only, and that the information managers have access to is limited to what they need to meet their obligations;
- are accurate and complete about why you are processing them; and
- remain accessible and usable. This means that you **should** put in place steps to ensure that you can recover the information if it is accidentally lost, altered or destroyed.

In particular, if you hold special category or criminal offence information about your workers you **should** think carefully about its security. For example, limiting access to only those who need to see it, such as password protecting it. If a physical record exists, you **should** keep it in a sealed envelope in the worker's file or in a lockable cabinet, and make sure that only people who need it have access to it.

Example

An organisation collects information about its workers' health conditions and disabilities so that they can provide additional support or reasonable adjustments to workers who need it, as well as for equality monitoring purposes. The organisation determines which members of staff need to know this information (certain staff in Human Resources and workers' line managers) and makes sure that no other staff have access to the records.

When you are reviewing your information management systems that you use for employment records, you **must** consider data protection by design and by default, so that data protection is built in to your systems. If you are reviewing your existing systems, you **must** consider how you can incorporate this requirement.

You **should** make sure that access to necessary information is protected against any automatic deletion processes. Also you **should** ensure you still have access to information if staff leave or change roles. For example, you **should** store employment records centrally, rather than locally so you are not dependent on the availability of individual managers for access.

Further reading

Read our guidance on:

- Security
- Data protection by design and default
- 11 practical ways to keep your IT systems safe and secure

- How to minimise the risk of personal data breaches happening
- Practical methods for destroying documents that are no longer needed

What do we need to tell workers about the records we hold of their personal information?

Data protection law requires fairness and transparency, and provides a right for people to be informed about how you are using their personal information and why.

Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with your workers.

You **must** tell your workers:

- your purposes for collecting and using their personal information;
- your lawful basis;
- your condition for processing (if it includes special category or criminal offence information);
- your retention periods for the information;
- who, if anyone, you plan to share their information with;
- their rights over their information; and
- details of where you got their personal information from, how you are going to use it, and who you will disclose it to.

If you are collecting this information directly from your workers, you **must** make this privacy information available to them at the time you collect their information. If you are collecting the information from other organisations, rather than directly from the worker, you **must** provide them with privacy information within a reasonable period, but at the latest within one month of obtaining it.

You **must** provide this information in a way that is easily accessible to your workers, easy to understand, and in clear and plain language.

There are a range of ways you can provide this privacy information, but you **must** make workers aware of it and give them an easy way to access it. You **could** provide it:

- as part of your staff privacy notice on your organisation's intranet;
- as part of your general data protection policy;
- as separate privacy information in a worker handbook;
- using 'just in time' notices if using online workshops, platforms or tools where personal information might be collected or shared with others;
- as a general notice on a staff notice board; or
- by sending a letter or email to workers.

What method you use and the most effective way of giving privacy information to your workers will depend on the nature of your organisation and what way fits best with your needs.

You **should** make sure that you periodically remind existing workers about this information too. If your

organisation is large, you **could** check with a random sample of workers that they:

- are aware of this information;
- received it; or
- know how to find it.

You **should** regularly review and, where necessary, update your privacy information. You **must** bring any new uses of people's personal information to their attention before you start the processing.

Further reading

- Right to be informed
- How to write a privacy notice and what goes in it – guidance for small to medium sized enterprises
- We have also produced a privacy notice template.

Do workers have a right to access their employment records?

Yes. The right of access is commonly referred to as a subject access request (SAR). It gives someone the right to obtain a copy of their personal information from your organisation. This includes where you got their information from, what you're using it for and who you're sharing it with.

There are no formal requirements about how the request is made. A SAR can be made verbally or in writing, including by social media. Workers can make requests to any part of your organisation, and they do not have to direct it to a specific person or contact point. However, you **should** have a designated person, team and email address for SARs. You **could** set up a specialist portal or process for your workers to help them make SARs efficiently and to help you to recognise and respond to them.

Workers are especially likely to exercise their right to access their employment records during grievance or disciplinary proceedings, or in the case of dismissal. You **should** make sure that managers in your organisation are aware that a worker going through a disciplinary or grievance proceedings still has the right to access their personal information.

You **must** respond to a SAR from a worker without delay and within one month of receiving the request. However, you **could** extend the time limit for responding by up to two months if the SAR is complex or if they have sent you a number of requests.

