

About this guidance	2
Data protection and recruitment	4
Responsibility for data protection compliance during the recruitment process	27
Finding candidates	35
Automated decision-making and profiling for recruitment and selection	37
Information provided by candidates	48
Shortlisting, testing, and interviewing candidates	53
Verifying candidates	56
Pre-employment vetting of candidates	58
Keeping recruitment records	64
Recruitment and selection impact assessment summary	68

# About this guidance

Our [consultation on this draft guidance](#) is open until 5 March 2024.

## In detail

- [Who is this guidance for?](#)
- [What are the key definitions?](#)
- [How is this guidance structured?](#)
- [How do we use this guidance?](#)

## Who is this guidance for?

This guidance is aimed at employers and organisations which carry out recruitment on behalf of employers, such as recruitment agencies, head-hunters or consultancies. It covers recruitment in the context of all potential employment relationships, including employees, contractors, volunteers or gig and platform workers.

As an employer or recruiter, you are likely to process information for the purpose of recruitment and selection about candidates, prospective candidates, temporary workers, contractors, referees, emergency contacts, and dependants. Some of this information may be sensitive and include, for example, details about health, diversity, or criminal convictions.

The labour market supply chain can be complex, with end-to-end recruitment processes often involving several organisations. The use of novel technologies in recruitment processes means that organisations are processing increasingly large amounts of information about people.

This guidance is designed to help employers and recruiters understand their data protection obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) (we refer to these as data protection law) when handling the personal information of candidates.

The guidance aims to:

- help provide greater regulatory certainty;
- protect candidates' data protection rights; and
- help employers and recruiters carry out effective recruitment exercises in compliance with data protection law.

We also provide links to other pieces of key data protection guidance if you want to find out more information.

## What are the key definitions?

The terms 'recruitment', 'recruitment process' and 'recruitment and selection' are used throughout this guidance to refer to the process of identifying, selecting, verifying, and vetting candidates.

The term 'candidate' is used throughout this guidance to refer to a person who has either applied for work or has been identified through a selection process or talent search.

The term 'recruiter' is used throughout this guidance to refer to a recruitment agency, head-hunter or consultancy, other than the employer itself, which is involved in the headhunting, recruitment and selection of candidates.

## How is this guidance structured?

This guidance covers all aspects of the recruitment and selection process from advertising vacancies through to deleting information about candidates. It has two main parts:

- The first section, Data protection and recruitment, is an overview of how data protection law applies to processing candidates' information for recruitment purposes. It looks at the data protection principles and the basics for compliance.
- The rest of the guidance focuses on the specifics of the recruitment process in which you process candidates' information. It looks at what the law requires you to do and provides good practice advice.

While we recommend that you read the guidance in full, you can choose which parts of the guidance you read to fit your needs.

## How do 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.

# Data protection and recruitment

Our [consultation on this draft guidance](#) is open until 5 March 2024.

## In detail

- How do we use information about candidates fairly during the recruitment process?
- How do we use information about candidates lawfully during the recruitment process?
- What lawful bases might apply if we want to process candidates' information?
- What special category conditions might apply?
- Do we need to tell candidates about how we are using their information?
- What do we need to tell candidates if we are a recruiter?
- Do we have to explain our purpose for using candidates' information?
- How do we limit how much information we collect during the recruitment process?
- How do we keep candidates' information accurate and up-to-date?
- How do we keep candidates' information secure?
- How long can we keep candidates' information?
- Do we need to make reasonable adjustments in the recruitment process?
- Can we transfer candidates' information internationally?
- When do we need to carry out a Data protection impact assessment (DPIA) for recruitment purposes?
- What rights do candidates have over their information?

## How do we use information about candidates fairly during the recruitment process?

It's important that you collect and use information about candidates in ways that are fair and proportionate. You **must**:

- be clear about what information you are collecting and how you will use it for recruitment purposes; and
- only collect information that is relevant and necessary for recruitment. For example, you may need to ask candidates about their academic qualifications and previous work experience, but not whether they have dependants or not.

You **should** ensure that decision-makers are not presented with irrelevant information about the candidate before they make their decision.

### Example

---

An organisation's online application form automatically assigns a reference number to each candidate.

Two staff members screen the application forms to remove irrelevant personal details, such as the candidate's name, contact details and equality information. They then send the information about their qualifications and work experience to decision-makers for shortlisting.

It's important to consider when to ask for certain information. You **should**:

- avoid asking for personal information at the start of the recruitment process if you don't need it until later on. For example, if you only need a copy of the successful candidate's degree certificate, it's not fair to ask all candidates to provide this; and
- carefully consider whether it's fair to get information about candidates from other sources. In most circumstances, it is only appropriate to vet the candidate who is offered the job.

In general, you **should not** use information:

- in ways the candidate would not reasonably expect;
- which you have not told them about; or
- which may have adverse effects for them.

However, if you use a candidate's information to decide not to shortlist them for a job, this is fair, reasonable, and not unexpected, even though they may view it as an adverse effect.

## How do we use information about candidates lawfully during the recruitment process?

You **must** identify a lawful basis in order to lawfully collect and use information for recruitment purposes. There are six to choose from. You **must** identify the lawful basis that is appropriate for each type of processing activity you intend to do at each stage of the recruitment process, and which reflects the context and nature of the information.

In each case, you **must** determine your lawful basis before you begin your processing, and document it.

Using information lawfully also means that you don't do anything with candidates' recruitment information which would potentially breach other laws. For example, you **must** ensure that you do not breach a duty of confidence, other legislation, or regulations you are required to comply with.

Below we set out the lawful bases that are most likely to apply when you are using candidates' information for recruitment purposes.

### Further reading

- [Lawful basis guidance](#) and [interactive guidance tool](#)
- [Lawfulness, fairness, and transparency](#)

## What lawful bases might apply if we want to process candidates' information?

Below we've listed some of the lawful bases most relevant to recruitment, and explained when they may apply. We've also explained when it may not be appropriate to rely on a specific lawful basis for processing

candidates' information.

## Legitimate interests

You can rely on this basis if the processing is necessary for your legitimate interests or the interests of a third party. However, you cannot rely on this basis if the need to protect the candidate's interests, rights and freedoms outweighs those legitimate interests.

This basis is likely to be relevant in many recruitment contexts. For example:

- collecting and reviewing information on application forms or CVs;
- shortlisting candidates;
- collecting new information at interview;
- collecting information at assessments; and
- verifying candidates.

You **should** carry out a legitimate interests assessment if you plan to rely on this basis.

### Example

A charity has selected a number of candidates to interview for a public-facing role. As part of the selection process, it decides to do manual searches of candidates' public social media profiles, to ensure that it does not employ someone whose behaviour is inconsistent with the values of the organisation, or would compromise the person's ability to do their job.

The charity has informed candidates that public social media checks will be used as part of the recruitment and selection process. Candidates will be asked about their social media use at interview, and have an opportunity to answer questions or address concerns. The charity relies on legitimate interests to carry out this processing. It applies the three-part test:

1. The charity has a legitimate interest in ensuring that a candidate's public persona does not compromise its values or work, and that the person they employ is suitable and capable of doing the job.
2. It is necessary to screen the candidate's public social media use, as the role is public-facing and their public social media profile is relevant.
3. The processing may carry high impacts as it may prevent someone from being employed. However, the charity depends on both public and private funding, and it considers the extent to which it needs to take these steps to safeguard its reputation and ensure that those it employs respect and uphold its values. The charity **must** decide whether, on balance, the checks are necessary and proportionate, taking into account all the circumstances.

You are not required to carry out a separate legitimate interests assessment for each candidate, as long as your reasons for processing information about each candidate are the same, and the information they provide is broadly similar in nature.

## Example

A call centre receives a large number of applications for vacancies. It decides to shortlist candidates on the basis of legitimate interests. It carries out a general legitimate interests assessment for this processing and considers the following points:

- The candidates have been asked to provide similar information about their qualifications, experience, and contact details.
- It is necessary to shortlist candidates to carry out an effective recruitment exercise.
- The call centre applies the same criteria in reviewing each application.
- This process benefits candidates and the organisation.
- The candidates have a right to know if they have been shortlisted or not.
- Some candidates will be eliminated from the process and can no longer be considered for the role. However, this is a necessary and foreseeable part of the recruitment process. It will not prevent the eliminated candidates from applying for future roles with the organisation and therefore the impact is minimal.

However, this basis is unlikely to be relevant if you are using the information in ways the candidate might not reasonably expect or you are under a legal obligation to process the information.

## Further reading

- [Legitimate interests](#) and in particular the section [How can we apply legitimate interests in practice?](#)

## Consent

You can rely on a candidate's consent to process their information if:

- their consent is freely given and unambiguous;
- they have complete control over their information;
- their consent includes an affirmative action;
- their consent is specific and granular; and
- they can withdraw their consent at any time without detriment.

An affirmative action means that a candidate expressly consents to you using their information for a specified purpose. This means they need to 'opt in' to the processing. For example, by ticking a box to say they expressly agree to you using their information for a particular purpose. However, just because a candidate submits an application form for a vacancy, does not mean they have given their express consent to you using their information – even if you think it's obvious they want to be considered for a particular vacancy.

Consent needs to be specific and granular, which means that you **must** obtain a candidate's separate

consent for each processing activity. Candidates may feel that they have no choice but to give you consent in order to be considered for a job. As there is likely to be an imbalance of power between the candidate and the employer or recruiter, consent is unlikely to be an appropriate lawful basis to use at most stages of the recruitment process.

You **must not** rely on consent unless you are confident that you can show that it was freely given.

You **must not** rely on consent in order to consider a candidate for multiple roles, or future roles, as their consent will not be specific, granular and informed. This means that it's unlikely that recruitment agencies will be able to rely on a candidate's consent for processing their personal information in such circumstances. Instead, recruitment agencies are most likely to rely on the legitimate interests basis.

You **must** make it easy for a person to withdraw their consent. If a person withdraws their consent, they will also withdraw from the recruitment process. This is a reasonable outcome, and not unexpected or unduly detrimental.

However, you **should not** rely on consent if you would process the information anyway, using another lawful basis, or if relying on consent would be misleading or unfair.

### Example

A bank makes a conditional job offer subject to receiving the following from the candidate:

- a clear criminal records check; and
- evidence of their right to work in the UK.

It's not appropriate for the bank to rely on consent for this vetting and screening. This is because it needs to carry out these checks before the candidate starts work. Even if the candidate refuses to give consent, the bank will use another lawful basis to process this information.

### Contract

You can rely on this basis if using the candidate's information is necessary:

- to perform a contract of employment; or
- because the candidate has asked you to take specific steps before entering into a contract of employment (eg they have accepted your job offer).

In the context of recruitment you can only rely on this basis once you have made the candidate a conditional or unconditional job offer and they have accepted your offer. This is the case, even if they have not yet entered into the contract. In this guidance, we refer to this as the 'pre-contractual stage'.

Therefore, you **should not** rely on this basis at the earlier stages of the recruitment process to shortlist, test, or interview candidates.

As an employer, you may only rely on this basis if processing the candidate's information is necessary to enter into a contract with them. This means it needs to be a targeted and proportionate means of achieving



your objective in the recruitment process. This might be the case if you require evidence of a candidate's academic or professional qualifications once you have made them a conditional offer of employment and they have accepted your offer.

### **Example**

Following a successful interview, a candidate receives a provisional offer for a specialist role within an IT firm, which they accept. The firm relies on the contract lawful basis to obtain evidence of the candidate's degree and professional IT qualifications at the pre-contractual stage, with the intention of entering into a contract of employment with them once these documents have been verified.

However, if the contract does not occur or the candidate changes their mind and no longer wishes to accept the job offer, you **must** immediately stop processing the information.

This lawful basis is unlikely to be appropriate for the majority of the recruitment and selection process, and you may need to carefully consider whether another lawful basis may be more appropriate in the circumstances.

As a recruiter, you may rely on this basis for processing if:

- you have a contract in place with the candidate; and
- that contract clearly sets out that you will process personal information for the purposes of fulfilling your obligations under the contract.

### **Example**

A recruitment agency is used by an events company to find temporary festival staff. It identifies and shortlists relevant candidates for the temporary positions.

Although successful candidates undertake work for the events company, they are directly employed by the agency. The agency is responsible for recording the hours worked by each temporary staff member and paying their weekly wages.

Once all successful candidates accept the offer of temporary festival work, they enter into a temporary working contract with the agency. The agency relies on the contract lawful basis in order to fulfil the terms of their contract with candidates, which include paying each person directly for the hours they have worked for the events company.

## **Legal obligation**

This basis applies if the processing is necessary for you to comply with the law. You can rely on this basis where you are processing a candidate's information to comply with a common law or statutory obligation.

You **should** have a clear basis in law for the processing.

