

Data protection

How the law protects you from organisations misusing your personal details



Overview

From junk mail to government records, any organisation holding personal information that relates to you must use that data in a fair and proper way. The General Data Protection Regulation (GDPR) provides the legal framework for this protection. GDPR came into force on 25 May 2018 when the Data Protection Act 1998 ceased to have effect.

The GDPR is supported by the Data Protection Act 2018 in the UK. This factsheet gives an overview of the GDPR, and also highlights some of the data protection issues which might arise in the context of the employment relationship.

When does the GDPR apply?

The GDPR applies when personal data or sensitive personal data is held or processed on a computer (or other electronic equipment) or in some form of manual or paper files (where this comprises a 'relevant filing system'). The person whose personal data is held is called the 'data subject', and the person or organisation processing that data is called the 'data controller'.

What constitutes personal and sensitive personal data?

Personal data is information which relates to an identifiable living individual, and includes opinion as well as fact. The Courts have determined that data would only be related to a living individual if the data affected a person's privacy in some way. A person's name is personal data within definition of the GDPR.

This means that the mere mention of someone's name in a document will not compromise personal data.

However, information that has been manipulated with a view to concealing the identity of living individuals will nevertheless constitute 'personal data' where the individuals can still be identified by the data controller.

Sensitive personal data is information about an individual which relates to particularly sensitive subjects. These can include racial or ethnic origin, political opinion, religious beliefs, health, sex life, criminal convictions and trade union membership. More extensive responsibilities relate to the processing of sensitive personal data.

Processing

Processing personal and sensitive personal data is very widely defined, to include obtaining, recording, amending, holding or deleting information.

What is a relevant filing system?

The GDPR applies to information held in a 'relevant filing system'. This system could be electronic or manual as long as the structure is such that the information is readily accessible. The Courts have established that only highly structured files would fall within this definition. If documents are placed in a filing system in

chronological order, it is unlikely that they would fall within the definition of 'data'. However if the accessibility of personal data is similar to that of a computer, they will probably be covered.

Obligations imposed by the GDPR

Data protection principles - The organisation processing the information must comply with the seven data protection principles. This is a legal requirement, not just suggested best practice.

The seven principles state that data must be:

1. Processed fairly and lawfully and in a transparent manner
2. Obtained and processed for specified purposes
3. Adequate, relevant, not excessive
4. Accurate, up to date
5. Held for no longer than is necessary
6. Kept secure
7. Processed in such a manner that the data controller can demonstrate compliance with these principals.

Contact us:

Telephone: 0800 916 9015

Email: enquiries@slatergordon.co.uk

Website: slatergordon.co.uk

Lawful processing

The key data protection principle is the first in the above list - lawfulness, fairness and transparency.

The GDPR requires at least one of the following conditions to be met for processing of personal information to be fair:

- The individual has consented
- Processing is necessary to perform a contract with the individual
- Processing is required to comply with a legal obligation
- Processing is necessary to protect the individual's vital interests
- Processing is necessary to carry out public functions such as the administration of justice
- Processing is necessary to pursue the organisation's legitimate interests and does not prejudice the individual's rights.

For fair processing of sensitive personal data, one of several additional conditions must also be met. These include:

- The individual has given explicit consent
- Processing is necessary for performing a legal duty in connection with employment
- Processing is carried out in the course of the legitimate activities of a non-profit organisation
- The processing is necessary in connection with legal proceedings or the administration of justice
- The processing is undertaken by a health professional for necessary medical purposes
- Any processing of personal data or sensitive personal data which is carried out without meeting the required conditions will be unlawful.

Data subject access rights

This is probably the best known of the rights under the GDPR. The subject of personal data has the right to see information which is held about them, for example, employment records, so long as the GDPR applies to the information in question. There are also a number of exemptions, such as information held for the purposes of preventing/detecting crime.

A data subject access request may be made to any organisation processing personal data. The request should be made in writing, and the organisation must respond without undue delay and in any event within one month of receiving the request.

The information which the organisation is obliged to provide includes:

- A description of all personal information held on the individual and its sources
- A copy of all the information held including an explanation of any codes used
- The purposes for which the information is being held or processed
- Likely recipients of any data which is being disclosed.

