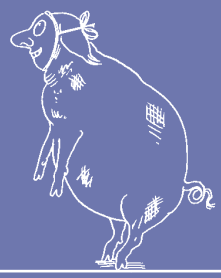
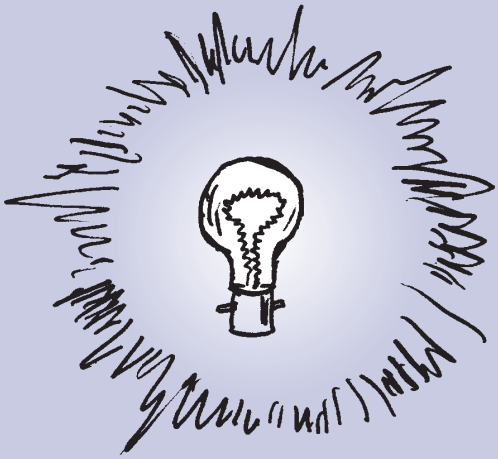
Data Protection



The 1998 Data Protection Act affects almost all voluntary organisations. However, many struggle to understand it, and worry that they might get into trouble by not complying. Or they take an over-cautious approach and allow their work to be hampered by unnecessarily tight restrictions. This guide aims to demystify the Act and give you a framework for deciding what your organisation needs to do about it.

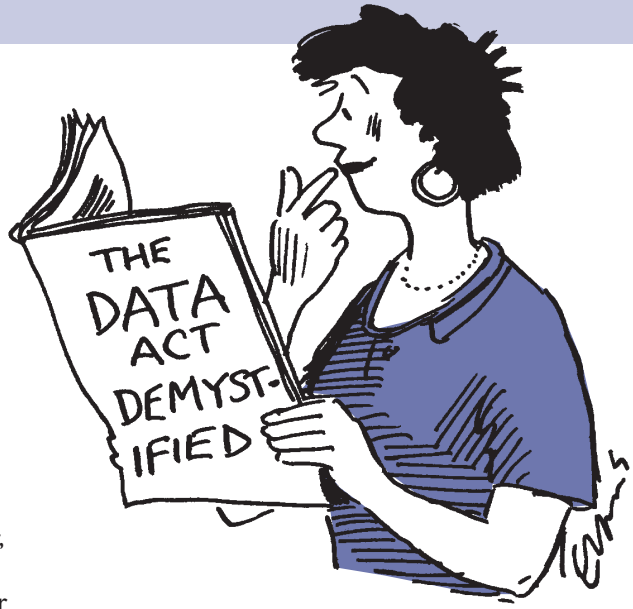


The Data Protection Act need not be a major problem. Its aims fit very closely with the concerns and culture of most voluntary organisations. In fact, seeking to apply good Data Protection practice means asking questions which can actually help to improve services or procedures. Understanding the Act can also help you to put up a challenge when your work, or your clients' lives, are frustrated by other organisations – perhaps refusing to supply information on the erroneous grounds that Data Protection prevents it, or insisting that things be done in a particular, awkward way.

What is Data Protection all about?

You must comply with the Data Protection Act, because it is the law. However, you normally have a choice about *how* to comply. It is easier to make your decisions about this if you understand what the Act is trying to achieve and what your priorities should be.

Data Protection is not about protecting data for its own sake; it is about protecting individuals from the consequences of data being misused or handled badly. This has to be your top priority. The Data Protection Act sits alongside other legislation that tells us to look after the people we come into contact with – in areas such as health and safety, child protection, discrimination, consumer protection and so on. The Data Protection Act is generally written so that it should never need to be used as a reason for doing something harmful. This does not mean that the right course of action is always clear, however, especially when it's a matter of balancing several different people's interests.



If preventing harm is the top priority, demonstrating respect for the individual comes a close second. In our information-rich society, organisations (and even individuals) can behave in intrusive, unpleasant or annoying ways if they use data without the knowledge, or against the wishes, of the individual. People are increasingly aware of this and feel strongly about it. No voluntary organisation can afford to alienate people by behaving in ways they find unacceptable.

These two themes: preventing harm and respecting the individual, run through the Act in many areas, in particular in the Data Protection Principles (see the centre pages of this guide). Before going on to discuss how to satisfy the Principles, however, we need to look at exactly what information we are talking about.

Personal data

The Data Protection Act only applies to "personal data". You probably hold other information which is not personal data but which nevertheless needs to be looked after carefully because it is confidential or important. That's fine. There is nothing to stop you having a policy which goes further than Data Protection would require – and in any case the dividing line is not always clear, so you will want to be on the safe side.

In some cases, however, you do need to know more accurately whether information is "personal data" or not – for example when responding to a formal "subject access request", which we will say more about later. You must also make sure that you do not assume certain information is outside the Act when in fact it is covered.