It may be relevant when:

- carrying out right to work checks on people before employing them, to ensure that they are legally entitled to work in the UK;
- carrying out enhanced vetting checks on social workers; or
- you need to recruit more people from ethnic minorities to comply with your statutory equality duties, provided that there is a legal basis for the processing (eg section 149 of the Equality Act 2010, the Fair Employment and Treatment (Northern Ireland) Order 1998, or section 75 of the Northern Ireland Act 1998)).

You **must not** rely on this basis if you have discretion over whether or not to carry out the processing, or there is another reasonable way to comply.

### **Public task**

You may rely on this basis for recruitment if the processing is necessary for you to perform a task in the public interest or for your official functions. You **must** have a clear basis in law for the task or function.

Public task often relates to a public authority's discretionary powers. It may be relevant where you need to recruit more people from ethnic minorities to comply with your statutory equality duties (although you can also rely on legal obligation – see the above section).

### **What special category conditions might apply?**

You are likely to use special category information for recruitment in order to carry out:

- reasonable adjustments at any stage of the process (eg designing an accessible application form, or providing an accessible testing or interview room);
- equality monitoring;
- pre-employment vetting (where required); and
- fitness to work checks.

Special category data is personal information revealing or concerning:

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

It needs more protection because it is sensitive and the risks of harm to the person from its inappropriate

---

disclosure or use are likely to be higher. In particular, if this impacts a person's right to work or be considered for a specific vacancy.

If you are processing special category information, you **must** have a special category condition as well as a lawful basis. There are 10 conditions for processing special category data to choose from. For five of these, you **must** meet additional conditions and safeguards set out in Schedule 1 of the DPA 2018. You may also be required to carry out a data protection impact assessment (DPIA) before you begin.

Remember that you **must** determine your special category condition before you begin the processing. You **must** document your decision, along with your lawful basis.

It may also be possible for you to infer or guess details about a candidate that fall within the special categories of information during the recruitment process. For example, you may be able to infer a candidate's race or ethnic background from the information they have provided to you within a job application form. Where such an inference is being made about a candidate, you are processing special category information. This is the case whether your inference about a candidate is correct or not. You **must** therefore have a special category condition, as well as a lawful basis for the processing.

In certain circumstances, you may capture special category information incidentally, when you're not planning to collect it. If you are likely to capture special category information, you **should** identify a condition to cover this.

### Further reading

- [What are the conditions for processing?](#)
- [Special category data - What about inferences and educated guesses?](#)
- [Data Protection Impact Assessments \(DPIAs\)](#)

## Appropriate policy document and safeguards

Some of the conditions require you to have an [appropriate policy document](#) in place and also apply the following safeguards to protect the person's rights and freedoms:

- Keep the appropriate policy document from the time you begin processing the personal information under this condition until six months after you stop using it (you **must** then destroy or anonymise the information).
- For as long as you retain the appropriate policy document, you **must** review and update it, as required, and provide a copy to the ICO on request.

Below we discuss some of special category conditions most relevant to recruitment (and explain when you are required to have an appropriate policy document and safeguards):

## Explicit consent

You can only rely on this condition if candidates have full control and choice over the processing. Explicit consent is not specifically defined in data protection law but is similar to the lawful basis of consent. To rely on this condition, you **must** ensure that:

- candidates affirm their explicit consent in a clear statement (whether written or oral);
- you have specified the nature of the special category information you are using (eg whether this relates to health, race, or a number of categories); and
- it is separate from any other consents you seek.

You **must** give candidates a genuine choice to give you their special category information, with no negative impact (either actual or perceived) if they choose not to. It may be helpful to refer to the earlier section on consent which explains why consent has limited use in the recruitment process.

While there may be some limited circumstances where this condition can apply, you **should not** collect special category information in the course of the recruitment process unless you can show that it is absolutely necessary.

### Example

A construction company needs to ensure that the people it employs are fit to work. However, it doesn't need this information in order to shortlist, assess or interview candidates. In fact, the employer only requires this information from the successful candidate. Therefore it would be unreasonable to ask each candidate to supply medical evidence to prove they are fit to work during the recruitment process.

The employer explains on the application form that it will collect this information from the successful candidate after they have made them a conditional offer.

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

You can rely on this condition if you need to process the information to comply with employment law or social security and social protection law. You **must** 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 industry guidance that explains generally applicable employment obligations or rights.

If you are relying on this condition, you **must** also meet the associated condition set out in Part 1 of Schedule 1 of the DPA 2018. This condition requires you to have an [appropriate policy document and safeguards](#) in place.

For example, if your right to work checks are likely to capture special category information, you **must** select a special category condition. You can rely on the Employment, social security and social protection condition as you are processing the information to fulfil an obligation set out in law.

This condition does not cover processing to meet purely contractual employment rights or obligations. For example, entering into an employment contract with the candidate.

### Information manifestly made public by the candidate

Data protection law provides that you may use special category information about people if it is clear that the person has willingly and deliberately made this information publicly available. For example, by regularly

blogging about it. However, just because a candidate has deliberately made their special category information publicly available does not mean it's fair or lawful to use it for recruitment purposes. Candidates are unlikely to expect you to use their information in this way.

### Example

A retailer checks a candidate's public social media profile when deciding whether they are suitable for a marketing job. It discovers that the candidate has a disability. The candidate blogs frequently about living with their disability to try and improve understanding of their condition and help others.

As the candidate has clearly made this information about themselves public, this condition applies. However, the retailer **must** still comply with the data protection principles, and it would be unfair for them to use this information to decide if the candidate is suitable for the role. The candidate shared this information to help improve awareness about living with a disability and will not expect the retailer to use it to decide whether they are suitable for a vacancy.

You **should not** make assumptions about a person's suitability for a particular role based on their special category information (eg their race, political views, sexual orientation, or gender). This is the case even if the person has deliberately made this information publicly available. However, if you consider this information to be significantly relevant to the role you are recruiting for, you can still use it as long as you do so fairly. For example, by giving candidates an opportunity to explain or comment at interview. For more details, see the chapter on [Shortlisting, testing and interviewing candidates](#).

If you actively need to recruit people with protected characteristics to address unfairness or underrepresentation within your organisation, you **should** follow your existing recruitment processes. For example, by asking candidates to provide equality monitoring information. You **should not** rely on this condition for using special category information you find online to make recruitment decisions about candidates. This is the case even if the candidate has deliberately and clearly made this information publicly available. You may still be in breach of the fairness principle if you use information irresponsibly and where it is clearly inappropriate. For example, where it may have detrimental impacts or exploit a person at risk of disadvantage or harm.

### Substantial public interest

This condition may be relevant if the processing is:

- required on grounds of substantial public interest;
- based on UK law; and
- proportionate to the aim you want to achieve.

If you rely on this, you **must** have specific measures in place to safeguard the person's fundamental rights and interests. This means you **must** have an appropriate policy document and safeguards in place. Read the earlier section of this guidance which gives more detail about putting in place an [appropriate policy document and safeguards](#).

The relevant basis in UK law is set out in section 10(3) of the DPA 2018. This means you **must** meet one of 23 substantial public interest conditions set out in Schedule 1 (at paragraphs 6 to 28).

Any of these substantial public interest conditions may be relevant in the context of recruitment. However, two of them are particularly relevant, and we discuss them in more detail below. They are:

- equality of opportunity or treatment; and
- racial and ethnic diversity at a senior level in organisations.

### Further reading

- [Special category data – what are the conditions for processing?](#)
- [What are the substantial public interest conditions?](#) and the section [What is an appropriate policy document?](#)

## Equality of opportunity or treatment

This condition is met if you're using information that is necessary for monitoring equality of opportunity or treatment of candidates in the following categories:

- people of different racial or ethnic origins;
- people holding different religious or philosophical beliefs;
- people with different states of physical or mental health; or
- people of different sexual orientation.

You can only use this information for promoting or maintaining equality of opportunity between the above groups. This means that you can ask candidates to provide you with their special category information, as long as you tell them what you will use it for. For example, you **could** ask candidates to provide equality monitoring information in response to a recruitment campaign to ensure that your workplace is fair.

However, the equality of opportunity or treatment condition does not apply if:

- your processing relates to decisions or measures about a particular person;
- your processing is likely to cause substantial damage or substantial distress to any person; or
- a person gives you notice not to use their information or to stop using their information within a reasonable time period.

You **must** have another lawful basis and special category condition to be able to take action where, for example, your monitoring reveals discrimination about one person. In these circumstances, you may rely on the employment, social security and social protection condition instead.

## Racial and ethnic diversity at a senior level in organisations

This condition allows you to use information about a person's race or ethnicity, in particular circumstances, for the purpose of recruiting ethnically diverse people for senior roles. It applies only where the processing is:

- about information concerning race or ethnicity;
- carried out as part of a process of identifying suitable people to hold senior roles; and
- necessary to promote or maintain racial or ethnic diversity at senior levels in organisations.

Senior roles can include:

- senior managers (those who make organisational or managerial decisions);
- directors;
- company secretaries; or
- partners.

This condition means that, where necessary, you may take into account information about a candidate's race or ethnicity for the purpose of recruiting enough ethnically diverse people into senior roles, even if you don't have their consent. However, you **must not** use this information for any other purpose.

### Further reading

- [What are the conditions for processing special category data?](#)

Do we need to tell candidates about how we are using their information?

Data protection law requires transparency. Candidates have a right to be informed about how you use their information. This is called privacy information. You **must** provide them with certain details including:

- your purposes for processing;
- how long you will keep their information; and
- who you will share it with.

You **must** provide privacy information at the time you collect personal information from the candidate. For example, in your job advert or in your application form.

You **must** provide candidates with privacy information within a reasonable period, and no later than within one month, if you obtain personal information about them from other sources.

If you receive anonymised information about a candidate from a recruiter, you **must** give them your privacy information before you collect their personal information.

If you receive information about a candidate but you do not wish to consider them for a vacancy (eg where a candidate or a recruitment agency provides a CV), you **must** delete their information as soon as possible.

You **must** provide these details even if you think it's obvious how you will use the person's information. You can satisfy this requirement by including a link to your privacy information.

Depending on the nature of the role, you may need to provide further information to candidates. For example:

- where special checks are required (eg safeguarding, disclosure of spent convictions);

- the circumstances in which it may be an offence to apply for certain roles (eg where a person is on the childrens' barred list);
- your verification and vetting procedures, including at what stage this will be carried out; or
- whether and when you will seek information from third parties, in addition to references the candidate has provided.

You **must** tell candidates how long you will keep their information for, including whether you plan to keep it to consider them for future vacancies. If you're not able to tell them this, you **must** at least be able to tell them what criteria you will use in deciding how long to keep their information for.

You **should not** use the person's information in ways they would not reasonably expect. If you plan to use their information for reasons not linked to recruitment, you **must** inform them and have a lawful basis for your processing.

If you are using automated decision-making and profiling, there are additional rules about what privacy information you **must** provide. This is covered in our chapter on [Automated decision-making and profiling for recruitment and selection](#).

## What do we need to tell candidates if we are a recruiter?

In general, if employers use a recruiter to find potential candidates, the recruiter is responsible for advertising the vacancy, not the employer.

If you are a recruiter acting on behalf of an employer, you **must** provide your name and contact details, and explain how you use and disclose the personal information you receive, even if you consider this to be self-evident.

You are not required to provide the name and contact details of the employer at the beginning of the recruitment process. However, you **must** inform any candidates about the employer's identity as soon as reasonably practicable, if their applications are to be pursued further by the employer. Or, at the latest, when the employer first obtains the personal information.

You **must** limit any candidate information you disclose to an employer to what is relevant to the recruitment decision being made at that particular stage in the process.

If you have not provided an employer's identity to the candidate, you **should only** send anonymised candidate information to the employer.

### Further reading

- Our guidance on the topic of anonymisation is currently under development. However, please see '[ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance](#)' for further information.

## Do we have to explain our purpose for using candidates' information?

Yes, you **must** be clear about what you will use candidates' information for from the start. You **should**



document and keep a record of this, and keep candidates informed.

It's likely that your main purpose for collecting and using candidates' information is to consider them for a specific vacancy. You **should only** collect the information you need for this purpose.

In some circumstances, you may wish to keep information about candidates to consider them for future vacancies. However, you **should not** keep information about candidates 'just in case' you might use it, or because you might decide to recruit more workers in future. You **should only** keep candidates' information if this is fair. This means that you:

- genuinely intend to use the information;
- informed candidates about this; and
- explained how long you will keep their information for.

### Example

An accountancy firm receives a large number of applications for three vacancies. However, it plans to recruit more staff within the next six months, although it is not sure how many yet. The firm decides to keep information about the highest scoring candidates who have been unsuccessful this time because it is reasonably certain that it will recruit some or all of them in the future.

