

Data protection and direct marketing

This checklist highlights the key data protection issues your business should consider when carrying out direct marketing. It explains how your business should collect information about your customers (including individual customers, named individuals within a business and businesses themselves) and how to communicate information about your products and services to existing and potential customers.

What are the penalties for failing to comply?

- Serious financial, commercial and reputational issues for your business, including possible criminal penalties.
- A negative impact on the ability of your 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 marketing purposes

- Generally, your business can only collect information if it has a good reason for doing so (for example, you want to market new products to the customer contact).
- Make sure that people are aware when your business collects their data that it may be used for marketing and other purposes. The most effective way of getting this is by issuing a fair processing notice (FPN). An FPN is a notice given to an individual to explain what their personal data will be used for (for example, the notice may say that the personal data will be passed to third parties for marketing purposes).
- If your 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 your business is planning to collect bank or credit card details, as there are security implications.

Storing customer data for marketing purposes

- Ensure that personal information is kept secure at all times (for example, data stored on mobile devices should be kept to a minimum).
- Regularly “spring-clean” databases to ensure that data is accurate and up-to-date.
- 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

- Always give people the opportunity to opt in or out of receiving marketing from your business. This should be made as simple as possible (for example, clicking an unsubscribe link in an e-mail).
- Retain details of any opt-out requests you receive 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 you simply delete their details, you 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 your 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 your business requesting marketing material, you 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

- Your 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, your 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

- Your 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) your 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, your business must check that they have not opted out or signed up to a relevant preference service.

- If your business has collected a customer's SMS or e-mail details when selling something to them or negotiating to sell something to them, you 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".
- Your business is required by law to check databases against the relevant preference service regularly and comply with the preference.

Using external databases

- Your business should always take legal advice if it is considering purchasing an external database to make sure that you get the rights you need to use it effectively.
- The best way to ensure that your business can use the data is to contact the new customer by issuing an FPN to introduce your business and explain how you intend to use their data. In cases where your 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 your business purchased have signed up to any preference services.
- Your business should also check the details on the new database against existing databases to see whether anybody has opted out.

Selling databases to a third party

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

Allowing third party access to data held by your business

- Your 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. You 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.