If you have a large amount of information about someone, and their request is not clear, you can ask them to specify the information or processing activities their request relates to. In these cases, the time limit for responding to the request is paused until you receive clarification, although you **should** still provide any of the supplementary information you can do within one month.

You may have outsourced some of your processing to another organisation that holds personal information on your behalf (and you, as controller, do not hold that information). As a controller, you are still ultimately responsible for complying with SARs for employment records, not your processor.

The processor **must** help you meet your obligations for SARs and you **should** make this clear in the agreement with them. The processor **must** search for this information and, if necessary, give you a copy, if

you request it. See 'What are our obligations if we have outsourced some of our processing about our workers?'

Sometimes you may need to give or receive confidential references about someone. The personal information in a confidential reference is exempt from the right of access for prospective or actual workers. The exemption applies regardless of whether you have given or received the reference.

It is important to note that this exemption only applies to references given in confidence. You **should** make it clear to people, and those providing references, whether you are treating references confidentially or if you are adopting a policy of openness. You **should** do this through the privacy information you provide. For more information see our guidance on the right to be informed.

Further reading

Read our detailed guidance on the right of access. This includes detail on possible exemptions from the right of access, some of which may be relevant in the context of employment records, such as the exemption for confidential records.

Also see our separate SARs Q&A for employers.

Do workers have a right to have their employment records erased?

In some circumstances, people have the right to have their personal information erased. This is known as the right to erasure, or sometimes, the right to be forgotten.

It only applies in certain circumstances, many of which do not apply in an employment context.

However, the right to erasure does apply where the personal information is no longer necessary for the purpose you collected it for. The obvious example is after an employment contract has ended it may no longer be necessary to keep references provided by previous employers or job application materials. However, current workers may also have a right to have information in their employment record erased, if this is no longer needed.

Example

An organisation receives a complaint about one of its workers. After investigating, the organisation concludes that the complaint was vexatious, and they do not need to take any further action. The worker requests that the organisation erase the details of this complaint from their employment record. The organisation decides that it no longer needs this information for the reasons it collected it for and decides to accept the request.

People also have a right to have their personal information erased when it is being processed on the basis of consent, and they withdraw that consent. As mentioned in 'Can we rely on a worker's consent?' above, in

most cases you will not be relying on consent to process employment records. But if you are, and the worker later withdraws their consent, you **must** erase the information.

Example

An organisation asks some of their workers if their images can appear in marketing and promotional materials. They collect these images and publish them on the basis of the workers' consent. One worker who initially agreed, later changes their mind and withdraws their consent for their image to appear. The organisation must remove the worker's image from the marketing materials as soon as possible, and should erase them, if the worker requests it.

There are a number of reasons why you can refuse to comply with a request for erasure. In the employment context, the ones that are most likely to be relevant are if:

- you are under a legal obligation to keep some records about past workers for tax or social security reasons; or
- the request is manifestly unfounded or excessive.

Further reading

Read our guidance on the right to erasure.

Who is responsible for data protection and employment records in our organisation?

Accountability is one of the key principles in data protection law. The accountability principle means that you are responsible for what you do with personal information and how you comply with the other principles.

You **must** have appropriate measures and records in place to be able to demonstrate your compliance with your data protection obligations. This doesn't just include compliance with the principles (as explained in the preceding sections). But also, your other obligations, such as:

- taking a 'data protection by design and default' approach;
- documenting your processing activities; and
- carrying out data protection impact assessments (DPIAs) for uses of personal information that are likely to result in high risk.

You **should** identify who within your organisation has responsibility to authorise or collect your workers' personal information. You **should** ensure they are aware of your organisation's policies and procedures.

You **should** also make them aware of data protection law. If they lack proper authority and necessary training, this could lead to a risk of non-compliance. You should also consider any obligations under other

laws, such as employment law and health and safety legislation.

Ultimately, your organisation, as the controller, has responsibility for data protection compliance. If you use any processors that are processing workers' personal information on your behalf, you **must** have a written contract in place with them. See 'What are our obligations if we have outsourced some of our processing about our workers?'

If you have a data protection officer, you **must** involve them in any decisions about your processing of workers' information.

You also **must** be aware of the data protection rights workers have when you are processing their information.

