Employees - recruitment, records and monitoring

information commissioner
Barrantagh Fysseree

This guidance has been produced to help organisations comply with the data protection legislation when recruiting and employing workers. It is relevant to all "controllers" whether public sector employers, commercial enterprises, or organisations which recruit volunteers or unpaid workers.

The data protection legislation applies to information about living, identifiable people, including employees, volunteers and job applicants. It applies to any information about individuals, including that contained in emails, CCTV images, monitoring devices, psychometric tests, documents, spreadsheets, social media posts, messaging apps etc., and to information in manual records held in structured filing systems.

The data protection legislation regulates the way in which information about individuals is processed (collected, handled, used and destroyed), gives individuals rights, including access to their information, and compensation if things go wrong. Controllers must be able to demonstrate, and are accountable, for compliance.

THE RECRUITMENT AND SELECTION PROCESS

The data protection legislation does not prevent effective recruitment, but strikes a balance between an employer's need for information about the person, and that person's right to respect for their private life.

It applies to information collected or used about people as part of the recruitment or selection process, for example, CVs, completed application forms or other employment checks, and requires openness to ensure applicants are aware of what information about them is being gathered, and what it will be used for. Collecting information about an applicant covertly, for example, trawling social media, to assist in the selection process, is unlikely to be justified. In some cases, other laws apply restrict the information that can be requested, such as the Rehabilitation of Offenders Act 2001.

Getting it right for job applicants

- Make sure adverts identify the organisation – people need to know who they are applying to. A PO Box address on its own will not identify the organisation, neither will an email address such as jobadvert@yahoo.com (lawfulness, fairness, transparency)

- Design application forms to collect enough information for the purpose of identifying suitable candidates, but do not collect more information than needed – do not ask for information that is irrelevant just because it may be useful in the future. (Data minimisation principle)

- Do not collect information from all applicants that will only be required from the person recruited – for example bank account details, NI number etc.

- Do not ask for details of criminal convictions unless the type of job requires that information to be collected. Do not ask for details of 'spent' convictions unless the post is covered by the one of the Exception Orders to the Rehabilitation of Offenders Act 2001.

- If any verification of information occurs, i.e. 'pre-employment screening', tell them this will occur, and how it will be done, particularly if this is automated profiling.

- If criminal record information is to be verified – i.e. vetting checks – you can only do this by getting a 'disclosure' from the Disclosure and Barring Service, Disclosure Scotland, Access Northern Ireland, or equivalent organisation. There are strict guidelines as to when any disclosure other than a basic disclosure or standard disclosure can be made.

- Unless disclosure is required for the post by law, the individual must consent to a disclosure being sought and made. 'Disclosures' should only be sought for the person offered the post.

    - Make sure you are entitled to seek and receive this information,
    - Strictly follow any procedures or codes of practice issued by these bodies
    - Only keep a record that a satisfactory/unsatisfactory check was made
    - Do not retain a copy of the certificate, and
    - Do not disclose the details to any person other than the individual themselves.

- Only keep information obtained during the recruitment process for as long as there is a legal requirement or clear, justifiable, business need. (Storage limitation).

    - In circumstances where the successful applicant requires a **work permit**, certain information will need to be retained until the work permit has been issued.
    - The Work Permit Committee may, if necessary, ask for information including details of the number of applicants, redacted copies of unsuccessful short-listed candidates' CVs (i.e. with identifying information such as name, address, email etc. removed).
    - The relevant personal data can be disclosed to the Work Permit Committee without breaching the data protection legislation. Further guidance on work permits is available on the Department for Enterprise's website.

- Keep the information physically secure – consider locked filing cabinets for manual information and password protection or encryption for electronic information. If the use of portable media is necessary, these should be encrypted. Access to this information should also be limited to a few key personnel. (Integrity and confidentiality).

- Use the information you collect only for selection and recruitment. If you are going to use details, such as email addresses for direct marketing or sending details of future vacancies, then explain this to the person, seeking consent to do so. (Purpose limitation & transparency)

- Make sure that those involved in recruitment and selection are aware that the data protection legislation applies.

EMPLOYEE RECORDS

The data protection legislation does not prevent the collection, maintenance and use of employment records; however, a balance must be struck between the employer's need to keep records and employees' right to respect for their private life.

Openness is key to compliance and employees must be aware of what information is being processed, and what it will be used for. Gathering information covertly is unlikely to be justified.

