The New Data Protection Law
A Basic Guide

By Chris Stoddard, LLB

2005 Edition

This PDF file can be printed on any computer printer, you have our permission to forward this booklet to any colleagues you think might be affected by this law.

Provided as a public service by DRF Group LTD.

The New Data Protection Law - a Basic Guide

DRF Group Ltd. has prepared this basic guide to the main provisions of the new Data Protection Act (referred to as "the Act" in this booklet) as it affects fundraising. Most of it came into force on October 23rd 2001.

The Act contains many other provisions, mostly unrelated specifically to fundraising and it is advisable that you familiarise yourself with the Act as a whole, once you have a grasp of the main provisions discussed in this booklet.

DRF Group Ltd. provides specialist fundraising services to charities of all sizes. We have a particular expertise in developing support from individual donors at all levels of giving from small regular donations to major gifts and legacies. To find out more, please visit our website at: http://www.drfgroup.co.uk

DRF Group Ltd. - a specialist fundraising consultancy

We have taken care to summarise the position under the Act as accurately as possible, but are not holding ourselves out as specialist advisers on Data Protection or any legal matters. Where methods to secure compliance are suggested, these are not the only methods available and legal advice, on the facts, should be taken. It would be unreasonable for readers to treat the information in this book as advice from a lawyer and readers concerned about Data Protection issues should consider taking legal advice. Readers downloading this document accept they are doing so on these terms.

DRF Group Ltd., 2430 The Quadrant, Aztec West, Bristol, BS 32 4AQ. T. 01454 878573 F. 878673
Email. manager@drfgroup.co.uk

Contents

DRF Group Ltd.
2440, The Quadrant, Aztec West
Almondsbury, Bristol BS32 4AQ
Phone: (0) 1454-878-573
Fax: (0) 1454-878-673

http://www.drfgroup.co.uk

Updates since last edition

The following updates to Data Protection Law and guidance from the Information Commissioner are incorporated in to this revised issue of this Guide:

1. A better definition of "direct marketing" is incorporated

2. Extensive clarification of what counts as valid "consent" to the use and processing of an individual's personal data has been given

3. New rules are in force governing communication by email, text messaging, video messaging, "robot" phone calling and other forms of electronic communication.

4. The Commissioner has given guidance on the question whether a pre-existing relationship or specifically given consent is overridden by registration under the Mailing or Telephone Preference Services or whether the existing relationship or consent takes precedence.

The basic rules

Rule

If you are processing personal data you must comply with the Act.

What information is covered by the new law

Personal data.
This means any information about any identified – or identifiable - individual and includes their name, address, and phone number. [Go to page 8 for more detail on this]

Processing.
Processing is very widely defined, and includes any gathering, exchanging, storage or handling of data, whether on computer storage or on paper database. [Go to page 8 for more detail on this] Individuals have **rights** to prevent you 'processing' information about them, especially for direct marketing. [Go to page 11 for more detail on this]

What are the obligations on Charities?

A Charity will be a data controller if it is processing personal data. It must therefore register as a data controller with the UK Information Commissioner for all data processing activities which it carries out.

Eight Data Protection Principles underpin the Act in order for the processing to be legal. [Go to page 17 for more detail on this.] To briefly summarise, a charity must have grounds for processing the data within the meaning of the Act and must notify data subjects that their data is being processed and why and how it will be used.

Who has to ensure compliance?

The charity and its trustees, as responsible officers acting on behalf of the Charity, have to ensure compliance with the Act. Some breaches of the Act may, in certain circumstances, amount to criminal offences by the trustees personally.

Direct Marketing

The Act does give data subjects the right to object to direct marketing – most usually effected by giving the data subject the right to opt out of receiving direct marketing. Various other regulations will apply to direct marketing, depending on the medium used [see page 8 for further details]

The definitions of direct marketing and what constitutes valid "consent" have been clarified by the Information Commissioner [see page 9]

Action summary

- Treat all data as covered rather than try to pick holes in the legislation to avoid its provisions.
- To ensure your organisation complies with the Act, set up procedures for all employees to follow when obtaining data and subsequently using it and back rules up with disciplinary procedures.
- Publish a Data Protection Policy and incorporate this in communications with people you hold data on, so that they can have confidence in your organisation.

- Create a simple but comprehensive form that tells the individual all he/she needs to know about the data you hold or where and how that will be used and gives clear opportunity to, at least, “opt out” of receiving direct marketing.

- When direct marketing, keep an eye on the various registers to which data subjects can subscribe, to opt out of receiving direct marketing. Cleanse your lists regularly and note the restrictions on use of automated calling systems.