A data subject access request can be used to obtain a copy of your personnel file or even specific emails in relation to disciplinary or grievance proceedings.

If you are affected by the way personal information has been processed, you can ask the Information Commissioner to make an assessment of whether the GDPR has been breached.

The Information Commissioner is appointed by the government to oversee the GDPR and the Freedom of Information Act 2000 (FOI). The FOI relates to information held by public authorities. Under the FOI, any individual or organisation can request information held by a public

authority. The public authority must tell the applicant (normally within 20 working days) whether it holds the information. The authority must then supply the information unless it claims the information is exempt.

The Information Commissioner has also issued an employment practice Data Protection Code. Whilst not legally binding, failing to comply with it may be cited in any enforcement notice for non-compliance with the GDPR. The code and an assessment application form are available on the Commissioner's website at: www.ico.org.uk.

Some implications for employees

The GDPR may be relevant in many employment situations, some of the most common include:

References - There are rather complicated access provisions regarding confidential references. The GDPR distinguishes between the person giving the reference and the person receiving the reference. As far as an employer giving the reference is concerned, the GDPR makes an exemption so they are not obliged to release details of a confidential reference which they have written. The exemption does not apply to the person receiving the reference, but an employer is allowed to take steps to protect the identity of third parties (such as the writer of the reference).

Access to references received should be allowed, so long as releasing the reference does not identify a third party.

In protecting a third party, the employer should consider whether steps could be taken to keep their identity secret (for example by blanking out a name). If this kind of measure would not be sufficient - perhaps the content of the reference would make it clear who provided it - the employer must consider whether it is reasonable to withhold it. In practice, many employers or

Contact us:

Telephone: 0800 916 9015

Email: enquiries@slatergordon.co.uk

Website: slatergordon.co.uk

Data protection

prospective employers are reluctant to disclose references.

Recruitment and record keeping

- Individuals should be aware who they are giving their details to and how they will be used. For instance, recruitment agencies should always obtain consent before passing details on to a prospective employer. Only information which is necessary to enable a recruitment decision should be sought. Applicants should also be told if the employer intends to seek information about them from another source, for example if references are to be sought. Part 1 of the code deals with recruitment and selection and Part 2 deals with record keeping in employment.

Monitoring of employee communications

- Employers monitoring telephone calls, email messages and internet access must comply with the Regulation of Investigatory Powers Act 2000. The provisions of the GDPR may also apply to this type of monitoring, and to other activities such as call logging or recording the numbers of emails sent.

Whether the GDPR applies will depend on how the monitoring is carried out and the records kept. Furthermore, employers who obtain information about their employees by monitoring must also comply with the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, which make it lawful to intercept communications without consent so long as the interception is carried out solely for the purposes of monitoring, or keeping a record of, communications which are relevant to the business.

Part 3 of the code covers monitoring at work, which must be lawful and fair to employees. Monitoring should not intrude unnecessarily on employees privacy or autonomy at work.

The benefit from such monitoring should be carefully weighed against the adverse impact on employees.

The code recommends that monitoring should not be used if the adverse impact on staff is out of proportion to the specific business purpose for which the monitoring is introduced.

The code provides that employers should be open about the use of monitoring; it states that covert monitoring can only be justified in very limited circumstances. The Commissioner recommends that a policy should be in place to explain how and why monitoring of personal calls, emails and internet access is undertaken.

Medical testing

If records of medical tests carried out on employees are retained, the provisions of the GDPR apply. Part 4 of the code covers information about workers' health. It states that an 'impact assessment' should be carried out before medical testing to meet the needs of the business, and that other less intrusive alternative measures should be considered.

If you feel your rights have been infringed

As with most areas of the law, data protection cases can be complicated and this factsheet gives only a basic overview. To ensure your case gets the maximum chance of success, it is imperative to seek expert legal advice at the outset.

The GDPR gives individuals the right to seek compensation from a Court, if they suffer damage and distress as a result of a breach of the Act.

Contact us:

Telephone: 0800 916 9015

Email: enquiries@slatergordon.co.uk

Website: slatergordon.co.uk

**Slater
Gordon**
Lawyers