In order to be "personal", information must relate to an identifiable, living individual. The Court of Appeal in December 2003 decided[1] that it must also be *about* them in some way. So it's not enough just to mention someone; there has to be some additional information about them. The individual is "identifiable" if you can work out who they are in any way (for example by matching one set of data against another).

The definition of "data" is more complicated. It covers, firstly, information held on "equipment operating automatically in response to instructions given for that purpose" – in other words computers or any other computerised or programmable system.

Manual information is data if it is held in a "relevant filing system". That is a

"set of information … structured [so that] specific information relating to a particular individual is readily accessible". The Court of Appeal also considered the definition of "relevant filing system" and decided that the structure and indexing was key. It must be possible for someone with very little prior knowledge of the system to look someone up quickly and go straight to a specific piece of information about them, without having to wade through the file document by document.

Data Protection does not only apply to text. It can cover photographs, biometrics, video, CCTV or audio material; the key question is always: "is it personal and is it data?"

Records intended to go onto the computer or into a filing system are also counted as data. So the forms on which you collect information, or notes you take during an interview, would be covered as soon as you have them in your possession if the information will eventually end up on the database or in your client records, for example.

Finally, from 1 January 2005 public authorities will have to make a lot of their information available under the Freedom of Information Act 2000. Where the information relates to individuals, it will be treated as personal data, with access provided through the Data Protection Act. Health, education and social work records are already subject to slightly different rules. This Guide does not cover these specific issues.

There can be uncertainty about whether specific information is personal data or not, but it is likely that much of the information you hold about people, whether on computer or on paper, will be personal data.

With borderline material it is probably wise to take a cautious view, and treat information as personal data even if you think it may not be. There is nothing to stop you going beyond the minimum requirements of the Act, especially if the consequences of poor practice would be harmful to the individual. The key thing is to avoid assuming that things are not covered when they are. That could lead to serious mistakes.

To give a sense of how the definition of personal affects the information found in many voluntary organisations, the following tables show examples of how the two elements of "personal data" might interact. The word "probably" shows how difficult it can sometimes be to decide. Only the top left-hand box is covered by Data Protection requirements.

	Personal (probably)	Not personal (probably)
Data (probably)	• Your membership database. • A card index of your management committee members. • Most of your personnel files. • Order forms from individuals.	• An email discussing the timetable for a project. • A spreadsheet containing statistics on the types of client who used your services last year. • A database of voluntary organisations in the area, used for printing a directory.*
Not data (probably)	• A file of letters of complaint, in date order, with no index. • A set of training course files, organised course by course, where individual participants' booking forms and other details are kept.	• The plaque explaining why your centre is named after someone long dead. • The printed minutes of a meeting where they refer to someone agreeing to do something.

* But the contact details for individuals within the organisations may well be personal data.

1 Durant v Financial Services Authority [2003] EWCA Civ 1746, Court of Appeal (Civil Division)

The Data Protection Principles

Whenever you "process" personal data you must comply with all eight Data Protection Principles. By doing so you will achieve the aims of protecting individuals from harm and demonstrating respect. ("Process" means doing anything at all with information, including collecting it, storing it, using it, changing it, disclosing it or destroying it.)

The Principles are given in full on the centre pages of this Guide, with an indication of how specific Principles relate to the overall aims. In summary:

- Data 'processing' must be 'fair' and legal.
- You must obtain data only for specified purpose(s) and use it only in ways that are compatible with the purposes.
- Data must be adequate, relevant & not excessive.
- Data must be accurate & up to date.
- Data must not be held longer than necessary.
- Data Subjects' rights must be respected.
- You must have appropriate security.
- Special rules apply to transfers abroad.

Preventing harm

Your first priority must be to prevent harm to individuals through inappropriate or irresponsible use of data. The most likely sources of harm fall into three categories:

- If data you hold about someone is inaccurate or inadequate, that could result in you providing them with an inappropriate service or making the wrong decision.
- If you have poor security, or an inadequate confidentiality policy you could allow data to fall into the wrong hands.
- There are cases where you should disclose information in order to prevent harm to the individual or to someone else. You must not let misunderstandings about the Data Protection Act prevent you from doing the right thing.

The worst type of harm would be physical damage. For example, if you take clients out on a trip and record the wrong information about the dosage of someone's medicine the consequences could be severe. Or you may know someone's address or contact details; in most cases that's fairly innocuous data, but if the person is in danger of harassment or physical assault then you would have to be very careful to protect the information from being given out inappropriately.

Financial harm could result, for example, if you pay people the wrong amount because your data is inaccurate, if you give them the wrong benefits advice because you make a mistake in their case file, or if your inadequate security allows a fraudster to collect enough information about someone to perpetrate an identity theft.