Fair obtaining and processing ("the Fair Processing Code")

Rule

Processing must be "fair and lawful"
The first limb of this rule is that a charity must ensure that it has grounds for processing personal data, pursuant to the Act. Some organisations rely on the consent of a data subject for this; others rely on their right to process personal data in pursuance of their "legitimate interests": the ambit of the latter is less clear, however, and what will comprise pursuance of its legitimate interests will be a question of fact for each organisation. Many companies prefer the "certainty" of obtaining consent, particularly when their activities include direct marketing [see later on page 13].

Rule

Transparency of data subjects
The second limb of the rule on "fair and lawful processing" is that every person has the right to fair treatment regarding data "processed" about him or her. This means that he or she should be provided with the "fair processing information", namely:

- that you are processing their personal information
- the purposes for which it is processed
- any other relevant information.

These two rules are collectively known as the "fair processing code". There are further rules about the quality and quantity of information that can lawfully be kept and used and how long it may be kept and used. [For detailed information on this go to page 10].

How to ensure consent

Written consent. The best way to be absolutely sure that the individual has consented to processing by the charity of its personal data (including for direct marketing) is to obtain a signature from the data subject agreeing to the keeping and use of a clearly defined set of information about him or her. We call this a Data Protection Statement.

A specimen Data Protection Statement is provided at page 26.

Implied consent? There are situations where it can probably be taken that an individual has impliedly given their consent to further use of information about them. For example if they have been a regular donor by standing order, there is a good case to argue that they have consented to you writing to invite them to renew their standing order when it expires. Or you could add a statement that you intend to write to them in these terms in the papers initially sent out to the donor, when the financial donation is processed.

Note that consent can however be withdrawn at any time and best practice dictates that records are regularly updated to reflect this. It is also best practice to regularly refresh consent – as consent cannot endure forever.

Three ways of getting information

Newly obtained from the person him or herself. If you obtain information directly from the data subject, the best thing to do is to include a Data Protection Statement reasonably prominently on the form on which the information is requested, which should also satisfy the transparency requirement of the fair processing code.

From someone else. If you obtain information from a third party (such as a list broker), the fact that they (presumably) have permission to disclose it to you does not necessarily mean you have the right under the Act to use it. You must satisfy yourself that you have a valid ground for processing that data [see above at page 13] at the earliest opportunity and if that ground is consent (and you have not obtained consent directly from the data subject), then you should satisfy yourself that the third party has obtained consent to your use of that data and in respect of all the uses you intend to put the data to on your behalf. Remember that you will also need to satisfy the transparency requirement of the fair processing code and provide information [see Rule on page 8].

So, for example, if you rent or swap a mailing list, you must give a Data Protection Statement to any person on those lists when you first contact them.

Data you have had for a long time and don't use often.

Old data needs careful treatment. Bear in mind that data should be accurate, kept up to date and not held for longer than necessary, so you should satisfy yourself that these principles have been complied with. [See later on pages 13 and 14].

This means that the fact that you were once in regular contact with a donor no longer gives you permission to revive contact for the original or a new purpose – and you may not even be entitled to have kept the data for so long. Presuming you can satisfy a condition for processing however, the most sensible thing to do is to provide a Data Protection Statement when you first restore contact, and carefully note and action any objections received. So, if you plan to include a 15 year old list of life members in a special appeal, the best thing to do is to give them a Data Protection Statement with the first new contact.

"Opt in" and "opt out " tick boxes

Another way to obtain unequivocal consent would be to provide what is often called an "opt in" tick box. This is a box which the individual ticks to indicate consent to the proposed use of the data (e.g. for direct marketing and/or list swapping). By ticking the box the individual is said to be "opting in" to the proposed use. This form of indication of consent is approved by the Information Commissioner.

Less certain is the status of the widely practiced "opt out" box. Here the individual is told about the proposed use of data (e.g. direct marketing and/or list swapping) and asked to tick a box if he or she objects. In this way the individual is said to have "opted out" of the proposed use.