We also produced the Accountability framework which can help any organisation, whether small or large, with their obligations. You may wish to use the framework to help you assess your organisation's accountability.

Further reading

Read our guidance on:

- Accountability principle
- Accountability and governance
- Data protection by design and default
- Documentation
- Data protection impact assessments
- Controllers and processors
- Contracts
- Data protection officers
- Individual rights
- Accountability framework

Using employment records

Our consultation on this draft guidance is open until 5 March 2024.

In detail

When can we share workers' employment records with other people or organisations?

From time to time you may receive requests for information about particular workers that come from other people or organisations. You are not necessarily required to share information about your workers just because someone has asked for it. However, there are occasions where you may need or want to.

In some cases, you may have no choice but to share the information requested about a worker. This is when there is a legal obligation to share, arising from laws outside data protection legislation which you **must** respond to. For example, you are under a legal obligation to respond to requests for information about your workers from HMRC. If this is the case, data protection does not stand in the way of sharing.

In other cases, you have a choice whether or not to share. You **should** consider the request carefully and only share information about a worker when you are satisfied that it is right to do so. You **should** carefully weigh the potential benefits and harms of sharing or not sharing the information. If you are not sure, you **could** ask the worker for their consent to share their information.

You **must** have a lawful basis for sharing your workers' personal information with other organisations. You **must** make sure that you only share necessary information, and that you send it securely to the correct person. You **must** also make your workers aware about who you are sharing their information with, and why you are sharing it.

You **should** work out who in your organisation will be responsible for dealing with requests to share

information, and give them adequate training to do so.

If you are asked to share personal information from a worker's record in an emergency, you **should** carefully decide whether to share. You **should** take into account the nature of the information being requested and the likely impact on the worker of not providing it. You can and **should** share information about someone in an emergency if it will save their life or protect them or others from serious harm.

Further reading

We have developed a data sharing page which includes the Data sharing code of practice, as well as FAQs, checklists and case studies to help you work out what you need to do to share personal information with other organisations.

What do we need to consider when providing references?

Providing or receiving a reference about a worker with another organisation involves sharing that worker's personal information. Data protection law allows you to share information for this purpose.

In general, the references that you provide will relate to the worker's employment with you. However you may sometimes be asked to give references in other circumstances, such as character references for voluntary roles or a financial reference for a mortgage application. These still count as references and still involve sharing the worker's personal information.

You **must** be as open as possible with workers about information which relates to them. They have a right to challenge information that they consider to be inaccurate or misleading, particularly when, as in the case of a reference, this may have an adverse impact on them.

Example

A worker, who has been employed at Company A for several years, applies for a job at a Company B. Company B requests a reference from Company A, asking for information about the worker's performance, capability to perform the role they have applied for and attendance records. Company A can rely on the legitimate interests lawful basis to share this information about the worker. Company A should share only the information that is necessary for Company B to make an assessment of the worker's suitability for the role.

Can we publish information about our workers?

You may wish to publicise your activities and operations in a way that involves sharing information about your work force. For example:

- annual financial reports;

- advertising materials;
- media articles; or
- social media posts.

If you are a public authority, you may be under a legal obligation to publish information that contains your workers personal information, under the Freedom of Information Act (FOI) or the Environmental Information Regulations (EIR).

You **must** balance the benefits to you of publishing information about your workers with their reasonable expectations of privacy. Where possible, you **should** use information that does not identify individual workers.

You **could** implement an employee information disclosure policy that sets out how you approach this. You **could** set out what factors to consider when deciding whether to publish personal information about workers, either proactively, or in response to, FOI and EIR requests.

If it is necessary to publish your workers' personal information, you **must** make them aware of this in advance. You **must** make sure that you do not publish more information than necessary. For example, if you are publishing information in response to FOI requests, consider whether you can redact any information that identifies your workers.

You **must** identify a lawful basis to publish information about your workers. If this involves special category information, remember you **must** also identify a special category condition.

Further reading

Requests for personal data about public authority employees (PDF) (FOI and EIR guidance)

How do we handle sickness and injury records?

We have covered the issue of sickness records in our guidance on information about workers' health.

What are our obligations if we have outsourced some of our employment records about our workers?

You may have outsourced some of your record keeping to another organisation, such as human resources or payroll functions. You are considered the controller of the personal information and the other organisation is acting as a processor.