Harm could be less tangible, but nevertheless serious, including embarrassment or breach of privacy. There is no reason for someone's colleagues to know why they are off work, unless they choose to say; it might be the kind of hospital visit they would rather not talk about. Service users may not want their case written up in enough detail in your newsletter for their friends to guess who the "anonymous" person was.

Harm from a failure to disclose could result in vulnerable people being put at risk because someone who could help them was unaware of the problem, or because someone behaving inappropriately was not reported in time.

Finally, the Act recognises that other countries may not offer the same protection as those in the European Union. Where data cannot be protected when you transfer it abroad, you normally need the consent of the Data Subject.

Accuracy and adequacy

The third and fourth Data Protection Principles say that data must be "adequate", "accurate" and "up to date". The test of harm gives you a way of deciding how far you need to go. A mailing list for your newsletter probably need be checked no more than once a year; if you are supporting a client in a benefits case your information must be right up to date at all times. If you want to get a rough idea of your clients' ages, tick boxes for age bands (35–45, and so on) are probably fine; pension records must have the exact date of birth.

One of the decisions you need to make, therefore – in respect of each set of data you hold – is how accurate and up to date you need to be, and how you are going to ensure that your data meets your requirements. You need to be particularly careful where information is not provided by the individual themselves. If your clients are referred from another agency, do you take the information they provide on trust, or do you check it immediately with the client? If your staff and volunteers put their own comments into a file, how do you make sure that they only record statements and information that can be substantiated?

Security

The seventh Data Protection Principle says that you must have "appropriate" security to prevent two kinds of problem:

- unauthorised access
- accidental loss or damage

The use of the word "appropriate" here relates directly to the aim of preventing harm. You need to carry out a risk assessment to see how much harm, and to how many people, would result from a breach of security, then put your main effort into preventing the most serious harm.

Before looking at security you must spell out what access is authorised. Any other access is therefore "unauthorised". Some material could be in the public domain, with no restriction on access; for this, obviously, no security might be needed. For more confidential material it is important to be clear where the boundaries of confidentiality lie: will the information a client gives you stay just with the case worker? with the case worker and their supervisor or their team? within the organisation? And despite all that, under what circumstances would you breach confidentiality in order to protect other people? Everyone benefits from this clarity: your staff and volunteers, your clients, your funders and other external agencies that you come into contact with.

Having decided who is allowed to see the information, and in what circumstances, you then must ensure that you prevent other people from seeing it. The measures you take must be "technical and organisational". Technical measures would include physical security – locks and barriers to access – and things like passwords, anti-virus software and back-up systems. Organisational measures are usually more important: training (and policies to base training on), induction, supervision and a general culture of security.

You should also think about the always thorny issue of how to encourage people to spot and own up to security breaches. Inevitably things will go wrong; the best organisations learn from their mistakes, and offer redress without being forced into it. But security breaches are usually embarrassing so the natural tendency is to hope that no one will notice.

There is a British Standard on Information Security Management (BS7799, also known as ISO 17799). While this has some useful pointers, it is more appropriate for very large organisations which need more formal systems and can afford the cost of being assessed for compliance regularly.

Although the primary responsibility for a security breach is the organisation's, an individual is committing a criminal offence, punishable by a fine, if they knowingly or recklessly access data without authorisation, knowingly or recklessly allow another person unauthorised access, or sell data accessed without authorisation.

Transfers abroad

When personal data is transferred outside the UK you must try to maintain protection if possible. There are two main ways to do this: by law, or by contract. All the countries in the European Economic Area (the 25 states of the European Union plus Norway, Iceland and Liechtenstein) are deemed to have (and generally do have) acceptable laws, as are some others, including Guernsey, the Isle of Man and Switzerland.

Alternatively you can protect the data by having an "approved" contract with the recipient organisation or, in a special provision for the USA, where the recipient has signed up to the voluntary "safe harbors" agreement.

Otherwise, you should normally get informed consent from the Data Subject for the transfer. Many people would say that this means you also need consent if you are going to publish any personal data on your web site, unless you can control where it goes or who sees it.

Breaking confidentiality

Most of the time your staff and volunteers need to have a cautious approach. If you give information out inappropriately there is no way of getting it back, whereas if you hold off giving it out while you check, you can then give the information if it turns out to be the right thing. Provided you minimise any delay, this is the safest course of action.

However, it is important to realise that the Data Protection Act does not impose a blanket ban on disclosure, even where you do it without the knowledge or consent of the Data Subject. Where harm to anyone – whether your Data Subject or not – would result from keeping data to yourself, you should consider whether the potential harm is serious enough to make disclosure the right thing.

The Act says specifically that in effect Data Protection is not breached:

- if another law requires you to provide information, or
- if you choose to disclose information because not doing so would prejudice crime prevention, catching criminals or collecting taxes or duties.

In either case the disclosure can be on your own initiative – because you spot a problem and decide to report child protection concerns, a breach of care standards or a suspected fraud, for example – or at the request of an official agency.