The firm documents this purpose as part of their business plan and explains this to candidates from the start of the recruitment exercise. It also explains that it will only keep the candidates' information for six months.

### Example

A recruitment agency advertises an administrative assistant job role on behalf of a client organisation. The agency receives a large number of applications.

Whilst the agency recommends the majority of these applications to the client, it considers that several candidates would be more suitable for other roles it is currently recruiting for.

If the agency wishes to use certain candidate applications for other roles, it **must** have a clear lawful basis for this processing when it initially collected this information. It **must** also include this lawful basis in its privacy notice.

Alternatively, the agency **could** seek the consent of candidates prior to additionally processing their applications for a different purpose.

However, if your purposes change over time, or you want to use the candidates' information for a new purpose which you did not originally anticipate, you can only do this if:

- your new purpose is compatible with your original recruitment purpose;
- you get the candidate's specific consent for the new purpose; or
- you can point to a clear legal provision which requires or allows you to use the information in the public interest.

'Compatible' means that the new purpose is strongly linked or related in some way to your original purpose. However, the new purpose is not compatible with the original purpose if it is not related to your original purpose.

### Example

A local authority wants to use the personal information it obtained during its recruitment exercise to research the types of candidates who make applications to it. This research will help the authority comply with its equality duties. This new purpose is fundamentally different and therefore not compatible with the original purpose. In addition, candidates are unlikely to expect the local authority to use their information in this way when they applied for a role.

If you are required to use candidates' information to comply with a legal obligation, you **must** explain this in your privacy information. For example, if your organisation is part of a regulated sector, such as financial services or the solicitor's profession, you may have a duty to report fraud (eg identity theft or money laundering).

### Example

In the course of verifying a candidate's information, a bank suspects that this particular candidate has provided false documents and is using another person's identity. The bank has a legal obligation to report crimes of this nature to the police and has explained this in its privacy notice.

In most cases, you **should not** seek the consent of a candidate to use their recruitment information for a new purpose.

### Further reading

- [Documentation](#)
- See the earlier section on [Consent](#)

## How do we limit how much information we collect during the recruitment process?

You **must not** collect more information than you need to achieve your purpose. When collecting information for recruitment, you **should** tailor your application forms to ensure that candidates only provide the information you need. You **could** also make it clear what information you don't need them to provide. See the section [Information provided by candidates](#).

You **should** only collect information from candidates when you need to. This means that it's better to avoid collecting information from all candidates at the start of the recruitment process, if you only need this information from the candidate you eventually appoint. For example, as a recruiter, you are unlikely to need copies of a candidate's academic or professional qualifications until they have accepted a provisional job offer from the employer.

### Further reading

- Guidance on [Data minimisation](#)

## How do we keep candidates' information accurate and up-to-date?

You **must** take all reasonable steps to ensure the personal information you collect for recruitment purposes is not incorrect or misleading as to any matter of fact. You **must** keep candidates' information accurate and up-to-date. For example, if a candidate's contact details change, you **must** update your records. You **could** provide candidates with a contact on the application form in case they need to update their details.

If you discover that the information you have is incorrect or misleading, you **must** take steps to rectify or erase it as soon as possible. You **must** carefully consider any challenges made to the accuracy of the personal information. However, it may not be fair to change or erase a candidate's information once they have provided it for recruitment purposes.

If a candidate mistakenly provides incorrect information about their work experience or qualifications, it may not be appropriate to rectify this information where this would impact the fairness of the recruitment process.

### Example

A hospital is running a recruitment campaign for typists. It asks candidates to return their application forms by 8 March and makes it clear that late responses, or information provided after the closing date will not be considered.

The hospital receives a large number of responses by 8 March. On 10 March, one of the candidates contacts the hospital and informs it that some of the details they provided on their application form were inaccurate. In particular, they tell the hospital that they forgot to include their most recent typing qualification and used the wrong start date for their current job. They ask for these to be amended.

The hospital decides that it would be unfair to other candidates to allow someone to submit additional

details in support of their application after the closing date. So it doesn't include the candidate's most recent typing qualification.

However, the hospital think it's important that the panel know when the candidate started their current job. It attaches a note to the application form, stating that the candidate informed them on 10 March that they mistakenly entered the wrong date on the application form, and asked to correct this. The hospital are confident that this does not impact the overall fairness of the recruitment process.

If you obtain information from third-party sources, it's important that you're confident that these sources are reliable. You **should** ensure that candidates can explain or challenge any information that may not be accurate. For example, information you obtain about the candidate on their public social media profiles.

### Further reading

- Guidance on [Accuracy](#)

## How do we keep candidates' information secure?

You **must** have appropriate organisational and technical measures in place to manage risk, and protect any personal information you collect during the recruitment and selection process. This means that you **should**:

- assess the security risks;
- collect information in a way that ensures security (eg by having a secure online application system or ensuring that candidates can securely send their information using encrypted emails);
- restrict access to only those staff who require access to the information for recruitment and selection purposes, and ensure they are appropriately trained;
- store hard copies of information in locked cabinets and electronic information in secure drives;
- delete information securely and permanently in line with your retention and disposal schedule; and
- anonymise information securely and permanently.

## How long can we keep candidates' information?

Please refer to the separate chapter in this guidance on [Keeping recruitment records](#).

## Do we need to make reasonable adjustments in the recruitment process?

Yes, you **must** ensure that each stage of your recruitment process is fully accessible for disabled people.

- You **must** make your application forms available in different formats, such as large print, audio formats, email or Braille. However, if a person needs particular consideration given their circumstances, you **must** accommodate them.
- If you invite candidates to attend a test, assessment centre or interview, you **must** ensure that the test itself and the systems used to access it, as well as the premises, are fully accessible. For example, by interviewing a person who uses a wheelchair in a wheelchair accessible room.

- If there is a risk of discrimination, you **must** mitigate the risk or avoid using the software or algorithms. For example, an AI assessed video interview may discriminate against someone with a speech impairment. You **should** do an in-person interview instead.
- What is a reasonable adjustment will depend on someone's specific needs and you **must** be certain about exactly what reasonable adjustments are required. If you are unsure, you **should** communicate with the person to check (eg by speaking to them).

If someone thinks you have failed to make a reasonable adjustment, they can make a claim under the Equality Act 2010, the Disability Discrimination Act 1995 (NI) or the Fair Employment and Treatment (NI) Order 1998.

Further information about your legal obligations and how to make effective reasonable adjustments is available from the [Equality and Human Rights Commission](#) or from the [Equality Commission for Northern Ireland](#).

## Can we transfer candidates' information internationally?

Data protection law restricts the transfer of personal information to countries based outside the UK or to international organisations.

If you want to transfer information about candidates to other branches of your organisation based outside of the UK, this will not be a restricted transfer. The transfer restrictions only apply if you are sending personal information outside your company or organisation. However, if you do want to send candidate information to your branches based outside of the UK, you **must**:

- inform the candidate that you want to do this and explain why it is necessary; and
- have a lawful basis for making the transfer and a condition for processing, if this involves special category information.

If you use a third-party processor based outside the UK, the rules on international transfers apply.

### Further reading

- [International transfers](#)

## When do we need to carry out a Data protection impact assessment (DPIA) for recruitment purposes?

DPIAs are an essential accountability tool. Completing a DPIA will help you to identify and minimise the risks of any recruitment activity you might plan.

You **must** carry out a DPIA before undertaking any processing likely to result in a high risk to candidates' interests, rights and freedoms. For recruitment, this may include:

- using systematic and extensive profiling with significant effects (eg using recruitment tools to profile candidates or predict behaviour);
- using innovative technology (eg using automated decision-making or profiling or AI to help you make recruitment decisions);

- processing special category or criminal offence information on a large scale; or
- collecting personal information from sources other than the candidate, without providing them with privacy information.

It's unlikely that you would process special category or criminal offence information on a large scale for recruitment purposes. You are only likely to need this information from the candidate who is appointed, so you **should only** collect this information from the successful candidate at the end of the process. You **must** minimise the amount of personal information you collect. However, you **should** consider doing a DPIA if you are processing criminal conviction information or other highly sensitive information, including about candidates at risk of disadvantage, even if this isn't large-scale.

Even if there is no specific indication of likely high risk, you **should** do a DPIA for any new recruitment project which involves using personal information. While you are not required to do a DPIA for every recruitment campaign, you **must** do so if you have changed your processes in ways that are likely to result in a high risk to candidates. For example, if you decide to use AI software to help you make recruitment decisions about candidates. If your recruitment processes change, you **must** review and update your DPIA accordingly.

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

### Further reading

- [DPIAs](#), especially the subsection [When do we need to do a DPIA?](#)
- See also the subsection [Do we need to consult the ICO?](#)
- [Data protection officers](#)
- [Data protection impact assessments](#)
- Read our [checklists](#) to help you screen for the need to do a DPIA exercise.

## What rights do candidates have over their information?

Candidates can exercise certain rights over the information you hold about them. These are set out below:

### Right of access

Candidates can make a subject access request (SAR) for their personal information. They are entitled to access and receive a copy of their information, including any outcomes or results relating to them at all stages of the recruitment process. If you receive a SAR you **should** consider the following:

- Did you obtain the information directly from the candidate? This does not mean they already have a copy of it (eg they may request a copy of their online application form if they do not have this). However, it's helpful to ask the candidate to clarify what information they want and to check whether they already have the information you hold.
- Did you obtain information from other sources (and not directly from the candidate)? If so, you **must** provide this information unless you can rely on an exemption (eg if a reference has been provided in confidence, you are not required to disclose it).

- Does the information relate to both the candidate making the request and other people (eg other candidates or your staff)? If so, you **should** carefully consider the circumstances in deciding whether you can disclose the information.

### Further reading

- [Subject access request Q and As for employers](#)
- [Right of access](#) and in particular the sections on:
  - [Confidential references](#)
  - [Can we clarify the request?](#)
  - [What should we do if the request involves information about other individuals?](#)

## Right to rectification

You **must** rectify inaccurate personal information about candidates and complete any incomplete personal information you hold about them when you become aware of the inaccuracy, or they request this.

This right applies at any stage before, during or after the recruitment process. You **should** have systems in place which allow you to amend or change information at any stage in the recruitment process.

However, candidates are responsible for ensuring that the information they provide for recruitment purposes is accurate. If a candidate has provided inaccurate information on their application form and asks you to amend it, it may not be appropriate to comply if this would impact the fairness of the recruitment process. However, you **must** still consider any request for rectification carefully. For example, it may be appropriate to update a candidate's contact details. See the above section, [How do we keep candidates' information accurate and up-to-date?](#)

If you have made a factual error, this is something that you **must** rectify. However, if the candidate disagrees with your opinion or decision, it is sufficient to note their concerns and the fact they disagree. If they wish to appeal any decision, they can use your normal procedure as outlined in your recruitment policy.

### Example

A recruitment agency is asked to conduct initial stage candidate interviews on behalf of a client organisation. The agency agrees to make notes on each candidate interview and provide these to the client once all interviews are completed.

A candidate subsequently requests a copy of their interview notes from the agency. As they disagree with some of its contents, the candidate requests that the agency amends a section of the interview notes to reflect their recollection of events.

After reviewing the disputed section of the candidate's interview notes, the agency is satisfied that the information is accurate. This is because the contents reflect the opinion of the interviewer at the time of

writing.

The agency informs the candidate that they are satisfied the interview notes are accurate and that they will not be amending the information. However, the agency agrees to add a note to the record to explain where the candidate disagrees with its content as a matter of good practice.

#### Further reading

- [Right to rectification](#)

### Right to erasure (the right to be forgotten)

People have a right to ask you to delete the information you hold about them. This is not an absolute right, and only applies in certain circumstances.

If a candidate asks you to erase certain information about them, this may mean that you can no longer consider them for the role they have applied for. You **should** explain this to them first and check if they are happy for you to proceed.

#### Further reading

- [Right to erasure](#)

### Right to restrict processing

People have a right to restrict the processing of their information in certain circumstances. This means they can ask you to limit the use of their information, where they have a particular reason for wanting the restriction.

#### Example

A member of staff wants to apply for an internal vacancy. However, as they were involved in a personal dispute with an interview panelist's personal assistant a number of months ago, they have asked that this person does not have access to their personal information.



## Further reading

- [Right to restrict processing](#)

## Right to object

Candidates have a right to object to how you are using their information. This means they can ask you to stop using their information altogether. Candidates can only object to the processing if you are relying on either public task or legitimate interests to process their information.

You may refuse to comply with their request, although it's unlikely that you would continue to process information for recruitment purposes if the candidate has objected. This may also mean that the candidate is withdrawn from the recruitment process.

Candidates have the absolute right to object to you using their information for direct marketing purposes, including profiling for these purposes. In the context of recruitment, this is likely to mean sending adverts directly to them as part of a recruitment campaign, or profiling people to decide if they get sent the advertising. If a person objects to this, you **must** stop using their information for these purposes.