As controller, you have ultimate responsibility for making sure that your processing of workers' personal information complies with data protection law. This includes any processing that is carried out by a processor on your behalf.

You **must:**

- comply with the data protection principles;

- make sure that your workers can exercise their rights about their personal information;
- make your workers aware of your use of a processor and inform them who you are sharing their information with and what you are sharing;
- have contractual arrangements in place to guarantee that you can deal with SARs properly, irrespective of whether the request is sent to you or the processor;
- implement appropriate technical and organisational security measures to ensure the security of personal information;
- make sure that any processor you use adopts appropriate security measures, both in terms of technical and organisational measures;
- have a written contract with your processor, which requires the processor to only use your workers' personal information in line with your instructions, and to maintain appropriate security;
- comply with the UK GDPR accountability obligations, such as maintaining records, carrying out data protection impact assessments and appointing a data protection officer; and
- comply with the UK GDPR's restrictions on transfers of personal information outside the UK.

Further reading

Read our guidance on:

- Controllers and processors
- Contracts and liabilities between controllers and processors
- Right of access
- Security
- Accountability

Can we collect workers' information to use for equal opportunity monitoring?

You may be under a legal or regulatory obligation to collect information about your workers to monitor equality of opportunity and prevent discrimination. This may include collecting information about workers' ethnic origin, disabilities, religion, or sexual orientation.

In Northern Ireland, section 75 of the Northern Ireland Act 1998 requires public authorities to monitor and promote equality of opportunity between people of different religious belief, political opinion, racial group, age, marital status or sexual orientation.

This type of information will often be special category information, which you **must** handle especially carefully. You **must** make sure that you do not use information you collect to monitor equality of opportunity for any other purpose. See 'What conditions for processing special category information might apply?'

Where possible, you **should** anonymise this information. When collecting this type of information from job applicants, you **should** make sure that you can separate it from any identifying information about the job candidate, so that you can save it anonymously as statistical information.

Be aware that equal opportunity monitoring information might potentially identify particular workers, even if the names have been removed. For example, if it makes reference to a characteristic shared by relatively few of your workers. In this case, you **should** make sure that any staff with access to this information are aware of its sensitivity and the need to keep it secure and confidential.

You **should** make sure that your equality monitoring questions are designed so that the personal information you collect is accurate and not excessive. You **should** ask questions that allow workers to identify themselves accurately. For example, in ethnic origin monitoring, do not limit the range of choices given so that workers are forced to make a choice that does not properly describe them.

Further reading

- Special category data
- Anonymisation guidance when published

Can we use employment records to detect fraud?

You may receive a request for your workers' personal information from external organisations tasked with preventing or detecting fraud. They may ask for your workers' records to check, for example, that they are not receiving benefits they aren't entitled to. This can involve electronic comparison of data sets held for different purposes to identify inconsistencies or discrepancies which may indicate fraud. This is known as data matching.

You **must** only share personal information from your workers' employment records for fraud detection purposes if:

- you are required by law;
- you believe that failure to disclose in this specific case is likely to prejudice the prevention or detection of crime; or
- your workers' employment contracts allows you to share information in such cases.

If you are using your workers' personal information for fraud prevention or detection purposes, you **must** inform new workers about this. You **should** also give existing workers periodic reminders. The only exemption from this is when informing a worker would be likely to prejudice the prevention or detection of crime, for example by tipping off the worker that they are under investigation for suspected fraud.

Further reading

We have a data sharing page which includes guidance on data sharing, such as sharing personal data with law enforcement authorities, as well as the full data sharing code.

Other resources

The Cabinet Office has produced a Data matching code of practice.

What do we need to consider when using pension and insurance schemes?

Most workplace pension and health insurance schemes are run by third-party organisations. You **must** comply with your data protection obligations when you are sharing information about your workers with these organisations.

You **must** make sure that when a worker joins a health or insurance scheme, you make them aware of what personal information you will share with the scheme provider, and how it will be used.

You **must** make sure that you do not share more information with the provider than is necessary to run the scheme.

If you are sharing information with the provider about workers' sickness or injury records, or other health information, you **must** identify both a special category condition and a lawful basis. See 'What conditions for processing special category information might apply?', as well as our separate guidance on information about workers' health.