Where you are approached for information, it is reasonable for you to expect the request to meet certain conditions:

- It should normally be in writing.
- It should identify the basis for the request: are you being asked for help, or is there a law requiring it? If the latter, the requesting agency should be able to spell out where their power originates.
- The individual making the request should be authorised to do so: either by seniority, by the department they work in, or by name.

Whenever you contemplate a breach of confidentiality you should have a procedure for discussing it internally and

approving it, in writing, at the appropriate senior level.

The question of when you need consent for disclosures is discussed below.

If things go wrong

If, despite your best efforts, things go wrong and you end up causing harm, the Data Subject affected has several avenues for redress. These include:

- requiring you to stop causing them harm
- Subject Access
- "Assessment" by the Information Commissioner
- correction, deletion or clarification
- compensation
- informing those who have received wrong information.

If an individual believes that they are being harmed by your use of data about them, they can require you, in writing, to stop. You then have 21 days to stop, or give them a reason why not (which is not necessarily the end of the story). This provision is restricted to certain situations, so if you receive a demand to stop harming someone you should, of course, take it seriously, but also take advice so that you know the full legal position.

A more commonly-exercised – but still quite rare – right is that of Subject Access. This gives the Data Subject the right to see the information you hold about them, so that they can check that it is adequate, accurate and so on. Again there are restrictions, discussed below. Although this right has up to now not been exercised very often, especially in voluntary organisations, that does not mean it cannot happen. And it is an important protection for the Data Subject when things go wrong.

Having made a Subject Access request (if appropriate), a Data Subject who believes that they are being harmed by a breach of Data Protection can ask the Information Commissioner to make an "Assessment" of whether Data Protection is in fact being breached. The Commissioner must then, by law, make an "Assessment", and has various powers to assist in enquiring into the situation. More information on the procedures and policies of the Commissioner is available on their web site, *www.informationcommissioner.gov.uk*.

The Commissioner can only say that a breach of Data Protection has occurred. If the Data Subject wants tangible redress – assuming you don't offer it voluntarily – they have to take you to court. The court can order:

- correction, deletion or clarification of the offending information;
- compensation for actual harm suffered, and for "associated distress", but not normally for distress on its own;
- that anyone to whom wrong information has been disclosed must be informed, so that they can take corrective action, too.

Subject Access

The basic provision under Subject Access is that you must provide a permanent copy of all the personal data that you held about that person at the time their application was made. This could include printing out information held on computer and copying information held on paper.

You can make a charge for Subject Access, but it must not be more than £10, regardless of any photocopying costs you incur.

If you have to deal with a Subject Access request, it is important to take it seriously, but not to be panicked into acting too hastily. You have to reply as soon as possible, but the statutory time limit is 40 calendar days. Unless you are absolutely sure that there is nothing controversial in the data, and no uncertainty about which information you should release, you should take qualified legal advice.

You should not release information in response to a Subject Access request, unless it is personal data, but on the other hand you have to make your best effort to find all the personal data your organisation holds about that individual. You then have to check whether you are entitled, or expected, to hold back any of the data on other grounds. These could include not disclosing information about your intentions in relation to any current negotiations (such as restructuring plans for the organisation) and, in particular, not disclosing information that would breach someone else's confidentiality (the "third party" exemption).

In relation to Subject Access a third party is anyone who is mentioned in the information – another member of the Data Subject's family, for example – or anyone outside your organisation who is the source of the information – such as a referee for a job, or someone making a complaint. Where possible third party information should be released, if it is

Preventing harm

Data Protection is unlikely to prevent you from passing on information in order to prevent serious harm. See the Conditions in Schedules 2 & 3 that might allow you to disclose data without consent.

People must know enough about what you are doing with their data, so that they can alert you to any possible harm, for example if you pass it on in ways that they would not want you to.

When you are making decisions about people or providing a service, you must have enough data to ensure that you are not missing a crucial piece of information.

When you are making decisions about people or providing a service, your data must be accurate and up to date enough not to harm them.

People have the right to check the data you hold about them.

If your data handling causes harm to people you have to put things right and may have to pay compensation.

You must make sure that people are not harmed by their information falling into the hands of inappropriate people through your poor security.

You must make sure that people are not harmed by you losing crucial data.

If you transfer information abroad, you must be clear about whether it will stay protected and, if not, get consent from the Data Subject.

