filanthropiaconsulting
for charities and not for profit organisations

Data Protection and related issues: introductory guidance

Introduction

The following is a brief summary of the Data Protection Act 1998 ("the DPA") and some related compliance issues. It should not be treated as a definitive statement of the law and specific advice should be obtained for specific circumstances. We would be happy to advise further on any aspect of this note and prepare a (or review an existing) data protection policy.

Please note that any words (other than headings) which are emboldened indicates that they are defined in the glossary of terms set out in the appendix to this paper.

Background to the introduction of the DPA

The DPA came into force on 1 March 2000 and implements the EU Data Protection Directive into UK law. It is wider in scope than its predecessor (the Data Protection Act 1984). Since then there have been several pieces of supplementary legislation relating to data protection.

The DPA sets out the obligations of those who **process data**, the powers of the Information Commissioner to enforce those obligations and the offences that may be committed when they are not complied with.

Overhaul of data protection legislation in 2018

The General Data Protection ("GDPR"), a new EU data protection legal framework, will apply to the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect commencement of the GDPR.

Many of the GDPR's concepts and principles are much the same as those in the DPA. However, there are new elements and significant enhancements. The Information Commissioner's Office ("the ICO") has produced a checklist which sets out 12 steps that organisations should now take to ensure that they will be GDPR compliant by May next year. The checklist, together with other useful GDPR guidance, can be downloaded from the ICO website:

www.ico.org.uk

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Organisations complying properly with the current law will find that most of their approach to data protection will remain valid under GDPR: it can, therefore, be the starting point from which to ensure GDPR compliance.

The DPA in more detail

Notifications to/registration with the ICO

Except in limited circumstances (in relation to, for example, some not for profit organisations), all data controllers must notify the ICO of any **processing** of **personal data** which they carry out. The ICO publishes the details on a public register. The information which must be notified includes:

●the purposes for which data are processed;

●the classes of **data subject**;

●the classes of data;

●the classes of recipient; and

●any countries outside the European Economic Area to which the data may be transferred.

Full guidance notes and copies of the necessary forms for notification can be obtained from the Office of the Information Commissioner at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, or downloaded and completed online at www.ico.org.uk. The notification helpline is 01625 545740.

Individuals' rights

Individuals have a number of rights under the DPA in relation to data held about them. These are:

●a right of access to personal data (usually referred to as 'subject access');

●a right to prevent processing likely to cause them substantial unwarranted damage or distress or significantly to prejudice their rights and freedoms;

●a right to prevent processing for the purposes of direct marketing (see pages 6 and 7 below for more about direct marketing);

●a right in relation to automated decision-taking;

●a right to compensation for an individual who suffers damage arising from a **data controller's** contravention of the DPA; and

●a right to have certain data rectified, blocked, erased or destroyed.

There are exemptions from most of these rights which may apply in limited circumstances. Data controllers will need to check the availability of such exemptions in any given scenario.

The DPA also allows any individual who believes him/herself to be affected directly by any processing of data to ask the ICO for an assessment of whether it is likely or unlikely that the processing has been carried out in accordance with the DPA.

The data protection principles

There are eight **data protection principles** with which data controllers must comply. These are summarised in the appendix to this note but principle 1 (personal data must be processed fairly and lawfully) and principle 7 (protection against unauthorised and unlawful processing of data) are explained in more detail below.

Principle 1: personal data must be processed fairly and lawfully

There are two aspects to this. First, data cannot be obtained fairly unless the data controller has taken steps to ensure (insofar as is practicable) that the data subject is provided with information about:

●the identity of the data controller;

●the purpose or purposes for which it is intended the data should be processed; and

●any further information that is necessary to enable the processing in respect of the data subject to be fair.