Getting it right for employees

- Employees' consent is not required to keep records about them, but they must be informed about the purposes for using their personal data and whether, and to whom, their personal data may be disclosed; (lawfulness, fairness, transparency)

- Ensure that access to employee records is limited to key personnel and they understand that the data protection rules apply;

- Check what records are being kept about employees –
    - Are they accurate and up to date?
    - Is more than the minimum information necessary held?
    - Is there a legitimate business need or legal requirement for the information?

- Let employees check their records periodically – this will allow mistakes to be identified and rectified and keep the information up to date;

- Be wary when asked to disclose information in an employment record – make sure you know who you are disclosing to and that they have a legitimate right to ask for that information;

- There are legal requirements to provide certain information, for example, Income Tax Division. The data protection legislation does not prevent the supply of relevant information where there is an obligation to provide it;

- Do not provide a confidential reference or similar information unless you are sure that the employee would agree to this – if in doubt ask them. If you provide a reference this should be fair and accurate and should not contain any negligent misstatement about the person;

- Keep employee records secure;

- Particular records:

    - Sickness records – are details of sickness held separately from a simple record of absence and accessible only by key personnel?
    - Pension or insurance scheme – this information should only be used for this purpose and employees should be aware of what information is passed between the employer and the pension scheme provider or insurer.

- Equal opportunities monitoring – if you collect special category data about disability, race or sexuality, this should be anonymised as far as possible, so that it does not identify particular employees.

- Right of access to personal data

  The data protection legislation provides individuals with a legal right of access to their personal data. **This legal right is a backstop**. If an employer is open, permits employees to check their personnel file and provides copies of documents on request, there should be no need for employees to exercise their legal right. If an employee (or ex-employee) finds it necessary to exercise their right of access, guidance on complying with that right is on the website.

- Other rights

  Employees may exercise any of their rights under the data protection legislation and employers must comply with those rights. Guidance on rights is on the website.

MONITORING EMPLOYEES

If you monitor your employees by collecting or using information about them, the data protection legislation will apply.

This can happen for example where CCTV permanently monitors compliance with health and safety rules, telephone logs are checked to detect excessive private use, email or internet usage is monitored, swipe card or biometric access systems are installed, or vehicle tracking systems or lone worker monitoring systems are used.

Employees should be made aware of any monitoring you undertake and the reasons for it, unless in the exceptional, limited circumstances where covert monitoring is necessary.

A data protection impact assessment will be required before commencing any new monitoring activity. Controllers must be able to demonstrate compliance with the data protection legislation when undertaking any monitoring.

- The data protection legislation does not generally prevent routine monitoring, but does require you to be open and transparent with your employees about these activities and ensure there is an appropriate ground for processing.

- Some monitoring activities are to protect your employees, such continuous monitoring to ensure health and safety rules to protect them are being adhered to (for example in dangerous or hazardous working conditions).

- Monitoring must be proportionate to the intended aim, not adversely impact the privacy of the individuals and be justifiable.

Considerations:

- Automated monitoring systems (such as email monitoring) are usually less intrusive;
- Email is a business tool and some personal use of the email account may be permitted by some employers; be wary when opening employees' emails if they clearly show that they are private or confidential;
- Target video monitoring appropriately, avoid toilets, changing rooms etc.
- Audio recording (other than business phone calls where this is necessary or is legally required) is unlikely to be justifiable.

- It would be generally unfair to tell employees that monitoring is being undertaken for one purpose and subsequently use the information obtained for another purpose.

    - Only use the information obtained through monitoring for the purpose for which you carried out the monitoring, unless the monitoring leads to the discovery of activity that no employer could reasonably be expected to ignore, for example breaches of health and safety rules that put other workers at risk.

    - It should not be used in disciplinary matters that are unrelated to the purpose for monitoring, for example, information obtaining through monitoring employees for health and safety purposes should not be used for employee time-keeping disciplinary matters.

- Keep the information obtained through monitoring for no longer than necessary and ensure that it is held securely with access limited to key personnel. If it is utilised in disciplinary matters, then it will not be required to be kept following the conclusion of that matter.

Covert monitoring (including audio recording)can rarely be justified and it may be appropriate to seek legal advice.

However, if there are substantial grounds for suspecting that criminal activity or equivalent malpractice is occurring, such matters should be reported to the police for investigation. Covert monitoring may require authorisation by the Surveillance Commissioner. If authorised as part of a specific investigation, covert monitoring should occur only for the shortest time necessary. Do not use covert monitoring in areas such as toilets.

Getting it right for employees

- Make sure monitoring is lawful.

- Make sure your employees know **why** they are being monitored.

- Make sure your employees are aware, and regularly reminded, that they are being monitored.

  This may, for example, be through employee handbook, warnings on computers at log in. signage in vehicles, notices on notice-boards, email reminders, staff meetings.