Employees - recruitment, records and monitoring

information commissioner
Barrantagh Fysseree

This guidance has been produced to help organisations comply with the Data Protection Act (DPA) when recruiting and employing workers. It is relevant to public sector employers, commercial enterprises and to organisations, such as charities, that use volunteers or unpaid workers.

The DPA applies to information about living, identifiable people. This includes employees, volunteers and job applicants. It applies to computerised information that is about individuals, such as emails, CCTV, monitoring equipment, psychometric tests, word-processed documents and spreadsheets etc., and manual records that are held in structured filing systems.

The DPA regulates the way in which information about individuals is collected, handled, used and destroyed. The Data Protection Principles set out these rules and further information on the principles is available on our website and in our Brief Guide. The DPA also gives individuals rights, including access to their information, and compensation if things go wrong.

THE RECRUITMENT AND SELECTION PROCESS

The DPA does not prevent you from recruiting employees effectively, 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 you collect or use about people as part of your recruitment or selection process, for example, CVs, completed application forms or other employment checks you undertake, and requires openness on your part to ensure that applicants are aware of what information about them is being gathered, and what it will be used for. Gathering information about an applicant covertly, for example, trawling social media, to assist in your selection process is unlikely to be justified.

Getting it right for job applicants

- Make sure your advert identifies the organisation properly – 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

- Design your application form to collect enough information for the purpose of identifying suitable candidates, but do not collect more information than you need – do not ask for information that is irrelevant just because it may be useful in the future. The less information you have, the less damage can be caused if the information is lost.

- 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 this is justified by the type of job you are recruiting for. 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 you are going to verify the information a person provides, i.e. 'pre-employment screening', tell them that this will occur, and how it will be done.

- If you intend to verify criminal record information – i.e. do a vetting check – 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. Depending on the level of disclosure required, the individual themselves may be required to make the application.

  Unless disclosure is required by law, the individual must consent to a disclosure being sought and made, and such disclosures should only be sought for the person who has been 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 hold on to the detailed information, 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 clear business need for it. Please see our guidance on the fifth data protection principle for more information on the retention of personal data.

  - 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 you to supply, amongst other things, details of the number of applicants and copies of the CV's of the unsuccessful short-listed candidates in redacted form (i.e. with identifying information such as name, address, email etc. removed).
  - This information can be disclosed to the Work Permit Committee without breaching the DPA. Further guidance on work permits is available on the Department of Economic Development's website.

- Keep the information physically secure – consider locked filing cabinets for manual information and password protection or encryption for computerised 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. Please see our guidance on the seventh data protection principle for more information about protecting personal data.

- 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 you must explain this to the person, seeking consent to do so.

- Make sure that those involved in recruitment and selection are aware that the data protection rules apply and handle personal information with respect. Treat other people's personal information in exactly the same way you would expect your personal information to be treated.

EMPLOYEE RECORDS

The DPA does not prevent you from collecting, maintaining and using 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 the key to complying with the DPA and workers should be aware of what information is being collected, and what is will be used for. Gathering information covertly is unlikely to be justified.

Getting it right for employees

- You do not need to get the consent of employees to keep records about them, but make sure they know how you will use the records and whether, and to whom, you may disclose the information they contain;

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

- Check what records are being kept about employees –
    - Are they accurate and up to date?
    - Is there irrelevant or excessive information held?
    - Is the information still needed for a legitimate business need or legal obligation?

- 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 you are 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;

- You will be legally required to provide certain information under other relevant legislation, for example to the Income Tax Division. The DPA does not prevent you from doing this, but you should be careful to only supply the relevant information;

- 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 sensitive information about disability, race or sexuality, this should be anonymised as far as possible, so that it does not identify particular employees.

- Right of access

  The DPA provides individuals with a legal right of access to their personal data. This legal right is a backstop. If an employer is open with their employees and permits staff to check their personnel file for accuracy and provide copies of documents on request, there should be no need for employees to exercise their legal right of access.

  If an employee finds it necessary to exercise their right of access, there is comprehensive guidance available on the website to assist you in complying with your obligations under the DPA.

MONITORING EMPLOYEES

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

This can happen for example when you check telephone logs to detect excessive private use, monitor emails or internet usage, install swipe card or biometric access systems, use vehicle tracking systems or lone worker monitoring systems.

A customer for a business's services or products, for example contract cleaning services, may try to impose a condition requiring the supplier to monitor its workers, for example requiring that workers are vetted. If this monitoring involves processing personal data, it will not be justified simply because it is a condition of business. As the employer, and data controller, it is your responsibility to ensure that you comply with the DPA when processing the personal data of your employees; no obligation to process the personal data of your employees can be imposed on you by contract.

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.

Covert monitoring can rarely be justified, unless for example, there are real grounds for believing that criminal activity or equivalent malpractice is occurring and that telling people about the monitoring would make it difficult to prevent or detect such wrongdoing.

Covert monitoring must be authorised at the highest level and should only be undertaken as part of a specific investigation and stopped once the investigation has been completed. Do not use covert monitoring in areas such as toilets or private offices, unless you have real grounds to suspect serious crime and intend to involve the police.

- The DPA does not generally prevent routine monitoring, but does require you to be open with your employees about these activities.

- Some of these monitoring activities are to protect your employees, or to ensure that health and safety rules are being adhered to.

- Monitoring must be proportionate to the intended aim, not adversely impact the privacy of the individuals and be justified by its benefit to the employer.

  Considerations:
  - Automated monitoring systems are usually less intrusive
  - Be wary when opening emails, particularly if they clearly show that they are private or confidential;
  - Target video or audio monitoring appropriately, avoiding areas such toilets, changing rooms etc.
  - If it is necessary to monitor email accounts or voicemail of employees during their absence, make sure they are aware of this.

- 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 employee 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.

Getting it right for employees

- 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

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

  - If this is to enforce your rules and standards, make sure employees know what these rules and standards are, and that you stick to them. For example if your rules impose a complete ban on internet use, being seen to 'turn a blind eye' to a limited amount of activity may mean that you cannot rely on the complete ban as justification for monitoring.

Further guidance on employers' obligations

The Department of Economic Development's website contains guidance on employment rights.