Secondly, non-sensitive personal data cannot be processed lawfully unless one of a number of conditions is satisfied, the main ones being:

●the data subject has given his/her consent to the processing (which can include an implied consent in certain circumstances);

●the processing is necessary for the performance of a contract to which the data subject is a party;

●the processing is necessary to ensure compliance with a legal obligation;

●the processing is necessary to protect the data subject's vital interests;

●the processing involves the administration of justice (including a criminal investigation);

●the processing is carried out in order to comply with legislation;

●the processing is necessary for the legitimate interests of the data controller (see below); or

●the processing is in the substantive public interest, for the provision of confidential counselling, advice, support or any other service and is carried out without the data subject's express consent because it is necessary where such consent cannot be given.

What are legitimate interests?

The ICO has to date appeared to take a fairly wide view of what constitutes an organisation's 'legitimate interests' to enable it to process personal data without the consent of the data subject – save in relation to direct marketing and, again, see the separate section on pages 6 and 7 below .

So long as the organisation's interests are legitimate and the data subject is not prejudiced in an unwarranted or unreasonable manner, the processing can be carried out. Having said that, if consent is obtained there is more certainty that the data controller has complied with the above conditions.

Consent and sensitive personal data

There is a sub-category of personal data which is referred to by the DPA as 'sensitive personal data'. These are data which relate to an individual's political opinions, racial or ethnic origins, mental or physical health, sexual life, religious beliefs, trade union affiliation or criminal record (including any allegation of the commission of an offence), although not their financial status. The obligations imposed upon data controllers in relation to sensitive personal data are more onerous than those imposed in relation to personal data.

If the data being processed are sensitive personal data, one of several additional conditions must be satisfied, including that any required consent must be 'explicit'. In other words, the data subject must specifically and expressly agree to each purpose for which the data will be used in order for it to be lawful.

Principle 7: protection against unauthorised or unlawful processing of data and against accidental loss or destruction of, or damage to, the data

The steps envisaged could include using encryption, guidance for employees and volunteers to ensure that they are aware of the data controller's obligations under the DPA; their responsibilities as employees or volunteers of the data controller; and steps to ensure the physical security of the files which hold relevant data, such as password access to computerised records.

If a data controller fails to prevent unauthorised access to the data, it will be in breach of the DPA.

There have been several examples of security breaches (eg the loss of child benefit data by HMRC). The ICO enforcement notices issued required data controllers to encrypt sensitive data and to train staff to comply with the DPA.

The ICO has produced guidance on what practical steps organisations should take in relation to data security. The guidance is available on the ICO's website, www.ico.org.uk.

Data controllers must also ensure that data processors (ie those other than employees or volunteers of the data controller, such as a fulfilment house) that process data on their behalf enter into a written contract under which they agree to take similar measures and to use the data only in accordance with the data controller's instructions.

Subject access rights

Data subjects are entitled, on making a written request with a fee of not more than £10 (fees may vary in relation to credit and health records), to be given within 40 days a description of:

●the personal data held (in an intelligible form);

●the purposes for which those data are being processed; and

●to whom they may be disclosed;

together with a copy of all the information comprising the personal data.

The following exemptions apply:

●the data subject agrees the information need not be disclosed;

●the data subject has not provided sufficient information to enable the data controller to satisfactorily identify the data subject or otherwise comply with the request;

●the data controller has already complied with the same or a similar request within a reasonable period;

●disclosure of the data would also disclose information relating to another individual unless:

–the other individual has consented; or

–it is reasonable to disclose the information without such consent.

In considering whether it would be reasonable, regard must be had to:

●any duty of confidentiality owed to the other individual;

●any steps taken by the data controller to seek consent from the other individual;

●whether the other individual is capable of consenting;

●any express refusal of consent.

There are also special requirements concerning certain health, social and educational records.

If a data subject does not supply sufficient information to enable the request to be complied with or does not pay the fee, it is not enough to sit back and wait; the data controller must explain the problem to the data subject.

Enforcement

The ICO may serve information notices upon data controllers, either upon receiving an assessment request from a data subject or, if reasonably required by the ICO, to determine whether a data controller has complied with its obligations under the DPA.

The ICO may also serve an enforcement notice on any data controller which the ICO is satisfied is in breach of one or more of the eight data protection principles. The notice will set out the steps to be taken by the data controller to remedy its breach and a timetable within which this must be done.

