Black Graf solicitors LLP

Data Protection and Direct Marketing

This newsletter gives an overview of key data protection issues a business should consider when carrying out direct marketing.

What customer data needs to be protected?

Any information held on a computer or in an organised filing system which could be used to identify the customer – *for example, names, addresses*

Penalties for failure to comply with data protection legislation include:-

- Possible criminal penalties, as well as serious financial, commercial and reputational consequences for the business.
- Potentially being barred from trade bodies

When can a business collect customer data?

Generally, only if the business has a good reason for doing so – *for example, to market a new product to customers*

When a business collects customer data, that business MUST make customers aware that their data may be used for marketing purposes – *one way of doing this is to issue a fair processing notice (FPN). For example, telling the customer that their data will be passed to third parties for marketing purposes.*

If a business intends to collect customer data via its website, the website should include a prominent privacy statement, along with an FPN. – *if the business intends to collect bank or credit card details via its website, there are further security implications and the business should take legal advice.*

How to store customer data?

- Customer data must be kept secure at all times.
- Data should be reviewed regularly, to ensure that it is up-to-date and relevant, as well as to confirm that the business still has a good reason for holding the data.

If you would like to discuss any of the matters raised in this newsletter or other commercial issues, 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

Allowing customers to opt in and out?

A business must allow customers to easily opt in and out of receiving direct marketing from that business – *opting in or out should be made as easy as possible, for example, adding an 'unsubscribe' link to the bottom of emails to customers.*

A business should retain copies of any customer requests to opt out of direct marketing, so that the business does not accidentally contact the customer again in the future.

A business should not continue to contact customers who have opted out of receiving direct marketing, unless necessary to do so – *for example, because the business needs to send a bill to the customer.*

NB. A business should not rely on pre-ticked opt in boxes. Nor should a business rely on silence as an indication of opt in. Customers should be required to take positive steps to confirm that they opt in for direct marketing.

Solicited marketing?

If a customer approaches a business and requests marketing materials then the business can provide these, even if that customer has opted out of direct marketing.

Preference services hold details of customers who do not wish to receive direct marketing.

Preference services can be used to store details of individuals who do not wish to receive direct marketing by particular means, for example, by telephone.

Unsolicited marketing by telephone or post?

A business can contact customers via the telephone or post for direct marketing purposes, unless that customer has expressly opted out of direct marketing.

Unsolicited marketing by SMS, fax or email?

Generally, a business will need express consent from individual customers, including named individuals at companies, before sending unsolicited marketing by SMS, fax or email.

Generally, there is no need for express consent from customers who are businesses themselves, UNLESS the customer has expressly opted out of direct marketing.

HOWEVER, if a business has collected a customer's SMS or email details when selling or trying to sell them a product in the past, the business can use these details to market the same or similar products to that customer in the future, WITHOUT prior express consent ('soft opt in').

External database?

A business should always take legal advice before buying an external database of customer information.

A business must introduce itself to customers before using their data – *for example, by sending an FPN* - and must obtain the customers' express consent where applicable.

A business must check existing databases, to ensure that customers have not opted out of direct marketing in the past.

Selling a database to a third party?

A business should always take legal advice before selling a database of customer information.

A business will still be responsible for protecting the data contained within its sold database, unless a formal agreement is put in place.

A database can only be sold if the business has the consent of all the customers whose details are held on the database, or if the sale is in the legitimate interests of the business – *for example, because the business is being sold.*

Allowing third parties access to a database?

For example, a business may wish for a third party to manage its database. A business should always take legal advice in these circumstances, as controls will have to be put in place to deal with issues such as confidentiality.