### Example

A recruitment agency has been tasked with advertising a number of IT specialist roles on behalf of a client organisation.

Using its current database of job seekers who have previously opted-in to receive job alerts, the agency searches for people with relevant IT experience using an automated filtering system. The agency uses this same system to group together and contact people that are deemed likely to be interested in or suitable for the roles.

In this case, the agency's act of grouping people together using partly-automated means to make a decision about whether to send them the job advert constitutes profiling.

Over the coming days, the agency receives requests from a number of those people objecting to its use of their information for direct marketing purposes.

The agency **must** comply with their objections to its direct marketing. However, the agency **should** put their details onto a suppression list rather than deleting them. This will allow the agency to check against this list to avoid using their information for future direct marketing purposes (including profiling) in error.

The agency may still be able to retain certain information about these people if it has a lawful basis for doing so and this complies with its established retention policies and procedures. However, if upon review the agency no longer requires this information, it **must** fully anonymise it (eg if required for statistical purposes only) or securely delete it in line with its retention policy.

### **Further reading**

- [Right to object](#)
- [Direct marketing and privacy and electronic communications](#)

### **Rights related to automated decision-making including profiling**

We explore in detail how these rights work in the context of recruitment and selection in the section [Automated decision-making and profiling for recruitment and selection.](#)

### **Further reading**

- [Rights related to automated decision making including profiling](#)

# Responsibility for data protection compliance during the recruitment process

Our [consultation on this draft guidance](#) is open until 5 March 2024.

## In detail

- [What do we need to consider if we want to work with others during the recruitment process?](#)
- [When are we a controller and what are our responsibilities?](#)
- [When are we a joint controller and what are our responsibilities?](#)
- [When are we a processor and what are our responsibilities?](#)
- [Can our status as a controller or processor change during the recruitment process?](#)
- [Are we a controller if we use job boards for recruitment purposes?](#)

## What do we need to consider if we want to work with others during the recruitment process?

Sometimes you'll want to work with others on your recruitment campaigns. You **must** be clear about who has responsibility for data protection compliance. You **should** take the time to assess and document:

- the status of each organisation as either a controller, joint controller or processor; and
- the personal information you collect, use and store in support of your recruitment and selection-related activities.

Recruiters are likely to act as controllers in most circumstances. However, if you act as a processor on an employer's behalf, you **must** have a binding written contract in place.

If you are acting as a joint controller with another organisation (eg you are the employer and someone else is the recruiter), you **must** have a transparent arrangement in place which sets out your agreed roles and responsibilities.

### Further reading

- [Controllers and processors](#)
- For more detail on when a contract is needed and why it is important, please see our guidance [Contracts and liabilities between controllers and processors](#).

## When are we a controller and what are our responsibilities?

As an employer, you will typically be a controller, as you decide what candidate information you need to collect and what you use it for.

You are also responsible for retaining or destroying the personal information of candidates in line with your established retention policies and procedures.

If you are recruiting on behalf of another organisation, you are a controller if you collect and use candidate information for your own purposes. For example, you may use candidate information in order to enter into a service agreement with a job-seeker prior to sending their application to a client organisation. You may also process the financial information of temporary workers you have placed within a client organisation in order to pay their salary directly.

### **Example**

A factory decides to use a recruitment agency to conduct an advertising campaign and candidate search on its behalf. The factory has instructed the agency to only accept candidate applications that meet the minimum qualification or experience requirements set out in the job description.

Once the agency has gathered a list of relevant applications, the factory will use this information to shortlist candidates. It will then conduct its own candidate verification and pre-employment checks, as necessary.

For the purpose of this recruitment exercise, the factory is the controller for the candidate information being processed.

However, if the agency decides to also use the candidate information for its own purposes, for example to explore alternative job opportunities with unsuccessful candidates at their request, then they will also be a controller for this information.

Employers or recruiters may also be controllers in circumstances where they are only processing personal information to comply with a particular statutory obligation. This processing requirement would be undertaken in line with their own professional obligations which cannot be transferred or shared with another organisation.

### **Example**

After providing relevant applications to the factory, the recruitment agency retains certain records about the individual applicants. This is in line with its statutory obligations under relevant employment agencies legislation.

As the agency is acting without the factory's instructions, by determining the purpose and means of retaining these records, it is the controller for this processing.

Whether you are an employer or a recruiter, it is important to remember that you are ultimately accountable for the data protection compliance of any processor you decide to engage. In particular, you

**must** ensure that they provide you with sufficient guarantees that they will implement appropriate technical and organisational measures to meet the requirements of the data protection law.

### Further reading

- [Contracts and liabilities between controllers and processors](#)
- [What responsibilities and liabilities do controllers have when using a processor?](#)

## When are we a joint controller and what are our responsibilities?

You are likely to be acting as joint controllers if you and another organisation both determine the purposes and means of processing the same personal information during the recruitment and selection process.

### Example

A law firm engages a recruitment agency to search, sift applications and conduct first stage interviews for permanent paralegal positions at their organisation.

The law firm briefs the agency on the minimum qualifications and training required for the role; how many positions it is looking to fill; and the timeframe in which the initial recruitment stage has to be completed.

Both organisations agree that the agency will decide:

- the advertising channels;
- how many candidate interviews will be conducted;
- the interview questions; and
- the format of each interview (ie by telephone, video call or in person).

The agency determines both the information to be requested from candidates during initial interviews and how the interviews will be conducted without instruction from the law firm. However, the law firm retains ultimate control over how candidate information will eventually be used (ie to shortlist relevant candidates for potential employment).

Both organisations are joint controllers of the personal information being used for the initial stage of the recruitment exercise.

### Example

A temporary staffing agency places a group of workers at Company A for a period of six months.

As the agency is responsible for paying their wages, it tells each temporary staff member that they need to complete a weekly timesheet of the hours they work. The agency uses these timesheets to calculate the total amount to bill to Company A.

Whilst the agency decides what information is collected within the timesheets, it shares this same information with Company A as they also need to record how long each staff member has worked for the purpose of billing and maintaining its own HR records.

The agency and Company A are joint controllers for this personal information as they mutually determine the purpose and means of its processing.

If you are acting as a joint controller with another organisation during the recruitment and selection process, you **must** both determine and agree who takes primary responsibility for complying with certain obligations under data protection law.

For example, you **should** have a transparent arrangement in place with the other joint controller setting out how you deal with SARs from candidates.

You **should** make information about the terms of this agreement available to candidates (eg through your privacy notice).

You are not a joint controller with another organisation during the recruitment process if you are processing the same information for different purposes.

### **Example**

An employer is required to check a job applicant's right to work in the UK.

It carries out a Home Office online check using the applicant's date of birth and right to work share code.

In response to the employer's request, the Home Office provides the applicant's immigration status via a Positive Verification Notice to confirm that they have a right to work in the UK. The employer's HR department retains this document for verification purposes.

The employer and Home Office are not joint controllers. They are both controllers in their own right for the processing of the applicant's personal information. This is because the employer is processing this information for the purpose of verifying an applicant's right to work, and the Home Office is processing this information for the purpose of fulfilling its own legal and official functions.

### **Further reading**

- [What does it mean if you are joint controllers?](#)
- [A guide to individual rights](#)
- [Subject access request Q and As for employers](#)

## When are we a processor and what are our responsibilities?

As a recruiter, you are typically contracted to source relevant candidates for a particular job role on behalf of an employer. In such cases, you are likely to be a processor, and the employer is the controller.

You have more limited compliance responsibilities under the data protection law as a processor. However, within the terms of your contract with a controller, you may make certain daily operational decisions including how you:

- store candidate information;
- transfer candidate information from one party to another; and
- delete or dispose of candidate information when it is no longer required as part of your contract with the employer.

### Example

A secondary school has contracted an executive search firm (ESF) to fill a number of its senior positions as soon as possible.

Given the urgency, the ESF has been given the freedom to use its professional knowledge and expertise to decide how it will source suitable candidates. It opts to do this predominantly through its subscription access to an executive job board and a professional networking site.

Although the ESF is using its professional judgement to decide how best to search for candidates, it cannot make any overarching decisions about the processing itself. This includes what personal information to collect or how it will be used by the school.

Therefore, the ESF is likely to be a processor for this specific processing activity, with the school as controller.

If you decide to employ a third party to assist you with the processing you are carrying out on an employer's behalf, they will be acting as a "sub-processor". For example, you may decide to contract a cloud service provider to securely store and back-up the candidate information you are processing.

However, before engaging a sub-processor, you **must** obtain prior written authorisation from the employer. If this is provided, you **must** enter into a contract with the sub-processor with terms that offer a level of protection for candidate information that is equivalent to the contract terms between you and the employer.

Processors are not responsible for complying with requests they receive on behalf of the controller from candidates wishing to exercise their data protection rights. Ultimate responsibility lies with the controller.

However, the contractual arrangements you have in place with a controller **must** guarantee that they can deal with candidate requests appropriately, regardless of whether you or the controller receives them. In practice, this means that as a processor, you **must** still help the controller to comply with requests from candidates in the exercise of any of their data protection rights.

### Example

A recruiter holds candidate information on behalf of a client organisation, and this is not held separately by the client.

The client may reasonably instruct the recruiter to search for this information and provide them with a copy in order to respond to a candidate's SAR.

People acting within the scope of their duties as an employee of the controller are not processors (eg a staff member who is tasked with conducting initial candidate shortlisting for a job role at their own organisation).

### Further reading

- [Controllers and processors](#), and more specifically [Can you sub-contract to another processor?](#)
- [Contracts and liabilities between controllers and processors](#), and more specifically [What responsibilities and liabilities do processors have in their own right?](#)

## Can our status as a controller or processor change during the recruitment process?

Yes, your status as a controller or processor can change throughout the recruitment process. This is because it is entirely dependent on the processing activity you are undertaking, and who is ultimately in control of the purpose and manner in which that processing is taking place.

For example, you may be both a controller and a processor for candidate information, but only where this relates to separate processing activities, or where you are processing the same candidate information for different purposes.

### Example

A recruitment agency initially holds candidate information as a processor on behalf of an employer organisation to fill a vacancy, but later retains this information to comply with a separate legal obligation it has as a controller under the Employment Agencies Act 1973.

Alternatively, you may be a controller for candidate information during certain stages of the recruitment



process and a joint controller with another organisation for others.

### **Example**

An employer is a controller for candidate information obtained by a recruitment agency on its behalf during an interview process. It is also a joint controller with the same agency for the purpose of processing a candidate's salary information where the agency is responsible for paying them directly.

### **Example**

A recruitment agency receives a CV from a prospective candidate who is looking for roles in the insurance sector on a speculative basis. It processes the candidate's information as a controller.

Upon their request, the agency shares the prospective candidate's CV with an interested client in the insurance sector for their consideration. At this stage, the agency and the client will be joint controllers for the purpose of identifying a relevant role for the prospective candidate.

Although the prospective candidate is considered for a number of roles at the client organisation, they do not receive a formal job offer.

The agency retains the prospective candidate's CV for further job opportunities. It is a controller for this processing activity.

It's important that the systems you use and procedures you follow clearly distinguish between the personal information you are processing in your capacity as controller and the information you are processing on behalf of a controller. This allows you to apply different measures to each data set as necessary, in line with your obligations under data protection law.

### **Are we a controller if we use job boards for recruitment purposes?**

Job boards offer both free and paid for job listings on their websites for employers and recruiters to help broaden their search for relevant candidates. Some job boards also offer candidates the ability to create their own job seeking profile where they can upload their CV for employers or recruiters who pay a subscription fee to view.

Job boards are not usually involved in the candidate hiring process. Therefore, any employer or recruiter that obtains and later processes personal information from a job board will typically be doing so as a controller in their own right unless they are specifically acting on the instructions of a separate controller. This is because the personal information obtained by employers and recruiters (from the job board) is processed for the purpose of identifying and placing candidates in specific roles. This purpose sits

independently from the job board's purposes for processing.

Therefore, your controller obligations under data protection law apply once you use the personal information you have collected from a job board for your own recruitment purposes.

# Finding candidates

Our [consultation on this draft guidance](#) is open until 5 March 2024.

## In detail

- [Do we need to provide privacy information when we advertise vacancies?](#)
- [Can we use social media to advertise our vacancies?](#)
- [Can we manually search for candidates online?](#)

### Do we need to provide privacy information when we advertise vacancies?

If you invite people to apply for a vacancy, you **must** provide them with privacy information, including when you are advertising vacancies on behalf of another organisation. You can advertise vacancies using any method (eg social media, websites (including job boards), voicemail, radio or newspapers).