The Data Protec

1 Personal data shall be pro
and, in particular, shall no

(a) at least one of the co
met, and

(b) in the case of sensitiv
of the conditions in S

2 Personal data shall be obt
specified and lawful purpo
further processed in any
that purpose or those pu

3 Personal data shall be ade
excessive in relation to th
which they are processed

4 Personal data shall be acc
kept up to date.

5 Personal data processed f
shall not be kept for longe
purpose or those purpos

6 Personal data shall be pro
the rights of data subjects

7 Appropriate technical and
shall be taken against una
processing of personal da
loss or destruction of, or

8 Personal data shall not be
territory outside the Euro
that country or territory
protection for the rights a
in relation to the process

ction Principles

ocessed fairly and lawfully
t be processed unless –

nditions in Schedule 2 is

e personal data, at least one
chedule 3 is also met.

tained only for one or more
oses, and shall not be
manner incompatible with
rposes.

equate, relevant and not
he purpose or purposes for
.

urate and, where necessary,

for any purpose or purposes
er than is necessary for that
es.

ocessed in accordance with
s under this Act.

d organisational measures
uthorised or unlawful
ta and against accidental
damage to, personal data.

e transferred to a country or
opean Economic Area unless
ensures an adequate level of
nd freedoms of data subjects
ing of personal data.

Showing respect

People must know enough about what you are doing with their data that they get no unpleasant surprises. You must not go behind their backs or keep them deliberately in the dark.

You must consider whether you need consent for what you want to do. If not, you must be sure that you meet one of the other conditions. This is particularly important if you are collecting or using "sensitive" data.

You should give people the chance to opt out of their data being shared with other organisations.

You must be clear about why you are collecting information and must not collect information for one purpose then use it for something completely different.

You must not ask for intrusive types or amounts of data.

You must not hold on to information once you no longer have a use for it, provided you meet statutory retention periods.

You must offer people the chance to opt out of receiving any kind of marketing material.

If someone tells you to stop sending them marketing material you must comply.

You should normally get consent before you put people's details on your web site.

reasonable to do so (for example if it is information the Data Subject already knows), or if the third party has given their consent. But if the third party has refused consent then in most cases the information that identifies them must be withheld.

This is only a brief summary of the Subject Access provisions. The key points are:

- Take it seriously but don't panic.
- Take advice.
- Don't record information unless you are confident that you could justify it being in the file should someone make a Subject Access request.
- Decide in advance your policy on whether to charge or not.

Acting for others

Everyone has their own individual Data Protection rights. (Even a married couple do not automatically have the right to see information about each other.) However, people can act on behalf of someone else. For example, someone might ask a solicitor to make a Subject Access request on their behalf, or a parent might act on behalf of a young child.

Anyone acting on behalf of another must be authorised and must be acting in their interests. Where the person is not acting on their own behalf because of incapacity (due to age, illness or mental condition, for example) it can be difficult to establish the appropriate authority, and you should seek qualified advice if you are in any doubt.

The situation with children is slightly clearer in Scotland, where children are expected to be able to exercise their own Data Protection rights from the age of 12. In England and Wales there is no specific provision, it depends on the particular child's capacity to understand, but one would need to consider the possibility of a child exercising their rights independently of their parents once they get to around 12.

Showing respect for the individual

The main elements which demonstrate respect for the individual are:

- fairness
- information
- choice
- not being intrusive
- not keeping information unnecessarily.

The first three of these come from the first two Data Protection Principles, which say that all "processing" (see above) of personal data must be fair, and only for specified purposes.

People understandably do not like feeling tricked into providing information that they would not have given if they had realised how it would be used. In particular they do not like information being passed on to other people or organisations where they were not aware that this would happen, or information being used to send junk mail or make annoying sales telephone calls.

So the key to getting people on your side is "transparency" – making sure that they have enough information about what is going on, and don't feel that you are keeping them in the dark or going behind their backs. If they know the score, they are much more likely to trust you, and much less likely to complain.

Where possible, you should give them a choice over whether to provide you with information in the first place (especially if you can manage without it) or whether to allow you to use it in particular ways.

This does not mean that everything depends on the consent of the Data Subject. There are many things you can legitimately do without consent, provided you take the interests of the Data Subject into account.

One area where you have no option about allowing people a choice is marketing. Data Subjects have the right, under the Data Protection Act to insist that you do not use their data for marketing or appealing for funds.

As well as making the provision of information optional if possible, you must not ask intrusive or unnecessary questions. All your data must be "relevant and not excessive". And you should not hang on to information once you no longer need it (but make sure to comply with statutory retention periods).

Transparency

Transparency lies at the heart of the 1998 Act. Under the previous (1984) Act, the legitimacy of processing was assured by registering the purpose with

the Data Protection Registrar (now the Information Commissioner). Under the current Act, legitimacy is assured by being transparent with the Data Subject – guaranteeing that they get no unpleasant surprises from your use of their data.

Specifically, they must know who is collecting their data and why, who else it might be passed on to, and how to raise any concerns or exercise their specific rights. The reason for this is clear: if the Data Subject has no knowledge, or insufficient knowledge, of what is happening, they have no basis for raising any concerns they might have and the organisation might take actions that cause harm unwittingly.