You **must not** access any personal information you collect on behalf of the provider to run the scheme and use it for general employment purposes. You **should** ensure that the only people in your organisation who have access to this information are those who need it to run the scheme. You **should** make them aware of their data protection responsibilities, and that they **must not** use the information for other employment purposes.

Further reading

See our detailed guidance on Special category data.

How do we handle employment records during mergers and acquisitions?

You may need to share personal information about your workers with another organisation as part of a takeover or other situation involving a change in organisational structure. For example, an acquisition, merger or insolvency. This may take place during the evaluation of assets and liabilities prior to the final merger or acquisition decision.

You **must**:

- consider information sharing as part of your due diligence;
- establish what personal information you're transferring, why you have it in the first place, and your lawful basis for sharing it;
- if you are transferring any special category information, identify a special category condition;
- comply with the data protection principles – especially lawfulness, fairness and transparency;
- tell your workers that there has been a change of circumstances, and remind them about their information rights; and
- document your actions and decisions.

Wherever possible, if you are sharing workers' information with another organisation in connection with a prospective acquisition, merger or business reorganisation, you **should** anonymise the information.

During negotiations, you **should** carefully assess any request for personal information from the other organisation. Prior to any final merger or acquisition decision, you **should** only hand over your workers' personal information once you have been assured that they will:

- use it solely to evaluate assets and liabilities;
- treat it in confidence and not disclose to other parties; and
- destroy or return it after use.

If possible, you **should** tell workers if you are going to share their employment records with another organisation before an acquisition, merger or business reorganisation takes place.

If the acquisition or merger takes place, you **should** make sure your workers are aware of the extent to which you are transferring their employment records to the new employer.

In some circumstances, 'insider trading' or similar restrictions will apply. For example, if providing an explanation to workers would alert them to the possibility of a takeover of which they would otherwise be unaware, and could thereby affect the price of a company's shares. In such circumstances, you may not have to explain to workers that you are sharing their personal information for the purposes of evaluating assets prior to acquisition.

As a new employer, you have all the same obligations about workers' information as their original employer did. You **must** make sure that records you hold as a result of a merger or acquisition are accurate, up-to-date and relevant, and do not include more personal information than necessary.

Further reading

- Anonymisation
- Privacy enhancing technologies

Other resources

The Financial Conduct Authority has produced a best practice note on identifying, controlling and disclosing inside information.

When can we share workers' information under the Transfer of Employment Regulations?

In the case of some mergers or acquisitions, you may be legally required to share certain information under the Transfer of Employment Regulations 2006 (TUPE).

The TUPE Regulations are designed to preserve employees' terms and conditions of employment when:

- an organisation (or part of it) is transferred to a new owner or employer, (eg by sale or merger); or
- a 'service provision change' occurs, such as when a service is transferred to a new provider, but the client remains the same.

Under the TUPE Regulations, the outgoing employer is required to provide the new employer with specific information about their new workforce in advance of any business transfer or change in service provision. This is known as 'employee liability information'. It includes:

- the identity (usually the name) and age of the transferring employees;
- information contained in their 'statements of employment particulars', such as a written statement of pay, hours of work and holidays (usually contained in the employee's offer letter or contract of employment);
- information about any collective agreements;
- information about any grievance procedure taken by an employee within the last two years;
- information about any disciplinary procedure taken against an employee within the last two years; and
- details of any legal action (before the court or employment tribunal) brought against the employer by an employee in the last two years and information about any potential legal action arising from their employment.

The original employer is required to provide this information at least 28 days before the transfer is completed. If special circumstances make this impractical, you should supply it as soon as possible.

Because providing this information is a legal requirement, you can rely on the legal obligation lawful basis. You **must** still comply with data protection law when providing workers' personal information.

Be aware that some transfers are outside the scope of TUPE (such as share takeovers). Therefore, in these cases there is not a legal requirement to provide employee liability information.

Can we share more information than is required by the TUPE regulations?

A prospective employer may, as part of their due diligence, request more information than is required by the TUPE Regulations.

Also, in the early stages of the sale of a business there may be a number of potential bidders. This means that although only one will become the eventual new employer, all of them need the information to assess whether to pursue the purchase.

