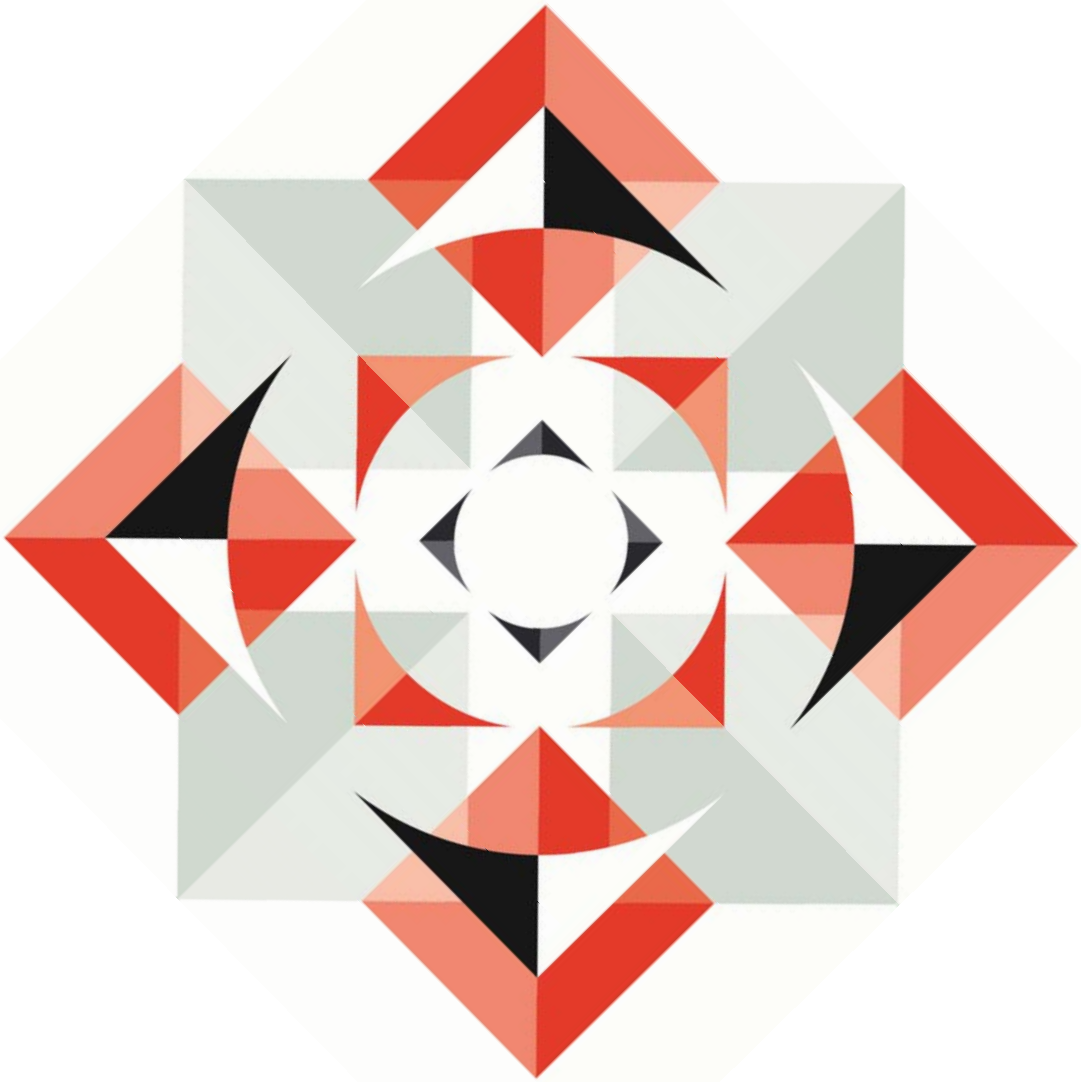
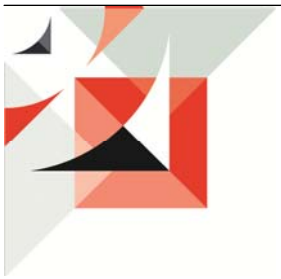
Ius Laboris UK Global HR Lawyers
LEWIS SILKIN

Data protection and employment



Inside



Introduction

Data protection legislation aims to protect privacy. Organisations using and processing personal data must do so fairly and properly.

The legislation is bolstered by giving individuals the right to know what personal data is held on them. The scope of the law is very wide, creating significant practical problems for employers. The Information Commissioner (the ICO) is increasingly using its powers to take enforcement action meaning that data protection compliance is necessarily becoming a higher priority for many organisations.