In Guidance notes provided during 2004 to aid interpretation of the new Privacy and Electronic Communications Regulations which came into force at the beginning of 2004, the Commissioner has provided clarification of his view on the status of "opt out" tick boxes and whether failing to tick an "opt out" box can be taken as an indication of consent. Here is what the Commissioner said : " We are concerned that the terms "opt-in" and "opt out" can be misunderstood. They are commonly taken to refer to the use of tick boxes. In this context, "opt-in" refers to a box that you tick to indicate agreement and "opt-out" refers to a box that you tick to indicate objection. Marketers have traditionally favoured the latter, e.g. where the default (an unticked "opt-out" box) indicates a failure to register an objection. The fact that someone has had an opportunity to object which they have not taken only means that they have not objected. It does not mean that they have consented….By itself, the failure to register an objection will be unlikely to constitute valid consent. However, in context, a failure to indicate objection may be **part** of the mechanism whereby a person indicates consent. For example, if you receive a clear and prominent message (i.e. not in the small print? – Editor) along the following lines, the fact that a suitable prominent opt-out box has not been ticked may help establish that consent has been given: e.g. "By submitting this registration form, you will be indicating your consent to receiving…marketing messages from us unless you have indicated an objection to receiving such messages by ticking the above box".

"Negative option" address. By extension of the above guidance, simply providing an address where the person can write to register objection to the proposed use of data is not any longer adequate. Anyone failing to write to such an address cannot be said to have consented.

Note. This guidance is given specifically in relation to electronic communications, but the law on "consent" in the Data Protection Act is the same for printed communications. Furthermore, both the Data Protection Act 1998 and the new e-commerce regulations stem from the same EC Directive (2002/58). It is clear therefore that the new guidance also applies to direct mail consent.

How long "consent" lasts

Consent is not a lifetime thing – once given never retracted. In fact it is deemed only to last "for the time being", which means that it lasts only as long as there are "solid reasons" (Information Commissioner's words) for thinking that it has not lapsed.

Action summary

- Satisfy yourself that one of the conditions for processing is satisfied. If you opt for the safest route (consent), you must get specific, informed and freely given consent to keeping and all uses to which you will put the data. In practical terms this may mean giving the person a Data Protection Statement and a statement which will also satisfy the second requirement of the Fair Processing Code lists regularly and note the restrictions on use of automated calling systems.

- Consent can also be given verbally or electronically as well as in writing, but records should be safeguarded as evidence.

- There are special rules about consent to keeping and using "sensitive data", e.g., information requested or volunteered about a medical condition, e.g. if someone voluntarily tells you they have diabetes, asthma or a disability. See pages 19 and 21 for more in this.

- Regularly review the accuracy of data held.

- Regularly review the need to hold on to the data at all.

- Check when you last gave a Data Protection Statement to any person you plan to contact. If longer than 12 months ago, it makes sense to include one at the next contact.

Carry out a Data Protection Audit

Rule

The definition of **Personal Data** adopted by the Data Protection Commissioner is so wide that if you are holding any data from which an individual is identified or identifiable, your activities will be caught by the Act.

This will include:

- Staff and volunteer record
- Membership lists
- Mailing lists of publications or Christmas cards
- Fundraising databases, including:
    - Lists of event attendees
    - Lists of donor prospects
    - Lists of trustees
    - Lists of "give as you earn" donors
    - Lists for Gift Aid

Whether it is held on computer, in paper batches in preparation for computer inputting or in manual files the rule above applies equally.

Action Summary

- Carry out a review of every list you hold on computer or paper and decide if it qualifies as "personal data".

- Review all uses to which it is put and check you are complying with the Fair Processing Code and that your data protection registration is complete.

- Apply the new guidance on "consent" to all the data you hold to make sure you have valid consent to use it in the way you plan. If unsure, re-send a suitably worded "opt-in" or very clear "opt-out".

- Ensure that the Data Protection Policy is being adhered to with each list.

- Set up a system that makes sure that any new list you create goes through this routine.

- Train employees in best practice and supplement contracts of employment with disciplinary action for breach.

- Review each list against the other Data Protection principles [see below on pages 10 and 13] and ensure you are regularly updating lists, keeping them securely and only transferring data outside the EU in appropriate circumstances.

- Carry out an audit every year to check the policy is being fully applied.

The legal restrictions obtaining, keeping and using 'Personal Data'

Rule

In addition to the rules on fair processing and the fair processing code, the Act regulates what **kind of data** you can obtain, its **quality and quantity** and for **how long** you can **keep and use** it

The rules are:

1. Data shall be processed **fairly and lawfully** [see discussion previously on page 8 in respect of the Fair Processing Code].

2. **Purpose.** You can only obtain data for one or more specified and lawful purposes. Lawful purposes include fundraising, maintaining membership and pursuing the objectives of a charity. If you are relying on consent, then you have to specify the purpose you intend for the data at the time you collect it and disclose your proper identity. Having specified the purpose or purposes for obtaining the data, you cannot use the data for other purposes unless you get consent.