The ICO has powers to obtain a warrant to enter and search premises, to inspect papers and equipment used for processing data, and to seize documents. Failure to comply with a notice is an offence unless it can be shown that all due diligence was exercised to comply.

Offences and civil penalties

The Criminal Justice and Immigration Act 2008 ("CJIA 2008") gives the Secretary of State a power to allow for imprisonment for offences under the DPA. No order allowing imprisonment has yet been made. Currently, a court may also, on conviction, order any document or other material used in connection with the processing of personal data which the court considers to be connected with the commission of the offence to be forfeited, destroyed or erased.

The directors and officers of a company which commits an offence may also be found guilty of the offence in question and be punished accordingly.

In addition to the criminal offences contained within the DPA, the CJIA 2008 has given the ICO a power to impose civil monetary penalties of up to £500,000 on data controllers where there has been a serious and deliberate contravention of the data protection principles or the data controller ought to have appreciated that there was a risk of such a breach and failed to take reasonable steps to prevent it. This new power came into force on 6 April 2010. The ICO has issued statutory guidance on how it uses these powers, which is available on its website: www.ico.org.uk.

There seems to have been a recent increase in the use by the ICO of its fining powers. This is evidenced by the fact that in December 2016 the ICO fined two household named charities for breaches of the DPA in relation to their collecting, use and storage of donors' data - essentially they were "wealth screening". This represents a much harsher stance by the ICO, given that it has previously not been inclined to fine charities.

Miscellaneous

The DPA imposes a number of other obligations of which data controllers should be aware. These include the following:

●unlawfully obtaining personal data (without the consent of the data controller) is an offence;

●selling or offering to sell unlawfully obtained personal data is also an offence;

●restrictions on the ability of an employer or prospective employer to oblige an employee or prospective employee to exercise his subject access rights to obtain a copy of his criminal record;

●restrictions on the enforceability of a term of contract which obliges an individual to exercise his subject access rights to obtain a copy of his medical records.

Direct marketing

"Direct marketing" is defined in the DPA as:

> "*the communication (by whatever means)... of any advertising material...which is directed to particular individuals.*"

The ICO has confirmed that all fundraising activity, as well as promotion of "aims and ideals" and campaigning activity of charities is covered by the definition of direct marketing. The marketing must be directed to particular individuals. In practice, therefore, all relevant electronic messages (for example, telephone calls (live and automated), faxes, texts and emails), as well as most addressed mail, which are directed to someone will constitute direct marketing.

When will individuals' consent be required in relation to direct marketing?

Pursuant to the Privacy and Electronic Communication (EC Directive) Regulations 2003 ("PECR"), consent will always be required in relation to electronic messages. The PECR applies to automated calls, faxes, texts and emails.

So far as live calls and post are concerned, the ICO considers that gaining consent to be good practice and the most advisable approach, although in some circumstances it may be possible to rely on the "legitimate interest condition" under the first data protection principle (personal data must be processed fairly and lawfully).

However, organisations would first need to check that an individual is not registered with the Telephone Preference Service and/or the Mailing Preference Service. Note also that the Fundraising Regulator launched the Fundraising Preference Service ("FPS") on 6 July 2017. The FPS allows individuals, especially the vulnerable, to receive only the fundraising materials they want and need. See the link below for further details about the FPS:

https://www.fundraisingregulator.org.uk/the-fundraising-preference-service/for-charities/

It should also be noted that the DPA allows data subjects to require (by written notice) data controllers to stop using their data for the purposes of direct marketing.

What constitutes consent?

The ICO's interpretation of consent

There is no definition of consent in the DPA. This means that organisations have often taken "consent" as being sufficient if it was "implied" – for example if someone had not "opted-out". Again, there are no legal definitions of "opt-in" or "opt-out": they are simply marketing terms used to address the key issue of consent.

However, the EU Data Protection European Directive (which the DPA implemented) provides greater clarity as to what constitutes consent. It provides that consent should be:

> "*freely given, specific and informed and involve a positive indication signifying the data subject's agreement.*"

The ICO has referred to the above European Directive wording in both its direct marketing guidance published in May 2016 and its recent penalty notices. Consequently, it seems to be using this as a benchmark for interpreting lawful consent.