You do not, however, have to tell people things they already know, or are reasonably likely to know. The information must be available if they ask, but you only have to go out of your way to tell them things that are not obvious. Examples would be where you intend to keep their information for a different purpose (such as marketing) after they might expect you to have finished with it, or where you are likely to pass the information on to other organisations.

How you tell people, again, is up to you. A notice in your waiting room or a short paragraph in your newsletter might do the trick. Or you could put a standard paragraph on your membership form or in your welcome letter. The important thing is that people end up knowing enough about what you are doing. In particular, you must allow them to judge whether any of your activities might pose a threat to them – for example if you propose to publish information that would identify them and put them in danger. Unless they know what you are up to, they will not be able to alert you to the problem and enable you to avoid the risk of causing them harm.

This new emphasis on transparency means that many voluntary organisations need to look carefully at what they do. Although you may have client or member involvement on your agenda, you may want to think about whether it goes as far as it should.

There is a common-sense provision which says that you need not meet the transparency requirement if you got the data from a third party *and* it would involve you in disproportionate effort. This means, for example, that you can usually use information that is in the public domain without telling the person concerned.

Consent

In addition to transparency there is a second plank to fairness: meeting one of the Act's Schedule 2 (or 'Fair processing') Conditions. This is where consent comes in. However, consent is only one of the six Conditions, and all processing must meet at least one, not all of them.

In summary the Fair Processing Conditions say that you can only process data:

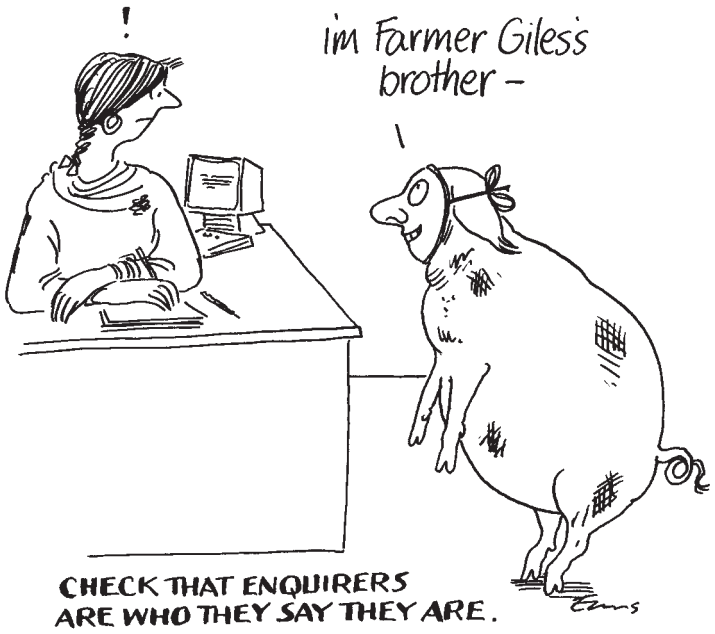
- with the consent of the Data Subject, or
- if the processing is necessary for a contract involving the Data Subject, or
- to meet a legal obligation, or
- to protect the Data Subject's "vital interests", or
- for a range of government and official functions, or
- if it is in your "legitimate interests" (or the interests of whoever you disclose information to) provided the Data Subject's rights, freedoms and interests are not infringed.

Very few organisations will find difficulty in meeting at least one of these conditions for their normal activities. You need to bear two things in mind, though. Firstly, if you are relying on consent, it must be a genuine choice. You must not appear to offer the choice, but then when someone says "no" turn round and say "we don't need your consent because we meet one of the other conditions". That would not be fair. Secondly, if someone has specifically asked you not to do something with their data you would have to be that much more certain that you really do meet one of the conditions, since you obviously don't have consent. (For example, if they say "take me off your database", you might be able to justify keeping them there – as part of your client records or financial records, for example – but guarantee not to use the information for any further activity.)

If you do decide to get consent, it must be specific, informed and freely given. One implication is that you cannot get genuine consent unless you have met the transparency requirements. Consent need not be in writing, but you may feel that written consent is worth getting in case you need evidence subsequently. Normally consent can be implied, provided the Data Subject has taken some clear action, such as filling in a form, in the full knowledge of how the information would be used.

Disclosure and data sharing

It is not unknown for organisations to allow their activities to be hampered by a mistaken belief that they need consent in situations where it is certainly an option but not mandatory. If you feel that a disclosure would prevent serious harm to the Data Subject, for example,



you are unlikely to need consent (although you should try to inform the Data Subject about the disclosure).

In many other cases you may feel that a disclosure is appropriate because the Data Subject knows it might happen and will not be harmed. You should check that the disclosure is "compatible" with the purposes that you hold the data for, however. Some organisations have felt uncomfortable disclosing information about clients to funders, for example, where this was not made clear at the outset and declared as a purpose. You should also check that a person asking you for information is who they say they are, if necessary by phoning back on a public number, or by getting the request on headed paper.