3. **Data stored must be relevant and not excessive.** The data must not be more than you need for the purpose you have stated. For example, if you do not need to know a date of birth, or a subscriber's medical condition, you should not ask for it!

4. **Quality.** The data must be accurate and, where necessary, kept up to date.

5. **Duration.** The data must not be kept for longer than is necessary to achieve the purpose or purposes you have stated.

6. **Security.** Appropriate security and organisational measures must be taken against unauthorised access to the data. This covers computer security and, in respect of manual data, everyday security precaution such as locking drawers.

7. **Restrictions on transfers overseas.** Personal data may not be transferred to a country outside the EEA unless that country has adequate protection (unless an exception applies, such as where a data subject has consented to such a transfer).

8. **Rights.** The data can only be processed in a way that does not infringe the rights of individuals under the new law. Go to page 21 for more on this.

What these new rules mean in practice

The new rules mean that you cannot simply gather or keep general lists of people and then use those lists for whichever purpose comes to mind. The new law gives every individual the right to have information about them used **only for the purpose** they gave their name and other data originally. They are entitled for it to be held securely and to be told to whom it is sent, where the recipient is situated and why they are receiving it.

In practical terms, this means that, when making first contact with someone, you cannot gather **more information than you need** for the immediate purpose you have disclosed. If the real reason for your activity is to build a general database (to mail, swap, rent out, sell Christmas cards and

other merchandise to, promote legacies, invite to events etc.) you need to specify all these as your purposes, otherwise you are collecting more data than is immediately needed. You will need to be sure your registration is up to date and transparent as well.

You must **not keep data for longer than is necessary** to achieve the originally stated purpose. It is likely that keeping names of people with whom you have not had any recent contact (e.g. lapsed donors, old lists of event attendees, former volunteers) is an infringement of the new law.

Sensitive data. There are even stricter rules on collecting and using what is termed 'sensitive data'. Of special relevance to fundraising, this includes details about someone's health. The effect of the new restriction here is that you cannot collect or use information about someone's health unless they have given absolutely explicit consent for the exact use you have in mind. So, if someone fills out a questionnaire from a cancer charity disclosing that he or she has cancer you cannot use that information for, say, legacy promotion without their explicit consent to this use.

Action Summary

- If you want your investment in database building of any kind to be safe from limitation on Data Protection grounds, you need to comply fully with the new law.

- Whether you are building a large donor database or just a small list of targeted individuals for events, functions and major donor cultivation, the effect of the new law is the same.

- This means transparency in respect of all your intended uses and any possible future uses in your Data Protection statement. Go to page 26 for a sample of this.

- If you come up with a new idea for using a list originally created for a completely different purpose you have to give a new Data Protection Statement to people on that list when you first use it for the new idea you have.

Special new rules on Direct Marketing

The phrase "Direct Marketing" now has an authoritative definition provided by the Information Commissioner, in addition to that provided in the Data Protection Act 1998 itself. The Act defines "direct marketing" as "the communication (by whatever means) of any advertising or marketing material which is directed at particular individuals". Some commentators have taken this to mean that the communication had essentially to be selling something for it to be caught by the Act. Not so. The Information Commissioner has stated very clearly that it also covers the promotion of an organisation's aims and ideas and includes appeals by charities for funds

Rule

The Act provides that an individual is entitled to require a data controller not to process, or to cease processing, his personal data for the purposes of direct marketing. As mentioned above, this is usually interpreted as asking a data subject to opt in or out of receipt of unsolicited direct mail, in its various mediums.

This applies, whether contact is by way of appeals, newsletters, Christmas card sales, merchandise catalogue, volunteer registration or any other kind of postal communication that is marketing a service or product.

It also applies whether the person has existing contact or not, e.g. has given to previous direct mail appeals from the charity concerned. **This is because direct mail even to previous contacts and donors is treated as "unsolicited".**

If you **swap** mailing list information with any other organisation you must not send any direct mail to any opt out names.

This is in addition to any names which have opted out of list swaps with any other organisations.

Try and buy only cleansed lists, which carry a contractual guarantee of having been cleansed, but note that such guarantees cannot enure forever, as individuals can opt out at any time.

Direct marketing by phone, fax or email is subject to other layers of regulation, also originating from the EU. In response to direct marketing by fax and telephone, the UK has established 2 services: the telephone preference service (TPS) and the fax preference service (FPS), which allow consumers to register their request not to receive direct marketing telephone calls, and bans direct marketing by way of faxes to "natural persons" (which means individuals and sole traders in the UK and partnerships in England, Wales and Northern Ireland).