#### Further reading

- See the earlier section, [Do we need to tell candidates about how we are using their information?](#)
- [What privacy information should we provide?](#)

### Can we use social media to advertise our vacancies?

You can consider advertising your vacancies in different ways.

You may decide to use methods that don't involve using candidates' information and direct marketing. For example, you might post details about the vacancy onto your social media page so that everyone who goes there can see it, or broadcast details of your vacancy to everyone who follows your account. Broadcasting to all of your followers in this way is not direct marketing as you are not targeting particular candidates on the basis of their personal information.

You might also want to use direct messaging on social media to tell specific people about your advert. For example, by sending someone a private message. Direct messaging on social media constitutes direct marketing and electronic mail under the Privacy and Electronic Communications Regulations (PECR). This means that you **must** comply with the rules around direct marketing and PECR.

Alternatively, you may consider using the tools provided by social media platforms to target your vacancy adverts to particular groups of people who use the platform. However, you **must** make sure that your use of these tools complies with data protection law as the activities in social media targeting are complex. For example, you **must** ensure that what you want to do is fair, lawful and transparent.

### Further reading

- [Can we use social media for our direct marketing?](#)
- [Guidance on direct marketing using electronic mail](#)

## Can we manually search for candidates online?

Yes, you can search for candidates manually online using appropriate public social media platforms. However, you need to consider the following:

- If you use publicly available information for your own purposes, you are a controller and are fully responsible for how you use it. You **must** still comply with data protection law. This includes providing candidates with your privacy information as soon as possible, and by no later than one month of obtaining it.
- It may be reasonable to manually search for information using recruitment-based social media platforms, as candidates are reasonably likely to expect their information to be used in this way.
- You **should not** search for candidates on their personal social media profiles, even when these are public-facing. People are unlikely to expect employers to obtain information about them in this way. You risk obtaining information about them which is detrimental or reveals special category information. You **should** avoid this as it is intrusive, high risk, and not likely to reveal relevant information.

Once you have found suitable candidates, you **must** comply with the rules on direct marketing if you wish to contact them directly.

### Further reading

- [Electronic mail marketing](#)
- [Direct marketing guidance](#) and the section, [Can we use publicly available information for direct marketing purposes?](#)

# Automated decision-making and profiling for recruitment and selection

Our [consultation on this draft guidance](#) is open until 5 March 2024.

## In detail

- [What is the scope of this chapter?](#)
- [How can we use solely or partly automated decision-making and profiling for recruitment purposes?](#)
- [What are the risks of using solely or partly automated decision-making and profiling for recruitment?](#)
- [How can we address the risks of using solely or partly automated decision-making and profiling for recruitment?](#)
- [What do we need to consider when using partly automated decision-making and profiling for recruitment?](#)
- [What do we need to consider when using solely automated decision-making and profiling for recruitment?](#)
- [What do we need to tell candidates about solely automated decision-making and profiling?](#)
- [Do people have the right to challenge the decision?](#)
- [Can our use of third-party AI solutions for recruitment purposes affect controllership?](#)
- [What else do we need to consider?](#)

## What is the scope of this chapter?

Solely automated decision-making refers to decisions fully made by automated means, without meaningful human involvement. It often involves profiling too. Profiling analyses aspects of a candidate's personality, behaviour, interests and habits to make decisions about them. In a recruitment context, this can mean using candidates' information from a number of sources to make inferences about potential future behaviour or make decisions about whether they are suitable for a particular role.

In this guidance, any reference we make to 'automated decision-making and profiling' or 'automated decisions and profiling' means automated decision-making for recruitment purposes which may or may not include, or be based on, profiling.

Data protection law restricts the use of solely automated decision-making and profiling that has legal or similarly significant effects on people. This includes a decision about whether to shortlist a candidate, recommend them for interview, reject them or promote them. In this guidance, any reference we make to 'recruitment decisions' means decisions about candidates that have legal or similarly significant effects on them.

We explain the circumstances in which you may be able to use solely automated decision-making and profiling to make recruitment decisions in the section [What do we need to consider when using solely](#)

## [automated decision-making and profiling for recruitment?](#)

You can use automated systems to assist you with recruitment decisions, provided that they are not solely automated, and there has been meaningful human involvement in the decision. We refer to this as 'partly automated decision-making and profiling' throughout this guidance. We explain what we mean by 'meaningful human involvement' in the section [What do we need to consider when using partly automated decision-making and profiling for recruitment?](#)

### Further reading

- [What is automated individual decision-making and profiling?](#)
- [What does the UK GDPR say about automated decision-making and profiling – What types of decisions have a legal or similarly significant effect?](#)

## How can we use solely or partly automated decision-making and profiling for recruitment purposes?

Solely or partly automated decisions and profiling can be made using Artificial Intelligence (AI) and its subset, machine learning. These two terms are not defined in data protection law but generally mean methods of simulating human intelligence processes by machines, so that machines can perform tasks which usually require human intelligence.

Organisations are increasingly relying on solely or partly automated decision-making and profiling, which may involve using AI, at various stages of the recruitment process. This is often seen as a more cost-effective way to screen applications, particularly where organisations receive a high volume of applications. It may help improve the efficiency of the recruitment process, but only if it is used responsibly.

For example, you can use solely or partly automated decision-making and profiling to:

- advertise using algorithms; or
- screen CVs using AI (eg to remove potential points of bias, such as location or ethnic background).

However, you **must** use these methods in a way that complies with data protection law.

### Further reading

- [Guidance on AI and data protection](#)

## What are the risks of using solely or partly automated decision-making and profiling for recruitment?

Solely and partly automated decision-making and profiling presents risks to candidates' rights and freedoms, including their information rights. It can result in unfair discrimination or impact their labour rights. For example:

- algorithms may target certain candidates in unfair or discriminatory ways on the basis of protected characteristics;
- profiling is often invisible to candidates;
- candidates may not expect their information to be used in this way;
- controllers might not fully understand how the process works, or be able to clearly explain the process to candidates who are affected;
- candidates might not fully understand how the process works or how it affects them, even if this is explained to them;
- the decisions may lead to significant adverse effects for some candidates; and
- there is always likely to be a margin of error or a risk of inaccuracy.

Solely or partly automated decision-making processes may also introduce biases or inaccuracies that can lead to unfair results. This may include software that:

- excludes candidates who live a certain distance away from the place of work, even if they intend to move to the area;
- incorrectly eliminates candidates who meet the job criteria;
- incorrectly decides that a person has no legal right to work in the UK; or
- eliminates candidates with gaps in their CV even though this was because the candidate had a serious illness.

### Example

A call centre decides to invest in AI for the purpose of recruiting call handlers. The software it uses has been trained using test CVs from mostly male applicants. As a result, it tends to approve applications from males and reject applications from similarly qualified females. As the software discriminates against people, the call centre is not using candidates' information fairly.

An organisation may not intend to discriminate against people. However, this may be an unintended consequence of its use of an AI system and how that system develops. As controller, you are responsible for the processing, and for ensuring that your AI system only uses information in ways you plan for or expect.

Partly automated decision-making and profiling can have similar risks as solely automated methods, although meaningful human involvement can work as a safeguard, and may reduce these risks. However, you **must** consider the risks of using any solely or partly automated systems for making recruitment decisions by doing a DPIA.

### Further reading

- [Fairness in the AI lifecycle](#)

## How can we address the risks of using solely or partly automated decision-making and profiling for recruitment?

You **must** do a DPIA if you plan to use solely or partly automated decision-making and profiling for recruitment purposes as both activities are high risk. In particular, you **must**:

- consider whether the automated method is necessary and proportionate in the circumstances;
- consider whether you can use less privacy-intrusive alternatives instead;
- be selective about when to use these methods and to what extent;
- ensure your software does not introduce biases, in particular those that target or discriminate against candidates based on their protected characteristics;
- ensure you don't discriminate against someone on the basis of their special category information; and
- carefully monitor and assess the operation of any software you plan to use.

You **must** manage risks of bias and discrimination in any system you use and be able to mitigate the risks before you use automated decision-making and profiling for recruitment purposes. You **should** take measures to:

- prevent candidates from being discriminated against on the basis of their special category information;
- ensure that you are able to correct inaccuracies and minimise errors; and
- keep the information secure.

Even if you have not developed the software yourself, you **must** still understand the data protection implications of its use, and whether it presents a risk to candidates. You **must** cover this in your DPIA. If necessary, you **should** obtain technical or legal advice about software you plan to use to ensure that it complies with data protection law. If you cannot mitigate the risk, you **should not** use the software.

### Example

A financial services organisation runs an annual scheme to recruit graduates. Due to its popularity, it's not practical for the organisation to sift applications without using an automated process. The organisation uses software designed to eliminate irrelevant applications and make a shortlist for the organisation to consider. The organisation is confident that the software is fit for purpose and operates with a high level of statistical accuracy. However, as there is a small margin of error, it **must** have safeguards in place, in the event that the software incorrectly eliminates someone.

If anyone meets the criteria and is not selected, then the automated system has failed, as it was designed to only eliminate irrelevant applications. As a safeguard, the organisation puts in place an appeal process for candidates who meet the minimum criteria but have not been selected. It also informs candidates that they are to follow this process if they meet the criteria but have not been shortlisted.

You **must** also make reasonable adjustments for people who have a disability. Where there is a risk of bias or unfair treatment, you **must** use alternatives to automated processing, or mitigate these risks.



## Further reading

- [What about fairness, bias and discrimination?](#)

### What do we need to consider when using partly automated decision-making and profiling for recruitment?

You may want to rely on partly automated decisions and profiling for recruitment purposes, for example by using AI to assist you in reaching your decisions. In this case, you **must** build meaningful human involvement into each stage of the process in which recruitment decisions are being made about candidates. This means that any decisions about whether to progress a candidate to the next stage are made by a human. You **should** ensure that:

- a human reviews any solely automated outputs that you may use to determine whether a candidate is selected or eliminated from the recruitment process;
- a human has the power to disagree with the AI recommendations or predictions, and can overturn them;
- where there are a number of candidates with similar qualifications and experience, the decision about who to interview is made by a human, although you can consider the recommendations made by the software;
- you don't attach disproportionate weight to the AI recommendations; and
- you have trained staff on how to consider AI-driven or solely automated decisions, without attaching undue weight to them, and they are able to reach their own conclusions.

## Example

An IT company receives a large volume of applications for a software developer vacancy. Candidates sit an aptitude test as part of the recruitment process, which shows whether they can use specific programs and methodologies. The test requires them to answer a number of multiple choice questions, and it is marked using a fully automated system. The scores are automatically attributed to the candidates based on the number of correct answers. The system then ranks candidates according to their scores. Each candidate is also required to attend an interview.

**Good practice:** the company attaches some weight to the test scores for each candidate but does not eliminate anyone on the basis of their test scores alone. It only takes the test scores into account as part of a wider recruitment exercise, but these are not decisive. Each candidate is also required to participate in a group exercise and attend an interview, both scored by a human. The overall decision about whether to recruit someone is made by a human, taking into account all available information about their performance (including the test scores).

**Bad practice:** the company uses the test scores to eliminate half of the candidates, without a human having considered their overall performance. This is unlawful. However, the company may only do this if they are able to rely on an exception to carry out the solely automated processing.

If a human has no power to overturn the AI recommendations, the recruitment decision has been made by solely automated means, and there has been no meaningful human involvement. This is the case even if the human has reviewed the information.

You **should** keep a record of each time a human reviewer overrides an automated recruitment decision. This will help you evaluate both the system you use and the effectiveness of the human involvement. Remember that human reviewers can potentially introduce unwanted bias into the recruitment system through their choices, and you **should** keep both under review.

## Further reading

- [What is the impact of Article 22 of the UK GDPR on fairness?](#)

## What do we need to consider when using solely automated decision-making and profiling for recruitment?

Candidates have the right not to be subject to solely automated decision making and profiling for recruitment purposes as this may have legal or similarly significant effects on them. If a decision is made based 'solely' on automated processing (whether or not this also includes profiling), this means that there has been no meaningful human involvement in the decision-making process.

Data protection law restricts you from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on candidates, unless you can rely on an exception.

Therefore, you **must not** shortlist candidates using solely automated decision-making and profiling unless you're able to rely on an exception **and** you have safeguards in place. There are three exceptions you can use if the decision is:

- necessary for entering into or performance of a contract between you and the candidate (see the section on using [contract](#) as a lawful basis for recruitment);
- authorised by law; or
- based on the candidate's explicit consent (see the earlier section on [explicit consent](#)).

In addition to relying on any one of these exceptions, you **must** also have suitable safeguards in place to protect the person's rights, freedoms, and interests. You **must** at the very least include the right for people to:

- obtain human intervention;
- express their point of view; and
- challenge the decision.

If you're using special category personal information you can only use solely automated decision-making and profiling if you can rely on one of the exceptions listed above **and**:

- you also have the candidate's explicit consent; or
- the processing is necessary for reasons of substantial public interest.

