Black Graf solicitors LLP

Data Protection and Direct Marketing

This newsletter highlights the key data protection issues a business should consider when carrying out direct marketing, including how a business should collect information about its customers and how to communicate information about the business' products and services to existing customers and potential customers.

Penalties for failure to comply?

- Serious financial, commercial and reputational issues for the business, including possible criminal penalties.
- A negative impact on the ability of the business to use databases for marketing purposes.
- Reputational loss and the potential to be barred from trade bodies.

What customer data needs to be protected and secured?

- Any information about a customer that is held on computer or in an organised filing system that could identify them (for example, names, addresses or e-mail addresses).

Collecting customer data for direct marketing purposes?

- Generally, a business can only collect information if it has a good reason for doing so (for example, the business wants to market new products to the customer contact).
- A business must make sure that people are aware when the business collects their data that it may be used for marketing and other purposes. The most effective way is by issuing a fair processing notice (FPN). An FPN is a notice given to an individual to explain what the business will use their personal data for (for example, the notice may say that the business will pass the personal data to third parties for marketing purposes).

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

Derek Aarons
da@blackgraf.com

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 February 2015.

- If a business has a website and intends to collect data using it, the website should include a prominent privacy statement with an FPN.

- Always take legal advice if the business is planning to collect bank or credit card details, as there are security implications.

Storing customer data for marketing purposes?

- Businesses must ensure that personal information is kept secure at all times (for example, data stored on mobile devices should be kept to a minimum).

- Regularly review databases to ensure that data is accurate and up-to-date.

- A business must make sure customer data is only stored for the purpose it is collected and only for as long as it is required (for example, do not keep an event delegate list for marketing purposes unless delegates were aware that their details could be used for marketing purposes and were given the opportunity to opt out).

Opting in and opting out?

- A business must ensure that people are always given the opportunity to opt in or out of receiving marketing from the business. The business should make this as simple as possible (for example, clicking an unsubscribe link in an e-mail).

- Retain details of any opt-out requests the business receives, so that the individuals who have opted out in the past are not contacted in the future (this is known as "suppressing" the details). If a business simply deletes their details, the business may obtain their data later from another source and will not know that they have opted out of marketing contact.

- Avoid contacting someone who has opted out, unless they are being contacted for another purpose (for example, sending a bill). In this instance, it would be acceptable to include a message from time to time stating that the business would like to send them marketing material and invite them to opt back in.

- It is not generally acceptable to include pre-ticked opt-in boxes or to rely on silence as an indication to opt in. Positive action is required from a customer (for example, returning a

form).

Sending solicited marketing?

- If an individual or company has contacted a business requesting marketing material, the business can send it out even if they are included in an opt-out list or have registered with a preference service. A preference service holds the details of people who do not wish to receive direct marketing material.

- Individuals and businesses can register with preference services to indicate that they do not wish to receive direct marketing by a particular means (for example, by mail or telephone).

Sending unsolicited marketing by post or telephone?

- A business can contact individuals and companies on its databases by post or telephone, unless they have stated that they do not wish to receive direct marketing.

- Before sending out marketing, the business must check whether an individual or company has opted out or signed up to the telephone preference service. It is good practice to check the mail preference service as well.

Sending unsolicited marketing by SMS, fax or e-mail?

- A business will generally need explicit consent from individuals (including named individuals at a company), but not businesses, to send unsolicited marketing by SMS, fax or e-mail.

- Before sending out marketing to individuals (including named individuals at a company) the business should check that they have given specific consent and that they have not opted out or signed up to a relevant preference service.

- Before sending out marketing to a company, the business must check that they have not opted out or signed up to a relevant preference service.

- If a business has collected a customer's SMS or e-mail details when selling something to them or negotiating to sell something to them, the business can use those details in future to market the same or similar products to them without prior express consent. This is known as the "soft opt in".

- Businesses are required by law to check databases against the relevant preference service regularly and comply with the preference.

Using external databases?

- A business should always take legal advice if it is considering purchasing an external database to make sure that it gets the rights the business needs to use it effectively.
- Before a business can use the data, the business must introduce itself to the new customer and explain how it intends to use their data (for example, by issuing an FPN). In cases where the business requires explicit consent for marketing purposes (SMS, e-mail and fax marketing to individuals) the customer must give consent.
- Always check whether any of the customers on the database that the business purchased have signed up to any preference services.
- The business should also check the details on the new database against existing databases to see whether anybody has opted out.
- Although the business may agree with the supplier that it will not supply the bought-in data to any other party, there is generally no way to prevent others from collecting the same data themselves or from sourcing them from somewhere else.
- Bought-in data may not be appropriate for use in targeted marketing campaigns or when data mining.

Selling databases to a third party?

- A business may be able to sell or transfer a database if it has all the customers' consent or it is in the business' legitimate interest (for example, if it is part of a merger).
- Always take legal advice before selling a database. A business will need to put a formal agreement in place as the business will still be responsible for protecting the data.

Allowing third party access to data held by the business?

- A business may want to allow a third party to manage data it

holds (for example, using a fulfilment house or a call centre).

- Always take legal advice before allowing a third party access to the data. The business will need a formal agreement in place to deal with confidentiality and security of the data. This applies even if the third party is a group company.