If you share data with other organisations routinely, you should make sure to tell the Data Subjects that this is what happens. Unless it is essential for the service you should ideally give them the chance to opt out of their data being shared. Otherwise they may choose not to give you information at all, which could leave them worse off.

You should also consider setting up a data sharing protocol with any organisations that you regularly share data with. You don't want to end up getting into trouble for a mistake that they make, and it is easy for two organisations to see the same situation in different ways without realising it. See also the discussion of who might be a Data Controller in these circumstances in the section *Who is responsible for what.*

Marketing

Direct marketing is defined in the Data Protection Act, but not in a way that is particularly helpful to voluntary organisations. It is clear that obvious marketing – such as promoting goods, publications, training or other services – is included, as is fundraising and related activities. Provision of information about a topic, rather than promoting your organisation, is probably not marketing, but the boundary is unclear. Also, the marketing must be directed to individuals, which presumably means that marketing your services to organisations is not covered.

Where you think you are collecting information that you will use for direct marketing you must, of course, specify marketing as a purpose. You must also offer the appropriate opt ins and opt outs. Although this is not the only way to do it, the simplest strategy for many organisations is to:

- Offer an opt out from:
  - mailings
  - sharing the data with other organisations
- Ask people to opt in to:
  - phone or fax marketing (where there are mandatory preference services)
  - email or text message marketing

Marketing by any electronic means is controlled by the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003 No. 2426), which came into effect on 11 December 2003. These tidy up the pre-existing restrictions on marketing by phone and fax (including the Telephone and Fax Preference Services), as well as extending restrictions to some email and text message marketing.

Under the Regulations, the Telephone Preference Service continues to operate (but from 25 June 2004 open to organisations as well as individuals), as does the Fax Preference Service. It is illegal to make a marketing phone call or send a marketing fax to anyone whose number is on the relevant preference service Register. To avoid having to check your numbers against the Register every time (which costs money), it is often easier to call or fax only those people and organisations who have given you permission. This overrides any entry in the Register. See *www.dma.org.uk/Shared/Consumer.asp* for more on all the preference services, including the voluntary Mailing Preference Service.

The Information Commissioner has adopted a fairly relaxed approach to the use of email details that were collected before the Regulations came into force. For a limited period it appears that you can use these to send advertising or marketing material, in the absence of a positive opt-in, provided every message includes clear instructions on how to opt out.

Whether you have offered opt outs or opt ins, the Data Subject has the right to "require" you in writing to stop using their details for any kind of marketing. Whether you offer a flexible range of options or not, your system must at the very least be able to cope with those occasions when the Data Subject insists on not receiving any further marketing.

'Sensitive' data

The Data Protection Act recognises a special class of data which it terms "sensitive". The list of "sensitive data" covers the Data Subject's:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- Trade Union membership;
- physical or mental health or condition;
- sexual life;
- offences, alleged offences and court proceedings.

People may be sensitive about other information, but there is no special provision for anything except the list above.

If you want to use sensitive data you are more likely to need consent from the Data Subject. However, this is not always needed, provided you meet one of the Conditions in Schedule 3 of the Act, supplemented by additional Conditions in Statutory Instrument 2000 No. 417. The list is long, but each Condition is quite specific. Since there is insufficient space to cover these in detail here, you may need to get further information if you want to use sensitive data without consent. Some of the possible Conditions you might meet are, in brief:

- legal requirements in connection with employment;
- to protect the vital interests of the Data Subject or another person;
- Church, Union & political party membership, subject to certain safeguards;
- where the information has been deliberately publicised by the Data Subject;
- where you are providing legal advice;
- various government and official functions;
- where you are providing medical care and owe a duty of confidentiality;
- where you are carrying out equalities monitoring based on race or ethnicity, disability or religion;
- where you need the information in order to provide a confidential service, including but not restricted to counselling, advice or support, and it is not possible to get consent, or it is reasonable not to have consent, or seeking consent would prejudice the provision of the service.

The last Condition (which can be found in the Statutory Instrument) is worth considering where the Data Subject's interests are protected by confidentiality and you want to focus on providing an immediate service to someone who is in distress or incapacitated, rather than going through the motions of getting consent.

Who is responsible for what

Legal responsibility for Data Protection lies with the "Data Controller".
In nearly every case this will be your organisation, not an individual worker or volunteer. However, you cannot choose to be a Data Controller on behalf of another organisation (for example a trading company that is separate from your charity).

You may well want to delegate Data Protection activities within your organisation to a specific Data Protection Officer. However, the responsibility still lies with the organisation and, ultimately, the Board of Trustees or Management Committee.