In either case, you **must** have safeguards in place to protect the candidate's rights, freedoms and legitimate interests.

### Further reading

- [Automated decision-making and profiling – When can we carry out this type of processing?](#)
- See earlier section [Substantial public interest](#)
- [What are the substantial public interest conditions?](#)
- [What is explicit consent?](#)
- [What are the appropriate safeguards – Fairness in the AI lifecycle](#)
- See the earlier sections of this guidance, [What lawful bases might apply if we want to process candidates' information?](#) for further information about contract and [Explicit consent](#)

## What do we need to tell candidates about solely automated decision-making and profiling?

If you are using solely automated decision-making and profiling to make recruitment decisions about candidates, there are additional rules about what to tell them. You **must** provide meaningful details about the logic involved and the significance and likely consequences for the candidate. This means that you **should** explain to candidates:

- what information you will ask them to provide and why this is relevant to the recruitment process;
- how the system uses their information, including how it makes decisions about them (eg the criteria it

uses to select or reject them);

- how you will store their information and for how long;
- what risks there are and how you will mitigate these risks (eg by regularly testing the software to ensure the methods remain fair, effective and non-discriminatory);
- the level of any human involvement in the decision-making; and
- their right not to be subject to solely automated decision-making.

For example, if you are confident in the statistical accuracy of your software, but there is a margin of error, you **should** explain:

- what the risks are and how this can impact the recruitment process;
- what safeguards you have in place to reduce these risks; and
- how people can challenge a decision and request human intervention.

You may have concerns that your explanations of automated decision-making processes may disclose commercially sensitive material about how your system works. However, you **must** provide people with an explanation about how your automated system uses their information. You are not required to disclose your source code or any algorithmic trade secrets. But it's unlikely that providing this information creates such a risk. If you consider that it's necessary to limit certain details (eg feature weightings or importance), you **should** be able to justify and document your reasons for this.

You **must** have in place straightforward ways for people to request human intervention or challenge a decision where the processing falls within Article 22.

## Do people have a right to challenge the decision?

People have the right to challenge any solely automated recruitment decision which significantly affects them and request human intervention. You **should** have simple ways in place to allow them to do this. When you decide to make solely automated decisions (which may include profiling), you **must** consider a person's ability to understand and contest those decisions. Remember that each candidate has the right not to be subject to solely automated decision-making and processing for recruitment purposes. This means that software which demonstrates sufficient statistical accuracy may not be appropriate to use for recruitment purposes in the absence of safeguards.

### Example

A financial services organisation consistently receives high volumes of applications for graduate roles every year. It purchases AI software to help it eliminate candidates who do not meet the minimum criteria specified in the job application.

After making enquiries about the accuracy of the software, the organisation is reassured that the system is 99.9% accurate. The organisation receives 20,000 applications from candidates. Based on the statistics, the software is likely to eliminate 20 suitable candidates from the process. However, the organisation considers this to be an acceptable error rate, provided it has suitable safeguards in place and ways for candidates to challenge the decision.

Each of these candidates has a right to challenge the solely automated decision. The organisation **must** apply safeguards to ensure there is meaningful human involvement so that they can use the software lawfully, fairly, and transparently.

In doing so, the organisation **must** be able to identify when the system has made an error. It can do this by informing candidates that it is using AI software to shortlist them and explaining what they will use the software for. By informing candidates that the software only removes those who do not meet the criteria, any of the candidates can challenge the decision on the basis that they do meet the criteria.

The organisation **must** have processes in place to enable candidates to easily challenge the decision and a process which allows a human to review the AI decision.

You **should** record and monitor the number of challenges made by candidates on the grounds of fairness. This helps you assess how effectively your AI software enables you to comply with data protection law. You **should** address unfair outcomes in a timely way. In the context of recruitment, you **must** be able address the error quickly enough so that you do not unfairly eliminate the impacted candidates from the recruitment process.

#### Further reading

- [Right not to be subject to automated decision-making](#)

### Can our use of third-party AI service providers for recruitment purposes affect controllership?

Yes. If you decide to use someone else's AI systems for your recruitment purposes, you **must** be clear about their role. This is because the development and deployment of AI systems which process personal information often involves multiple organisations. For example, it is possible for an AI service provider to be a controller or joint controller for some AI processing phases and a processor for others.

The decision to use an AI service provider is one you take as a controller. Being aware of the status of your service providers will help you to establish accountability - both from the outset of any AI processing activities in recruitment and during the course of its use. It will also enable everyone to understand their respective obligations under data protection law.

When using AI service providers for recruitment purposes, you **should** consider the types of decisions which may impact their status as a controller for each processing activity. These may include decisions about:

- the source and nature of information you use to train an AI model (both before its use and throughout its development);
- what is trying to be predicted or classified through your use of an AI model; or
- how the AI model you use will be continuously tested and updated (both before its use and throughout its development).

Your AI service provider can also make some technical decisions about how they process candidate

information for you and still be a processor.

Depending on the terms of their contract with you, these decisions may include:

- how machine learning algorithms are specifically implemented (eg the programming language they are written in);
- how candidate information and AI models are stored;
- the measures used to optimise learning algorithms and models; and
- how AI models will be deployed in practice.

If your AI service provider processes personal information for any other reason than what you've instructed them to do, then they are a controller or joint controller for this processing.

### Further reading

- [What are the accountability and governance implications of AI?](#)
  - For further examples, please see indicative example scenarios.

You **should** regularly review any AI services you have outsourced to a third party for recruitment and selection purposes and be able to modify them or switch to another service provider, if required.

You **must** conduct a DPIA for your use of AI in recruitment as this is likely to result in a high risk to the rights and freedoms of candidates. You **should** clearly document in your DPIA the relationships between you and your AI service providers, alongside the roles and obligations of each party. You **should** also cover who you share personal information with and when (eg via a data flow diagram or process map).

If you decide that you and your AI service provider are joint controllers, you **should** collaborate in the DPIA process as necessary.

Where your supplier is a processor, they **must** assist you in completing the DPIA.

### Further reading

- Broader guidance on controller and processor relationships in the context of AI can be found in our main [Guidance on AI and data protection](#) and more specifically in the section: [How should we understand controller / processor relationships in AI?](#)
- [Controller and processors](#)
- [Data Protection Impact Assessments \(DPIAs\)](#)
- [Data protection by design and default](#)

## What else do we need to consider?

As controller, you are responsible for the software you use to process personal information, even if you did not build the software or create the algorithm. When you plan to use software, it is your responsibility to ask how the system operates, and to ensure that it uses personal information in a way that complies with

data protection law. For example, you **could** ask for information on:

- the demographic groups a model was trained on;
- whether any underlying bias has been detected or may emerge; and
- any algorithmic fairness testing that has been conducted.

You **should** regularly review your AI system and have measures in place to check for bias or discrimination. In particular, you **should** regularly review the efficiency and algorithmic fairness of the software for people with protected characteristics and special category information.

If your software has been trained on particular information, it may be less statistically accurate if circumstances change.

### Example

An organisation's head office is based in a particular town in the UK. The organisation uses AI software to conduct interviews. As most of the candidates are local, the software has been trained using primarily local accents. It demonstrates a preference for local accents, but is still sufficiently statistically accurate, provided there are safeguards in place. This includes reviewing the decisions of AI where bias is likely or has been identified.

The organisation's working model has changed in recent years and it decides to recruit remote workers based in other parts of the UK and worldwide. The bias in favour of particular accents has reduced the statistical accuracy of the AI to a level that is no longer adequate or fair. This means that the organisation **should** consider retiring the software, as it is no longer fit for purpose. Alternatively, it **could** retrain the software with new representative data.

### Further reading

- [How do we ensure transparency in AI?](#)
- [How do we ensure lawfulness in AI?](#)
- [How do we ensure fairness in AI?](#)
- [Fairness in the AI lifecycle](#)
- [Guidance on AI and data protection](#)
- [Rights related to automated decision-making including profiling](#)
- [What are the substantial public interest conditions?](#)

# Information provided by candidates

Our [consultation on this draft guidance](#) is open until 5 March 2024.

## In detail

- How might we obtain information about candidates for recruitment?
- How might we deal with unsolicited applications or CVs?
- What information can we ask for in the application process?
- When can we ask for special category information?
- Can we ask candidates for details about their previous convictions at the initial application stage?

### How might we obtain information about candidates for recruitment?

You might obtain information about candidates in a number of ways, for example by:

- designing an application form and asking candidates to provide specific information about themselves so you can consider them for a particular role. (You **should** tailor your application form to the vacancy you are recruiting for to ensure that you only collect the information you need);
- asking candidates to provide their CV; or
- manually searching for candidates using publicly available sources (eg job boards or recruitment platforms).

You might also obtain information about candidates, even if you haven't asked for it. For example:

- a person sends you their CV on a speculative basis for you to consider them for future roles; or
- you receive a recommendation about a possible candidate from another person or organisation.

You might instead outsource your recruitment functions to an external recruiter. They will then send you information about potential candidates who meet your requirements.

### How might we deal with unsolicited applications or CVs?

If candidates send you their personal information, even if you have not asked for it, you **must** still comply with data protection law. This includes being transparent about how you deal with personal information.

You **should**:

- make it clear to candidates whether you consider unsolicited applications – this may help minimise the amount of information you collect;
- cover unsolicited applications in your retention and disposal policy; and
- explain how you deal with unsolicited applications in your privacy notice.

It is important that you are transparent with candidates about how you use their personal information,



even if you don't plan to use it immediately. For example, a recruiter or employer may receive and retain a collection of speculative applications for future roles if suitable vacancies arise. Particularly if you are a recruiter, this process may form part of your core business model.

If you receive personal information but do not plan to use it, you **must** securely delete it as soon as possible. If you do plan to use the information, you **should only** use it for recruitment purposes (eg when potential vacancies arise within your organisation or an organisation you are recruiting for). You **should** explain this in your privacy information.

### Further reading

- [Data minimisation](#)
- [Lawfulness, fairness and transparency](#)
- [Storage limitation](#)

## What information can we ask for in the application process?

You can ask candidates to provide the information you need in order to consider them for the next stage of the recruitment process. What you may need can vary depending on the role and you **must** be able to show why you are collecting the information.

### Example

A haulage company runs a recruitment campaign for lorry drivers. The application form asks candidates to confirm they can drive heavy goods vehicles and provide their driving licence number.

A few months later, the haulage company decides to recruit office-based staff for administrative roles. These staff are not required to drive, so the haulage company doesn't ask candidates if they can drive or for their driving licence number.

You **must** only collect information that is proportionate and relevant to the role. For example, the amount and type of information you may need to recruit a company director with resource management responsibilities is likely to differ from the amount and type of information you need for operational or administrative roles.

In general, you **should not** ask candidates to provide:

- information you don't need, even if you think it might be useful at a later stage or for other roles you are recruiting for;
- information you'll only need if you employ them (such as bank or emergency contact details);
- information that would be more appropriate to ask for at a later stage for verification purposes (eg details about spent or unspent convictions);
- special category information – unless you need this in order to make the recruitment decision (see the

following section); and

- information about trade union membership.

If you are a recruiter seeking information from a person who is looking for employment on a speculative basis, you can ask for information that will enable you to identify and match people to potential vacancies that are relevant to their stated interests. However, if a person has submitted their CV to you with a clear intention to find a job role in a particular industry, it would be excessive to request information from them that was not required or relevant to roles in their preferred industry.

## When can we ask for special category information?

You can ask for special category information if you need it for your particular recruitment purposes and you have a condition for processing it. For example, a politician may require the successful candidate to share the political beliefs of their party and ask for evidence by requesting examples of the candidate's campaigning work.

However, you **should only** ask for special category information at the stage in the recruitment process when you need it. This may often be at the verification or vetting stage rather than the application stage. However, you **should** explain to candidates at the early application stages when you will collect this information.

### Example

A construction company wants to recruit a roof tiler. As the successful candidate needs to be able to climb ladders and carry out physically demanding tasks, the company wants to ensure that it only shortlists candidates who are physically mobile and can perform these tasks.

The company explains the physical requirements of the job and asks candidates to confirm that they can perform the required tasks. It does not ask candidates to provide evidence (eg a medical letter), as this would be excessive. However, it may collect this information at a later stage or carry out a medical assessment on the successful candidate.

However, even if the company does not ask for evidence, the candidate's response to the question about their health is special category data, even if this simply involves ticking a box. Therefore, the construction company **must** have a special category condition for processing this information, in addition to a lawful basis.

In general, you **should not** ask candidates questions about their health unless it is relevant to the role. For example, if a medical condition may compromise the safety of the candidate or others in the workplace.