The ICO has confirmed that, as a matter of good practice, explicit consent should be obtained: in other words individuals should signify that they wish to receive marketing communication by opting-in. It has also confirmed that opting out (where individuals signify that they object to receiving marketing messages) may still constitute lawful consent if it involves "*some form of communication or positive action by which the individual clearly and knowingly indicates their agreement.*"

Recent guidance published by the Fundraising Regulator

In February 2017 the Fundraising Regulator also published guidance for charities on direct marketing entitled "*Personal information and fundraising: consent, purpose and transparency.*" The guidance has been issued partly as a result of (a) the forthcoming introduction of the GDPR and (b) the above mentioned recent fines imposed by the ICO on two charities in relation to what was held to be serious breaches of the DPA. The Fundraising Regulator has confirmed that it believes that there is now a commitment across the charity sector to make consent the primary basis for all fundraising activity.

The guidance sets out various examples as to when consent is legally required and what, as a matter of good practice, it considers the form of consent should be in various circumstances: it can be downloaded from the link below. It should be noted that the Fundraising Regulator's guidance is intended to supplement the ICO guidance on direct marketing and within the former's guidance there are references and links to the latter's guidance.

https://www.fundraisingregulator.org.uk/wp-content/uploads/2017/02/GuidanceFinal.pdf

Shift in what is now regarded as lawful consent?

It seems from recent guidance issued by both the ICO and the Fundraising Regulator that what charities and other organisations involved in direct marketing have regarded as lawful consent, may not be considered to be the case now. Consequently, a review of existing procedures and consents should be undertaken sooner rather than later.

The UK Code of Non-Broadcast Advertising, Sales Promotion and Direct Marketing ("CAP Code")

Organisations involved in marketing (including direct marketing) may also wish to familiarise themselves with the CAP Code which is created and enforced by the self-regulatory body called the Committee of Advertising Practice. It is intended that the CAP Code supplements the law and fills in gaps where the law does not reach, with a view to ensuring that that marketing communications are legal, decent, honest and truthful and consumer confidence is maintained. The CAP Code can be downloaded from the link below:

https://www.asa.org.uk/asset/47EB51E7-028D-4509-AB3C0F4822C9A3C4/

The law is stated as at September 2017

Sarah Chiappini
Director and Solicitor (non-practising)
Filanthropia Consulting
sarah@filanthropia.co.uk

This note provides a general summary only and it does not constitute legal advice. It is recommended that specific advice is sought in relation to the particular facts of a given situation.

If you have any queries regarding any aspect of this note or you would like us to assist you with a governance review and/or assist with the preparation of any relevant documentation please do not hesitate to contact Sarah Chiappini.

APPENDIX

Glossary of terms

Data: information which:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;
(b) is recorded with the intention that it should be processed by means of such equipment;
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
(d) does not fall within paragraphs (a), (b) or (c) but forms part of an accessible record as defined by section 68 of the DPA; or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Data Controller: a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed.

Data Protection Principles: the following eight data protection principles as set out in Schedule 1 of the DPA:

1. Personal Data shall be processed fairly and lawfully and, in particular, shall not be processed unless the specified conditions of processing are met.

2. Personal Data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal Data shall be accurate and, where necessary, kept up to date.

5. Personal Data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal Data shall be processed in accordance with the rights of Data Subjects under the DPA.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, Personal Data.

8. Personal Data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data.

Data Subject: an individual who is the subject of Personal Data.

Personal Data: Data that relates to a living individual who can be identified:-

(a) from that Data; or
(b) from that Data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller**,**
and includes any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.

Processing/processed/process: obtaining, recording or holding Data or carrying out any operation or set of operations on the Data, including:-

(a) organisation, adaptation or alteration of the Data;
(b) retrieval, consultation or use of the Data;
(c) disclosure of the Data by transmission, dissemination or otherwise making available; or
(d) alignment, combination, blocking, erasure or destruction of the Data.