Data Protection

This newsletter highlights the key legal obligations a business should consider when dealing with personal data about customers, suppliers, employees and other individuals who may be encountered during the course of business.

What is personal data?

Personal data is any information about an individual held on a computer or in organised filing systems that could identify the individual, either on its own or together with other information held by a business or third party. This may include:

- name;
- telephone number;
- email-address
- date of birth; and
- notes written about someone (such as annual performance review)

The individual could be a potential or actual employee, customer or supplier, or possibly someone captured on a business' CCTV footage.

Penalties for failure to deal with personal data properly?

Misuse of personal data could have serious financial, commercial and reputational implications for a business, including possible criminal penalties and fines.

Protecting and securing personal data?

Personal data needs to be protected and kept secure. Particular care must be taken with sensitive personal data, for example, medical records, as more restrictive requirements apply to this type of data.

Collecting personal data?

- A business must have a **legitimate reason** for collecting personal data (for example, because a new employee is joining the business).
- When a business collects data on an individual, the business must tell the individual what it intends to do with that data. If the purpose for which the business collects the data changes, the individual must again be informed.
- A business must only collect the information it requires at that particular time. In other words, a business cannot collect personal data it believes it may require at some point in the future.
- If a business wishes to use the personal data for marketing purposes, the individual must be informed. A business will generally

If you would like to discuss any of the matters raised in this newsletter please contact:

Mark Austin
mda@blackgraf.com

Tel: 020 7586 1141

The information in this newsletter is not meant as a substitute for advice on particular issues and is written in general terms. You should seek specific advice before taking any action based on the information in this newsletter.

Black Graf LLP 100 Baker Street London W1U 6WG
Black Graf LLP is a Limited Liability Partnership registered in England and Wales registration no: OC334046. Any reference to a partner is to a member of Black Graf LLP. Authorised and regulated by the Solicitors Regulation Authority no: 488394
www.blackgraf.com

This newsletter outlines the law as it stands at the date of writing in December 2014.

need the individual's explicit consent for email, fax and text marketing.

Using data collected on individuals?

A business is generally allowed to use an individual's personal data if that individual has given their express consent.
The data can also be used in other circumstances, for example, if the business:

- Needs to use the data to fulfil a contract with a customer (such as using their address to deliver goods to them); or
- Has a legitimate interest in using it, although this must be balanced with the individual's rights. For example, if part of a business has been sold to a third party and the business needs to transfer customer data to it.

- Data should only be used for the reason for which it was collected.
- If a business wants a third party to manage the personal data that business has collected, it should take legal advice. The business will still be responsible for protecting the data.
- If a business wants to transfer any personal data outside the European Economic Area, that business should take legal advice.
- Where a business is considering using sensitive personal data, that business should take legal advice.

Storing personal data?

All personal data held must be accurate and up-to-date. Data should only be held for as long as it is required and for the reason it was collected. Databases should be regularly updated and out-of-date information should be deleted.

Keeping data secure and confidential?

Personal data must be kept secure at all times (for example, computers and files should be password protected) and data being sent somewhere else should be sent in a secure way. Personal data must also be disposed of securely and any security breach must be reported to an appropriate person.

Enquiries about personal data?

Businesses should have a system in place to deal with individuals who request details of the personal data that business holds on them. A business is permitted to charge an admin fee of up to £10 for responding to this type of request.
This type of request should usually be dealt with by an employee who has responsibility for data protection issues.