This Inbrief provides a general summary of the impact of data protection legislation on employers.

Basic concepts

Data controller is the person who has control of the purposes and way in which personal data are processed.

Data is information processed on computer (including e-mails and word processing files) and information held within organised manual filing systems. Data held in a paper format without any coherent structure would not be covered: Manual files must be organised in such a way that it is possible to search for specific information about a particular individual. A shorthand test is whether a competent temporary worker could find the information easily. Some but not all personnel files will meet this test. It is important to remember that data includes not only centrally held information but also information held by line managers.

Personal data is data relating to a living individual who is identifiable from the data itself (or from the data read with other information). It includes not only facts but also opinions ('poor performer') and intentions ('promote next year'). It does not include every mention of a person's name. The information must be biographical in a significant sense, so that it affects the individual's privacy.

Processing involves obtaining, holding and using data, and changing and deleting it. Thus, everything an organisation might do to data is processing.

Sensitive personal data. Some personal data is treated as a special category of sensitive data to which more stringent conditions apply. This includes data relating to ethnic origin, health, sex life and sexuality, criminal offences and allegations of such offences, religious opinions and membership of a trade union.

Data protection principles

All data controllers must comply with good practice rules known as data protection principles. In summary, data must:

- be processed fairly and lawfully and in compliance with statutory conditions
- be obtained only for specified and lawful purposes and must not be processed in any manner incompatible with those purposes
- be adequate, relevant and not excessive in relation to the purposes for which processed
- not be kept longer than is necessary for those purposes
- be accurate and kept up to date
- be processed in accordance with the rights of subjects
- be protected against unauthorised or unlawful processing and against accidental loss or damage
- not be transferred outside the EEA unless there is adequate protection

Compliance with the data protection principles in practice

Awareness of the purpose for which data is collected and processed is central to any understanding of how data protection law works in practice and how to comply with it.

Fair processing information

Data controllers are required to ensure that individuals on whom they hold or are about to hold data have or are given 'fair processing information'. This is information as to:

- the identity of the data controller (i.e. the employer)
- the purposes for which data is to be processed
- any further information which is necessary to enable processing of data to be fair

As a rule of thumb, this information needs to be full and address all the purposes for which an organisation collects and processes data, the more unexpected the intended use of the data, the more information will need to be given.

For example, it is obvious that salary details will be passed to the employer's bank for purposes of payroll and little, if anything, needs to be said about that. If an employer passed information on salary to a direct marketing business, however, it would be necessary to tell the employee in advance, although that would not be the end of it; there would be other compliance hurdles to be met as well.

More detailed information needs to be given about sensitive personal data than non-sensitive data.

In an employment context, it is a good idea to develop general policy statements to be given to employees and other "data subjects" such as contractors, setting out information about what you collect and why, what you might do with that data, how long you retain it, who it is shared with and why and whether it is transferred overseas. Transfers to third party processors or associated companies are often overlooked but staff need to be informed.

Specific information will also need to be given in certain contexts, such as on online recruitment pages, or when collecting health information, or to inform employees of the type of monitoring activities you undertake, for example if you "monitor" social media.

Simply asking an employee to consent in a contractual document does not meet this requirement at all as full information must be provided.

Accuracy and retention

In a personnel context, the requirement that data is accurate can cause problems. A member of staff may dispute a record and say it is not accurate: claiming, for example, that a statement that his or her performance is poor is not accurate. If this happens, the principle is not broken provided the employer has taken reasonable steps to ensure the accuracy of the data and has added details of any dispute to the data.

A related issue is retention; HR systems should ensure that personal data is not retained for longer than necessary for the purposes you have identified.

Data Security

All data controllers have a responsibility to ensure the security of the personal data they hold. Data security issues are increasingly an issue for employers as so much information is carried around, and accessed, using mobile devices.

A range of measures will be appropriate ranging from physical security measures (locks, access controls) to sophisticated technological solutions. As many data security breaches occur due to human action or error, ensuring that the workforce receives targeted training and guidance about their responsibilities when handling personal data, is a pre-requisite.

When data is passed to third party processors, such as payroll agents, the employer retains responsibility for it. Specific measures need to be taken to ensure that security requirements are met such as vetting the service provider and imposing contractual obligations upon them.