### Example

The construction company needs to ensure that its tilers and heavy machinery operators do not suffer

from any health condition that may place them or other workers at risk. It includes a list of specific medical conditions on the application form, including seizures.

It explains that candidates may not be suitable for the role if they suffer from any of these conditions unless they can provide evidence that the condition is under control (eg a doctor's letter).

However, the company explains in the application form that it does not need candidates to provide further details or evidence at this stage in the process. The condition only permits employers to use health information to assess the working capacity of employees, so the company explains that it will only collect this information from the person who is offered the job. There are other rules they will need to follow when they collect this information.

### Further reading

- See the earlier section on [What special category conditions might apply?](#)
- [Employment practices and data protection: information about workers' health](#)
- [Special category data](#)

## Can we ask candidates for details of any previous convictions at the initial application stage?

In general, you **should not** ask candidates to make a criminal records declaration on the application form. Information about criminal convictions is particularly sensitive and subject to extra protection under data protection law. You are not required to ask about criminal convictions, and you **should** only do so if you can show why this is necessary.

In most cases, criminal conviction information will not be relevant to the decision to shortlist, interview, or offer a candidate a job. However, if you consider that it is relevant to a particular role, you **must** document your reasons why. For example, if you need to collect the information at an earlier stage to comply with specific safeguarding requirements.

### Example

A youth club is recruiting a team manager for a children's sports group. It needs each candidate to make a criminal records declaration at the application stage before they shortlist them. This is to comply with safeguarding provisions. The application form states clearly that:

'This role involves regulated activity with children. You must not apply if you are on the children's barred list and your application will not be considered.'

It's important that the application form makes it clear that it is a criminal offence for people who are on the children's barred list to apply for this role.

You **should** be careful about how you ask for information about criminal convictions and consider the language you use on your form. You **should not** ask general questions about whether someone has ever been convicted of a crime. This is because it may cause candidates to provide information that you are not legally entitled to or is unnecessary for your recruitment purposes.

You **must** comply with the data minimisation principle when you obtain personal information. It's unlikely to be necessary and proportionate for you to ask for this information from all candidates. In most cases, criminal records checks can take place as part of your pre-employment vetting. For further details, see the chapter on [Pre-employment vetting of candidates](#).

You **could** explain in the application pack that you will require candidates to submit a criminal records declaration form if you make them a conditional offer of employment. You **could** also include a copy of the criminal records declaration form within the application pack and explain why this information is necessary and relevant to the role. You **should** make sure that you can separate and detach the criminal records declaration form from the rest of the application form.

### Further reading

- [Data protection by design and default](#)
- [What is the right to be informed and why is it important?](#)
- [What privacy information should we provide?](#)
- [Documentation](#)

# Shortlisting, testing, and interviewing candidates

Our [consultation on this draft guidance](#) is open until 5 March 2024.

## In detail

- [What do we need to consider when shortlisting or testing candidates?](#)
- [What data protection issues do we need to consider when conducting interviews?](#)
- [What do we need to consider if we're carrying out interviews or testing remotely?](#)

## What do we need to consider when shortlisting or testing candidates?

How you select the most suitable candidates from the applications you receive may depend on the nature of the role, and the volume of applications.

Shortlisting can involve:

- reviewing application forms to select candidates based on their qualifications and experience;
- using automated systems to help you select candidates;
- psychometric tests, skills tests, or aptitude tests; and
- assessment centres.

You **must** comply with data protection law when shortlisting or testing candidates. You **should** select candidates in a way that is fair and consistent. For example, you might assess each candidate against specific criteria as this can help to ensure transparency. Having criteria in place also means that you're likely to collect information about candidates only for your specified purposes, and you're less likely to collect information you don't need.

You **should** inform candidates about the selection criteria you will apply to their information in order to shortlist them. You **should** provide these details before you collect the information. For example, by including it in the job description or application form.

If you are using tests or assessments, you **should** pseudonymise candidates' information, where possible. This is because any personal details about the candidate are unlikely to be relevant for marking their test or determining their score. Pseudonymisation can be an effective way of avoiding bias in decision-making and help ensure that decision-makers don't take irrelevant information into account.

For most roles, it will usually be appropriate to shortlist candidates based on the information they provide rather than information you collect from other sources (eg references or from public social media profiles). This helps to ensure that your processing is fair and transparent. However, there are some roles which are subject to specific legal requirements or carry particular risks to others. In these cases, it may be reasonable to shortlist candidates on the basis of information you have obtained from other sources. If so, you **should** set out your reasons, including any relevant provisions you rely on, and inform candidates at

the start of the recruitment process.

You **should** only provide staff who are making recruitment decisions with the information they need. For example, you **should** have a designated member of staff remove any irrelevant information from the application form before it's presented to the decision-makers. This helps to ensure that decisions are not based on irrelevant information.

## What data protection issues do we need to consider when conducting interviews?

Interviews can take many different forms. For example, you can carry out in-person, online or telephone interviews.

You are likely to collect additional information about candidates during the interview process. For example, you may record the candidate's responses during their interview or your own opinion about the candidate's suitability for the role.

Remember that the candidate can make a SAR for any additional information you record in the interview (eg interview notes). We have separate guidance to help you deal with SARs.

You **must not** collect excessive information about candidates at interview. For example, it is not usually necessary to make a video recording of each candidate's interview performance.

If you need to have a process in place to make a decision between candidates with the same scores, you **must** inform them that this will form part of your process, and explain why and how you will do this.

You **could** give candidates an opportunity to comment on the information you hold about them during the interview. This may be appropriate if you collected the information from another source and you cannot be certain of its accuracy or the wider context and circumstances.

### Example

A political party is recruiting a personal secretary for its party leader. The job description specifies that candidates have to share the political views and values of the party.

The party shortlists a number of candidates for interview. However, after performing an online search, it finds publicly available blogs, videos and conversation threads about one of the candidates. These suggest this person has strong views which align with those of another political party and oppose the views of the recruiting political party. This information shows that the candidate has publicly campaigned for issues that the party does not support and against issues the party does support. It is also clear that the candidate has deliberately made this information public.

The party does not want to interview the candidate. However, this would be unfair for a number of reasons:

- The information obtained online may be out-of-date or inaccurate – the party might have mistaken the candidate for another person with the same name or the candidate may have since changed their political views.
- If the party has not informed the candidate that they will use social media screening as part of the

recruitment process, then it would not be fair to use the information.

Due to the nature of the information and its relevance to the vacancy, the party does not believe it can ignore the information. However, because there is a risk of unfairness, they **should** give the candidate an opportunity to explain or comment at interview.

### Further reading

- [Subject access request Q and As for employers](#)

## What do we need to consider if we're carrying out interviews or testing remotely?

It's not uncommon for employers to ask candidates to complete online assessments remotely or to attend virtual interviews (eg by video call). Candidates are likely to complete these assessments or attend virtual interviews in their own home, using their own devices or at a location where they can access a computer and the internet.

If you plan to incorporate remote testing or virtual interviews into your recruitment practices, you **should** identify the type of processing involved and consider the need for a DPIA. You **should** also document your decision.

You **should** also consider taking the following steps:

- Consider and document what information you need candidates to provide.
- Ask candidates who are attending a video interview to remove any sensitive or irrelevant information from their desktop and close down other applications if there is a risk that this may be disclosed (eg during their screen sharing of a presentation you've asked them to give).
- Where possible, provide backgrounds to candidates attending video interviews to ensure that you aren't processing unnecessary information (eg content from their homes might reveal their religious beliefs).

You may need to consider whether there are any security implications if candidates are using their own devices and software to complete assessments and interviews.

### Further reading

- [A guide to data security](#)

# Verifying candidates

Our [consultation on this draft guidance](#) is open until 5 March 2024.

## In detail

- [What is verification?](#)
- [Does it matter how we ask candidates to send us their information for verification purposes?](#)
- [What do we need to consider when checking references?](#)

### What is verification?

Verification is the process that employers or recruiters use to check the information a candidate provides in support of their job application. It also includes checking references.

This is different from pre-employment vetting which is covered in the section on [Pre-employment vetting of candidates](#), and involves employers actively making their own enquiries, rather than checking the information provided by the candidates themselves.

You may decide to check the accuracy of the information candidates have provided in support of their application (eg by asking for evidence of their qualifications). You **must** only obtain the minimum information you need. For example, if you need to verify someone's identity, you may need a passport or driving licence, but it's unlikely that you would require both.

You **must** explain your verification process as early in the recruitment process as possible. For example, by setting this out in the application form. In particular, you **should** explain:

- the methods you will use;
- the specific information you will verify;
- how long you will keep any information you collect for these purposes; and
- any external sources you will use or rely on.

The stage in the process that you carry out verification is important. Where possible, you **should** only verify the information provided by successful candidates. If you need to verify the information at an earlier stage, you **must** be able to justify why this is necessary. For example, you may be under a legal obligation to carry out checks at an earlier stage for particular types of roles. However, in most cases you **should not** carry out verification checks for every candidate, as this is unlikely to be necessary and involve excessive processing.

### Does it matter how we ask candidates to send us their information for verification purposes?

If you are asking candidates to provide information for verification purposes, you **could** give them the option to provide this information in person. For example, if you are requesting original documents (such as



university degree certificates) which may be expensive to replace, or may be needed for other purposes, including sharing with other prospective employers. You can then verify the information, make a copy for your records (if you need to), and return it directly to the candidate.

If candidates are unable to attend your premises in person, you **could** suggest they send their information using another secure method (eg tracked delivery). However, if you don't need to see original documents, you **could** ask candidates to send their information by a secure electronic method (eg encrypted email).

## What do we need to consider when checking references?

You **should** only ask the referee for the information you require in line with your recruitment policies. For example, if you only need the referee to confirm the candidate's employment dates, then only ask for this information.

You may receive a confidential employment reference about a candidate. The personal information contained in a confidential reference is exempt from the right of access. This means that if a candidate makes a SAR for the confidential reference, you are not required to disclose it. If the reference is not consistent with information the candidate has provided, see the section, [What can we do if our checks are not consistent with the information provided by the candidate?](#)

However, this exemption only applies to references given in confidence, and not to references more generally.

### Further reading

- [Right of access guidance – Confidential references](#)
- The principles – [Principle \(a\): Lawfulness, fairness and transparency](#) and [Principle \(c\) Data minimisation](#)

# Pre-employment vetting of candidates

Our [consultation on this draft guidance](#) is open until 5 March 2024.

## In detail

- [When can we carry out pre-employment vetting?](#)
- [What do we need to tell candidates about pre-employment vetting?](#)
- [How can we decide what information to obtain for pre-employment vetting?](#)
- [Can we obtain information about criminal convictions?](#)
- [Can we ask if the candidate has been excluded or disciplined by a professional membership body?](#)
- [What can we do if our checks are not consistent with the information provided by the candidate?](#)
- [Can we use social media for vetting purposes?](#)
- [Can we perform a credit check on a candidate before we employ them?](#)
- [How long can we keep information collected for vetting purposes?](#)

## When can we carry out pre-employment vetting?

Pre-employment vetting is where employers make their own enquiries from third parties about a candidate's background and circumstances. It is particularly intrusive and goes beyond verification or simply checking the accuracy of the information candidates have provided about themselves.

Pre-employment vetting is not usually a requirement of the recruitment process and you are unlikely to need to do this for many roles. If you have questions about information the candidate has provided, you **should** contact the candidate about this.

You **should** only do pre-employment vetting where you are under a legal obligation (eg to perform right to work checks), or you can identify significant and particular risks to the employer, clients, customers, or others. The nature and extent of these risks may depend on the type of the role, but examples might include:

- breaches of national security;
- employing unsuitable people to work with children or adults at risk of harm;
- there is a danger to others;
- risk of theft; or
- disclosure of trade secrets or other commercially sensitive information.

It's important that the type of vetting you are thinking of doing is proportionate to an identified risk, and a targeted way of achieving your objective. Therefore, you **must** ensure that it's justified in the circumstances and there are no less intrusive alternatives. You **should not** routinely vet all candidates, unless you are legally required to do so.

## Example

A company wants to recruit a director. It decides to perform a bankruptcy search on the successful candidate. However, it's not necessary to carry out these checks on all candidates.

## What do we need to tell candidates about pre-employment vetting?

You **must** inform candidates if you intend to use pre-employment vetting as part of your recruitment process. This is part of your transparency obligations and you **should** include an explanation of:

- what information you need for the vetting;
- why you need to carry out pre-employment vetting;
- who will have access to the information;
- the processes you will use;
- how long you will keep the information; and
- where possible, the third party sources you will rely on.

Depending on the circumstances, you **could** also inform candidates at what stage in the process you will assess the information.