If you need to share personal information about workers that falls outside the scope of employee liability information, you **must** document another lawful basis for processing. The most likely one is legitimate interests. If it includes special category information, you **must** also identify a condition for processing this.

You **should** consider carrying out a data protection impact assessment for information that falls outside the

scope of employee liability information, particularly if this includes special category information.

You **should** also consider whether you could pseudonymise any personal information not required by TUPE before sharing it.

You **must** put in place safeguards to make sure unsuccessful bidders only use information in connection with the proposed business transfer, and that they will not keep it once they have used it for this purpose.

Can we give employment records to the new employer?

Once the transfer has taken place, it is likely that the new employer will need to keep a large proportion of a worker's employment record to manage the workforce and run the business.

The new employer should consider whether they need all the information contained in a worker's employment record, and destroy unnecessary information.

Can we, as the original employer, keep personal information after the transfer?

After the transfer has taken place, it is likely that the original employer will need to keep some personal information about former employees (eg to deal with any liabilities).

Data protection law allows this, but you **must** have a justifiable reason to keep this information, and only keep it for as long as necessary.

Further reading

ACAS has published guidance on Transfer of Undertakings (TUPE).

Checklists

Our consultation on this draft guidance is open until 5 March 2024.

Collecting and keeping employment records

☐ We give new workers privacy information to tell them what information we will collect about them, how we will use it, and who we will disclose it to.

☐ We remind existing workers about how to find our privacy information.

☐ We inform new and existing workers of their rights under data protection law, including their right to access the information we keep about them.

☐ We make sure that we only collect personal information that is necessary for our purposes.

☐ We ask our workers to regularly check their information to make sure it is accurate and up-to-date, and make any changes where necessary.

☐ We identify and document a lawful basis for collecting and using workers' personal information.

☐ We make sure that only those staff that need it have access to workers' records.

☐ If we want to collect special category information from our workers, we identify a special category condition (under Article 9 of the UK GDPR).

☐ If we want to collect criminal offence data, we identify a condition for processing under Schedule 1 of the DPA 2018.

☐ We dispose of worker records securely and effectively when we no longer need them.

☐ We periodically review the personal information we hold on our workers, and erase or anonymise it when we no longer need it.

☐ We have clear retention policies in place setting out how long we keep different categories of our workers' personal information.

Outsourced employment functions

☐ We have written contracts with the processors we use if we outsource any of our employment functions. These require the processor to only use workers' personal information in line with our

instructions, and to maintain appropriate security.

☐ We make sure that the contract states that the processor can only use workers' personal information in line with our instructions.

☐ We make sure that the contract states that the processor must maintain appropriate security, including technological and organisational measures.

Equality monitoring

☐ We have identified and documented a special category condition for collecting information about workers' ethnicities, religion, disability or sexual orientation.

☐ Where possible, we anonymise personal information we collect for equality monitoring purposes.

☐ We make sure that we don't use the information we collect for equality monitoring for any other purpose, and that staff with access to this information are aware of their data protection responsibilities.

Pension and insurance schemes

☐ We inform workers about what the scheme involves.

☐ We make sure that we do not share more information with the provider than is necessary to run the scheme.

☐ We make sure that workers are aware what personal information we will pass to the scheme provider.

☐ If we are sharing information with the scheme provider about workers' sickness or injury records, or other health information, we have identified a special category condition and documented this.

☐ We make sure that the staff involved in collecting information for this purpose are aware of their data protection responsibilities.

☐ We make sure that only the people in our organisation who need to help run the scheme have access to the personal information we collect for this purpose.

Mergers and acquisitions

☐ We consider sharing personal information about workers as part of our due diligence.

☐ We agree what information we should transfer, and how, before a transfer takes place.

☐ We tell our workers when there is a change in circumstances that affects who is responsible for their personal information.

☐ Where possible, we tell workers if we will share their employment records with another organisation before an acquisition, merger or business reorganisation takes place.

☐ We tell our workers about which parts of their employment records we will transfer to the new employer.

☐ We make sure those responsible for negotiating the transfer of staff are aware of their responsibilities to comply with the data protection principles (eg to keep personal information up-to-date and secure).

☐ Where applicable, we transfer enough information to meet TUPE obligations and to allow the new employer to run the business and manage the staff.

☐ We don’t transfer excessive and irrelevant information.