Transfer outside the EEA

Data must not be transferred outside the EEA (the EU plus Norway, Iceland and Liechtenstein) unless there is adequate protection in the receiving state. Since very few countries outside the EEA have adequate protection (not even the USA), there are exceptions permitting disclosure outside the EEA. Your organisation's approach to, and reliance on, these exceptions should be given careful thought. Over reliance on consent, for example, can backfire.

Statutory conditions for processing

As well as providing fair processing information, data controllers must ensure that they comply with statutory conditions for processing.

At least one of the statutory conditions for processing ordinary personal data must be satisfied. These include:

> showing that processing is necessary for the purpose of the legitimate interests of the employer balanced against prejudice to the rights, freedoms and legitimate interests of the data subject

> that the individual has given informed consent

> that processing is necessary for the performance of a contract or for compliance with statutory obligations

For sensitive personal data or when data is transferred outside the EEA, there are additional restrictive conditions which must also be satisfied. They include:

> the individual has given explicit and informed consent

processing is necessary for the purpose of rights or obligations conferred by law in relation to employment.

Subject access requests

An individual's right to make a data subject access request to find out what information a data controller holds about him or her is a central plank of data protection legislation. An individual making a subject access request is entitled to be told by a data controller whether personal data is being processed and, if so, to be given a description of that data including:

> the purposes for which the personal data is processed

> to whom the data may be disclosed

> the information comprising personal data

> any information available to the data controller on the source of the data

In other words, the individual can find out what information is held, where it comes from (the source) and to whom it is disclosed (the recipient).

In other words, the individual can find out what information is held, where it comes from (the source) and to whom it is disclosed (the recipient).

Handling a data subject access request

Subject access requests must be made in writing. Before complying, data controllers are entitled to a fee of up to £10 and to information confirming the identity of the individual.

A data controller must comply with a subject access request promptly and, in any case, within 40 days of receipt of the request or, if later, within 40 days of receipt of the £10 fee, of evidence to confirm the identity of the individual and of any information necessary to locate the information sought.

In some circumstances, the data controller may be clear as to the identity of the individual making the request (e.g. where an employee personally hands a request to HR). In other circumstances, the position may be less clear - it is then essential to check that the individual is who he or she claims to be.

What information to provide

An individual is entitled to be given a copy of information constituting personal data of which he is subject. Although it is normally easiest to supply a photocopy of a document, there is no obligation to provide the document itself; it is the information constituting personal data that must be supplied. It is permissible to create a new document setting out the information constituting personal data.

Third party information

Since data protection law aims to protect privacy, there are complex rules about a subject access request which might result in disclosure of information relating to another individual (a "third party").

The data controller should supply as much information as can be supplied without disclosing the identity of the third party.

The data controller may seek the consent of the third party to disclosing the information. If the third party consents, the data controller must disclose the information. There is however no obligation to seek consent.

Whether the data controller seeks consent, it must disclose the information if it is reasonable in all the circumstances to comply with the request without consent.

What happens if we do not comply?

If a data controller ignores data protection legislation, the Information Commissioner, the statutory regulator, has wide powers to take enforcement action. The Commissioner can impose fines of up to £500,000 on data controllers that knowingly or recklessly commit serious breaches of the data protection principles. In some circumstances, non-compliance is a criminal offence. Individuals affected may also have claims for damages and be able to obtain court orders requiring compliance.

What to do in practice

The Code of Practice prepared by the Information Commissioner is a really good starting point for guidance . This is available on the Information Commissioner's website at www.ico.gov.uk. In addition:

- Appoint someone with responsibility for ensuring compliance
- Audit the data you hold and what you do with it, who has access to it and how secure it is, how long you keep it, and why, who it is shared with, and why, and so on
- Provide fair processing information by preparing a statement or statements setting out the purposes for which data is processed and anything else necessary for fairness (e.g. unexpected disclosures)
- Ensure you provide such information in all contexts in which data is collected e.g. online recruitment portals
- Audit IT usage policies, BYOD and social media policies, to check sufficient information is given about processing in those contexts, and in particular any monitoring you undertake, security features, and the implications of the loss of hand held devices
- Train employees about handling data and target training to certain groups such as HR who have specific responsibilities
- Consider how to log and track subject access requests
- Audit your contracts with third party provides:
  - Do they meet security requirements?

For further information on this subject please contact:

Ellen Temperton
Partner
T + 44 (0) 20 7074 8424
ellen.temperton@lewissilkin.com

Alex Milner-Smith
Managing Associate
T + 44 (0) 20 7074 8196
alex.milnersmith@lewissilkin.com