## Further reading

- See the earlier section, [Do we need to tell candidates about how we are using their information?](#)

## How can we decide what information to obtain for pre-employment vetting?

Recruiting for certain roles may allow you to carry out more intrusive checks. You may wish to consider any relevant legislation to help you decide what level of checks are justified for the role. This may also help you decide at what stage in the process to carry out pre-employment vetting. For example, you may be legally required to vet candidates at the shortlisting stage for some roles that involve working with children.

You **must** only collect the minimum amount of information that you need. If you are requesting information from third parties, you **should** clearly explain what you need and why. Organisations need to understand why you are asking for this information so that they may make an informed choice about whether they can provide it or not. If there is a legal obligation, you **should** reference the specific provision you are relying on.

You **must not** make wide-ranging or vague requests to organisations, or ask organisations for more information than you require. However, you **should** ask for enough information to be able to understand the context and circumstances. For example:

- asking whether someone has a criminal conviction for a violent offence and receiving a yes or no answer

is unlikely to be helpful; or

- if you're asking about spent convictions, it's important to know what age the person was at the time the offence was committed, as this is likely to have a bearing on the relevance of the information.

You may also wish to consider other laws or relevant sectoral guidelines. You may wish to seek independent legal advice, or contact your other regulators for further details.




## Can we obtain information about criminal convictions?

If the nature of the role means you need to ask about criminal convictions, you **should** determine what level of checks are required. In many circumstances, you can ask candidates to make a self-declaration about their criminal record, or you can perform these checks, provided that you get the candidate's consent first. This applies to any criminal convictions, alleged offences, or information that confirms that a candidate does not have any convictions.

The process differs across the UK, and depends where the job is based:

- for England and Wales, use the Disclosure and Barring Service (DBS);
- for Northern Ireland, use AccessNI; and
- for Scotland, use Disclosure Scotland.

### Further reading

- [Disclosure and Barring Service](#) 
- [AccessNI](#) 
- [Disclosure Scotland](#) 

Some roles may require more in-depth checks, and it's important that you comply with other legislation and guidance on this area. You **must** tell candidates what level of checks are required and how you will carry these out at the beginning of the process. Because of the sensitivity of this type of information, in most circumstances the processing of criminal offence information for vetting will be high risk. Remember that you **must** carry out a data protection impact assessment (DPIA) in these circumstances.

In general, it's likely that you will only require information about unspent convictions, although for some roles you may also need to obtain information about spent convictions.

As far as possible, you:

- **must** only obtain criminal records disclosure of the person you intend to appoint; and
- **should** ensure that you do not share the information you obtain with other third parties (eg other employers).

To process criminal conviction information as an employer or recruiter, you **must** have a lawful basis and either:

- official authority; or
- legal authority.

Only organisations that perform public functions and exercise powers established by law can rely on official authority. Therefore, if you do not have official authority, you **must** meet a specific condition under Schedule 1 of the DPA 2018. The following are likely to be most relevant:

- the processing is necessary in order to comply with employment law obligations. For example, you are legally required to vet candidates for particular roles for safeguarding purposes, or to comply with Financial Conduct Authority conduct rules; or
- the processing meets one of the substantial public interest conditions set out in the DPA 2018. For example, safeguarding of children and of people at risk, preventing or detecting unlawful acts, or preventing fraud.

You **must not** mislead a person or organisation into giving you information about a candidate (either recklessly or deliberately) for recruitment purposes, as this is a criminal offence.

You **must not** obtain information about criminal convictions by forcing a candidate to make a SAR to any organisation, including the DBS, Access NI, and Disclosure Scotland.

### Further reading

- [Criminal offence data](#)
- See the earlier chapter on [Information provided by candidates – Can we ask candidates for details of any previous convictions at the initial application stage?](#)
- [Data Protection Impact Assessments \(DPIAs\)](#)

## Can we ask if the candidate has been excluded or disciplined by a professional membership body?

Professional membership bodies exist to uphold ethical and professional standards and rules in specific professions. Regulatory bodies may take disciplinary action against their members and apply various sanctions. For example, they may restrict a person's professional ability to practice.

You might consider it to be necessary and proportionate to enquire whether a candidate has been excluded by or subjected to disciplinary action from a professional membership body, if this is relevant to the job role. This may be relevant for some regulated professions (eg solicitors and accountants).

However, if you require information about spent or unspent convictions, refer to the relevant statutory framework instead (DBS, AccessNI or Disclosure Scotland).

If a candidate has been excluded from a membership body, you can assess this information on a case-by-case basis to decide how this impacts the job role you are recruiting for. You can refer to professional codes of conduct or other relevant legislation in making your decision about the candidate.

## What can we do if our checks are not consistent with the information provided by the candidate?

If some of your checks produce discrepancies between the information provided by the candidate, and your own findings, you **should**:

- have a policy which sets out a transparent process to follow in these circumstances;
- give the candidate an opportunity to explain these discrepancies to you;
- ensure that the candidate's explanation or comments are considered in your decision-making process;
- ensure that staff who are involved in verification and vetting are trained on the correct process to follow, including how to inform candidates and give them an opportunity to comment or explain anything you have concerns about; and
- keep records of your decisions.

You cannot assume that the candidate is being untruthful. Where the facts are unclear, you **should** make a reasonable decision based on the factual evidence, taking into account the nature of the information and associated risks.

## Can we use social media for vetting purposes?

If you want to check the candidate's public social media profiles as part of your pre-employment vetting, you **must** be able to justify why this is necessary. This means you **should** identify and document a specific risk. However, in doing these checks, you are also likely to find information that is not relevant to the role. It's important that you carry out these checks fairly.

As your vetting processes must be transparent, you **must** inform candidates if you intend to use social media. The staff members who research the candidate's social media profiles **should not** also make the recruitment decisions about them.

### Example

A care home is recruiting carers to look after elderly people. It informs candidates that it will check the successful candidate's public social media profiles for any behaviour or conduct which may mean they would be unsuitable to work with people who need care and support. The care home believes it has a duty of care to check public sources of information about staff it appoints for this particular role, and it has clearly identified the risk and documented its reasons for carrying out these checks.

As social media checks are likely to reveal irrelevant personal information about the candidate, the organisation asks one member of staff to do the social media checks, and screen the information for relevancy against the specified interview criteria. This member of staff passes only the relevant information to the recruitment panel.

It's unlikely to be lawful, appropriate or necessary to conduct intrusive or targeted checks of candidates on social media or online (eg by using specialist software to check information that is not publicly available).

Remember that information you find online may not be accurate or properly reflect whether the candidate is suitable for the role. It is unlikely to be fair and lawful to make a decision about the candidate based on this information alone. You **should** give the candidate an opportunity to provide further information or comment on the accuracy of the information you have obtained. This allows you to make a fully informed and defensible decision and ensures that you are using the information in a transparent way.

## Can we perform a credit check on a candidate before we employ them?

You may wish to undertake a credit reference check on a candidate, where this is relevant to the role you are recruiting for. You **must not** carry out credit reference checks routinely or without justification.

You **must** be able to justify why collecting credit information is necessary for the role. You **must** also inform candidates as early as possible in the recruitment process what information you require, and what methods you will use to carry out such checks.

## How long can we keep information collected for vetting purposes?

If you collect personal information as a condition for appointing someone, you **must not** retain it for longer than is necessary. This will often mean that you **should** securely and permanently destroy personal information obtained for vetting purposes once the recruitment process has taken place. However, you **could** keep a record of the outcome and your decision.

As information obtained for vetting purposes is particularly intrusive and sensitive, you **must** securely and permanently destroy it as soon as it is reasonably practicable to do so. This includes any information you've collected from third parties or through your own research (eg manual checks of the candidate's public social media profiles). You **should** address this in your retention and disposal policy.

### Further reading

- [Criminal offence data](#)
- [A guide to data security](#)

# Keeping recruitment records

Our [consultation on this draft guidance](#) is open until 5 March 2024.

## In detail

- [How long can we keep recruitment records for?](#)
- [When can we keep information about candidates?](#)

### How long can we keep recruitment records for?

Under data protection law, you **must not** keep information for longer than you need to. However, it does not specify timescales for keeping recruitment records. You **should** carefully consider how long you need to keep this information for and set clear retention periods.

#### Example

A restaurant receives 50 applications for a job vacancy. Unless there is a clear business reason for doing so, the restaurant **should not** keep recruitment records for unsuccessful candidates beyond the statutory period in which an applicant can bring a claim arising from the recruitment process.

You **should** also establish and document standard retention periods for the different categories of information you hold, when this is possible. Depending on the circumstances, you may be legally required to keep information for a specified period of time to comply with certain laws.

For example, recruitment agencies in England, Wales and Scotland are required to comply with the Employment Agencies Act 1973, while recruitment agencies in Northern Ireland are required to comply with the Employment (Miscellaneous Provisions) (NI) Order 1981.

### When can we keep information about candidates?

When you collect information for the purposes of recruitment and selection, it's unlikely that you will need to keep all of it after the recruitment process is complete and you've appointed someone to the role.

You may need to keep some details about the candidate you appoint. You **must** carefully select what information is needed for your employment relationship. If this information is no longer relevant now that the candidate is an employee, you **must** securely destroy it, in accordance with your retention and disposal policy.

However, if you destroy records about any of the candidates too quickly, it may be more difficult for you to



prove that your end-to-end process is transparent, fair and accountable. In particular, as candidates may make a SAR for their information. You **should** consider this when you set retention periods for recruitment information.

### Example

An airport uses psychometric testing and interviews to recruit staff. In setting retention periods, it considers the following issues in deciding how long it might need to keep the information for:

- candidates may request their information;
- its appeal process for candidates who believe the airport has reached a recruitment decision in an unfair way; and
- the possibility of legal proceedings being brought against the airport.

If you wish to keep candidates' information for a new purpose, you **must**:

- review whether you may need a different lawful basis (and if required, a condition) for processing the information;
- have previously informed candidates that you will keep their information for another purpose, and explained what this purpose is; and
- destroy the information you do not need.

### Example

A law firm is running a recruitment exercise for the position of assistant solicitor. There is currently only one vacancy but the firm has identified a business need to appoint more assistant solicitors within the next six months.

The law firm appoints one candidate but it also creates a waitlist by ranking candidates on their scores during interview and assessment. It informs candidates on the application form that it intends to retain the recruitment information for the top 10 scoring candidates for a period of six months, in case further vacancies arise within this time.

Retaining recruitment records may be necessary in case you need to defend yourself against claims of discrimination or other legal actions arising from recruitment. There are statutory limitation periods in place for bringing claims, which means that candidates have a limited period of time to bring a claim. This period varies depending on the nature of the claim, and may be a number of years. The relevant legislation is as follows:

- the Limitation Act 1980 (applies to England and Wales);
- The Limitation (Northern Ireland) Order 1989 (applies to Northern Ireland); and

- the Prescription and Limitation (Scotland) Act 1973 (applies to Scotland).

You may wish to refer to these statutory limitation periods for bringing claims and seek independent legal advice on how long you may need to keep these records for. However, the possibility that a person may bring a legal claim does not mean that you have to keep records about recruitment indefinitely.

In general, you **should not** keep information beyond the statutory period in which a legal claim can potentially be brought. It's also unlikely that you need to keep all the information you hold for the purpose of defending potential legal claims. You **must** only keep information if you can justify why this is necessary. If you have a different purpose for keeping the information, you may need to review your lawful basis and condition for processing.

If you need to keep candidates' information for statistical purposes only, then you **should** anonymise it. Fully anonymised records are not considered to contain personal information which means that data protection rules do not apply to them.

However, if you plan to retain candidates' personal information, then you **must** comply with data protection law. This is the case even if you intend to pseudonymise the information because it's still possible to identify people from pseudonymised information.

### Example

An organisation develops a secure portal to obtain equality and diversity information about candidates and existing staff members. This allows them to track the success of its equal opportunities initiatives in recruitment.

Candidates are required to submit their equality information using this secure portal when they apply for a vacancy. Existing staff members are invited to voluntarily submit and maintain their information online. After they have appointed a candidate, they will automatically delete the information about all candidates unless they explicitly consent by opt-in to the organisation using their information for the specified purposes. This applies to all successful and unsuccessful candidates.

The organisation **must** take the following steps:

- provide a link to its privacy information;
- make it easy for people to withdraw their consent; and
- restrict access to the information only to staff members who need to access it in order to track the success of the organisation's equality opportunity initiatives in recruitment.

The organisation uses the information to generate fully anonymised statistics. It does this by taking steps to ensure that people cannot be identified from the statistical information, using any other personal information.

The organisation **must** store the personal information securely until it has been fully anonymised and destroy it once it is no longer needed.

## Further reading

- [Documentation](#)
- [Data minimisation](#)
- [Storage limitation](#)

# Recruitment and selection impact assessment summary

Our [consultation on this draft guidance](#) is open until 5 March 2024.

Read the [recruitment and selection impact assessment summary](#)  (opens as a PDF document in a new tab).