The law on such direct marketing is provided by the Privacy and Electronic Communications (EC Directive) Regulations, in force from the beginning of 2004.

These regulations provide that communication by email, text, fax or automated phone call where the "voice" is recorded or simulated is all treated as "electronic communication" and governed by strict rules when used for "direct marketing".

The rules are:

1. Specific, informed and positive consent to electronic direct marketing communication must be obtained BEFORE sending any such communication.

This means obtaining a positive written indication of consent, such as a checked box. Most agree that best practice also requires a "double opt-in" where the customer is sent an acknowledgment which he or she is asked to confirm.

This applies to all communications except those covered by what the regulations call a "soft opt in", which arises from an existing relationship or set of negotiations in a commercial transaction. If relying on a "soft opt in", an opportunity to "opt out" must be given in every electronic communication. The "soft opt in" does not apply to charities and they cannot rely on an existing relationship to justify electronic communication without prior consent.

2. The sender's identity must be easily determined.

3. The sender must provide a valid address that is not high cost to use (i.e. not a premium rate phone number) so that recipients can opt out.

Direct Marketing by Telephone

- Direct marketing calls are prohibited to individuals who have notified the caller that they do not want to receive such calls or where they have been registered on the TP for 28 days or more;

- As part of all direct marketing calls, the caller must give their name, and on request, a freephone number or address by which they can be contacted;

- There are also restrictions on the use of automated calling systems.

Direct Marketing by Fax

- Sending of direct marketing faxes to "natural persons" is banned unless prior consent has been obtained. Note that "natural persons" can still register on the FPS for extra protection. More recently, the e-Commerce Directive 2000 brings in new regulations, controlling unsolicited commercial e-mail ("spam"). In particular, "spam" must be clearly and unambiguously identifiable as such as soon as they are received. Supplementing this is another set of regulations only recently approved by the EU, which also regulate direct marketing by "spam", SMS and MMS messages. Under these laws, a customer must have given specific consent (by opt-in) to direct marketing via these methods, but with an exemption where it is sent in the context of existing customer relationship, provided the e-mail addresses concerned are properly obtained (within the meaning of the EU Privacy legislation, including the Act) and that the customers are

always given the opportunity to opt out of further communications. In the UK, direct marketing by mail is regulated only on a voluntary, as opposed to statutory basis, and those charities which are members of the Direct Marketing Association will need to comply with the rules of that governing body.

Action summary

Include a clear opt out tick box in the first contact so that the individual can decide not to receive any further direct mail appeals from your organisation.

If using an "opt-out" rather than an "opt-in", make sure it complies with the new requirements set out on page 11 of this Guide.

- As an alternative to providing an opt-out on first contact, it is arguable that giving someone an address to write to so they can request an opt out form complies with the new law. The danger of going down this route is of a later ruling by the Commissioner or courts that this is not a fair practice and illegal.

- If a person ticks the opt out box they are also opting out of **list swap** ("**reciprocal"**) mailings from other charities.

Sample Data Protection Statement and direct marketing by mail

Here is an example of a tick box panel providing the consent and opt out opportunities the new law requires.

Respecting your privacy
Thank you for making contact with [name of charity]. [What your charity does] is a huge task and we need all the help we can get. That's why your support is so valuable to us and why we ask your permission to write and let you know from time to time of all the different ways you could help, including buying Christmas cards, coming to events we organise, supporting us financially and many others.

However, if you would rather not hear about these opportunities, you are welcome to let us know of your preference at any time, or by ticking this box now – and return it to us.

From time to time we may like to share mailing list information with other like-minded charities. This helps us to attract new supporters to our cause. If you would prefer us not to disclose your name to any other charity, do please let us know at any time, or by ticking this box now. [Pages 11 and 12]

If you have any concern at all about the way we respect your privacy, do please let us know by contacting [name and address of contact]. Again thank you for your support.

(NB: Extend wording for transfers outside EEA).

(NB: If you are direct marketing by phone, fax or email, take legal advice on sufficiency of wording).

Want to stay up to date?

To receive updates on this or other legislation affecting fundraising tick the 'update me' box on the Request Information page of our website: http://www.drfgroup.co.uk/findoutmore/requestinfo.lasso

DRF Group Ltd.
2440, The Quadrant, Aztec West
Almondsbury, Bristol BS32 4AQ
Phone: (0) 1454-878-573
Fax: (0) 1454-878-673

http://www.drfgroup.co.uk