Where you operate within an information-sharing consortium you may need to take advice on who is the Data Controller, because any one of three situations is possible:

- Each organisation is an independent Data Controller and they just pass data between them.
- Each organisation is a separate Data Controller but they are *jointly* responsible for the data, and could get into trouble for other organisations' mistakes.
- The consortium itself is a Data Controller, independent of its constituent bodies.

Your organisation keeps its Data Protection responsibilities even if it outsources work. An organisation that processes personal data on behalf of another is a "Data Processor". This could include, for example, a payroll bureau, a mailing house, a telephone marketing company, or a company which develops or supports your membership database or your web site.

Under the Data Protection Act you must have a written contract with the Data Processor, spelling out what they are to do for you. They must have appropriate security, to your satisfaction, so that you can be confident that their treatment of your Data Subjects will be just as responsible and reliable as if you were doing it yourself. For instance, if your staff have to have Criminal Records Bureau checks, should theirs?

Notification

Many voluntary organisations have received letters telling them that they risk immediate prosecution for not Registering under the Data Protection Act, and must pay a fee of £95 or more to an official-sounding agency with a name such as the "Data Protection Registration Service". This is a scam, although like many scams it does have a kernel of truth.

Some Data Controllers do have to "Notify" the Information Commissioner about their information-processing activities, at a cost of £35 a year. However, many systems and activities are exempt from Notification. This means that they are still subject to all the requirements set out in the rest of this Guide; the only thing they are exempt from is Notification itself. The main exemptions from Notification are:

- all manual systems;
- computerised personnel systems, including payroll & volunteer administration;

- computerised accounts and customer or supplier records;
- your own computer-based marketing, promotion & PR activities;
- computerised membership records of a non-profit organisation, or records relating to activities provided for people who are "regularly in contact" with your organisation "in connection with" your purposes. In some cases this might include service users or clients.

Since you are permitted to Notify voluntarily, even if you are exempt, many organisations take the view that £35 a year is a relatively cheap option when you consider that failing to Notify if you should is a criminal offence. The Information Commissioner publishes a free *Notification Handbook* and runs a Notification helpline (01625 545740) as well as having information on the web site.

More information

The **Information Commissioner** provides free information, on the web, by telephone and through a series of publications. This is always worth consulting, although it does not necessarily directly address the concerns of voluntary organisations.

www.informationcommissioner.gov.uk
01625 545700

Political responsibility for Data Protection issues lies with the **Department for Constitutional Affairs**:

www.dca.gov.uk

Data Protection in Voluntary Organisations, Paul Ticher, Directory of Social Change (020 7209 5151), 2nd edition, £14.95
ISBN 1 903991 19 6

Much of the action you need to take will have been obvious from the preceding discussion. It may be useful to summarise some of the key issues:

Priority 1: Preventing harm

- How do we make sure all our data is accurate enough to prevent harm?
- Have we got an appropriate confidentiality policy, making clear who is allowed to see or be given which information?
- Have we got an appropriate security policy?
- How do we ensure that our policies are followed?
- How will we ensure that we learn from security breaches?
- Do we get consent for transfers abroad, where necessary?
- Are we clear about the basis on which we can disclose information when this is necessary to prevent harm?

Priority 2:

- Are we giving our Data Subjects enough information about the use we make of their data?
- Are we giving them choices in the way we use their data, whenever appropriate?
- Are we ensuring that the data we hold is relevant and not intrusive?
- Do we have clear retention policies for our main sets of data?
- Are we being particularly thoughtful in our use of 'sensitive' data?
- Have we thought through any data sharing arrangements?

Priority 3:

- Are we offering the appropriate opt-outs from direct marketing and opt-ins for electronic marketing?
- Do we know how to respond to a Subject Access request?
- Have we checked whether we need to "Notify" the Information Commissioner about the scope of our use of personal data?
- Have we identified any Data Processors we use and checked our contracts with them?

action checklist

Lasa Computanews Guides

Lasa's Information Systems Team publish a series of Computanews Guides. These clearly written booklets cover many aspects of computer use and answer common queries.

Guides currently available

(at £5 each)

Buying IT

•

The Internet

•

Managing IT

•

Networks

(available as a free PDF download – see www.lasa.org.uk/computanews/guides.shtml)

Project Management

•

Security

For further details contact:

Lasa Publications
Universal House
88–94 Wentworth Street
London E1 7SA
TELEPHONE: 020 7377 2748
FAX: 020 7247 4725
EMAIL: publications@lasa.org.uk
WEBSITE: www.lasa.org.uk

The Lasa Computanews Guide to Data Protection

Written by Paul Ticher (July 2004)

Paul Ticher is a self-employed consultant, who has been concerned with Data Protection in voluntary organisations since 1986. He can be contacted by email at paul@paulticher.com.

Cartoons by Phil Evans

Layout by Third Column. Printed by Russell Press.

Funded by London's local councils