MEDIA BRIEFING

Information Commissioner

Contents

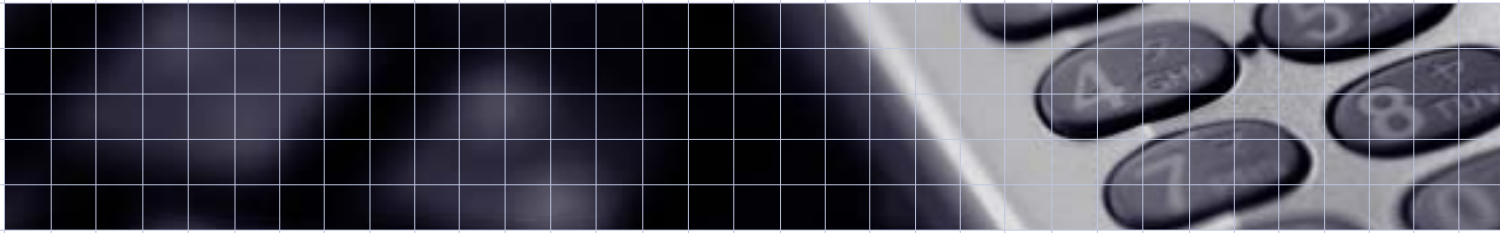
Overview

The Data Protection Act 1998 (DPA) came into force on 1 March 2000, repealing the Data Protection Act 1984. It sets rules for processing personal information and applies to some paper records as well as those held on computers.

The DPA derives from EU Directive 95/46/EC which requires "Member States to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data."

The Freedom of Information Act 2000 (FOI) was passed on 30 November 2000. It gives a general right of access to all types of 'recorded' information held by public authorities, sets out exemptions from that right and places a number of obligations on public authorities. Individuals can start exercising their full rights under the Act on 1 January 2005, although individuals already have the right to complain to an authority or the Information Commissioner regarding the authority's publication scheme.

This paper outlines the role of the Information Commissioner's Office under these two Acts of Parliament. There is also a glossary at the back of the briefing to explain the most frequently used terms within both Acts.



The Role of the Information Commissioner

The Information Commissioner has specific responsibilities for the promotion and enforcement of both the Data Protection Act 1998 and the Freedom of Information Act 2000. The Commissioner's Office is in Wilmslow in Cheshire, where approximately 200 staff deal with data protection for the UK and freedom of information matters for England, Northern Ireland and Wales.

In the UK, the Commissioner's duties include the promotion of good information handling and in certain cases the development of codes of practice for data controllers, (anyone who decides how and why personal data, i.e. information about identifiable, living individuals is processed). The Commissioner is independent of Government, reports directly to Parliament and has both a national and international role.

The Commissioner assesses alleged breaches of both the DPA and FOI Act.

He is able:

- in certain circumstances to serve information notices. This requires a data controller to provide the Commissioner with specified information within a certain time period, which will help him to assess compliance;
- where there has been a breach, to serve an enforcement notice (which requires data controllers to take specified steps or to stop taking steps in order to comply with the law).

Appeals from these notices can be heard by the Information Tribunal (a tribunal which is specifically for matters concerning enforcement notices or decision notices issued by the Information Commissioner).

Under the **Freedom of Information Act 2000**, the Commissioner will have powers to:

- approve/revoke publication schemes;
- promote the following of good practice including the observance of the provisions of the codes of practice;
- promote public authorities' compliance with the Act;
- issue a practice recommendation where a public authority is not following good practice;
- deal with complaints that requests for information under the Act have not been fulfilled;
- require public authorities to disclose information in appropriate cases.

Richard Thomas

Richard Thomas took up the role as Information Commissioner in December 2002. A qualified solicitor, Richard's career includes working as Director of Policy at Clifford Chance, Director of Consumer Affairs at the Office of Fair Trading and Head of Public Affairs at the National Consumer Council (NCC).

Richard was previously a non-executive Director of the Financial Ombudsman Service (FOS) and a member of the Independent Television Commission Advertising Advisory Committee.

Richard's key challenges are:

- challenging traditional cultures of unnecessary secrecy across the public sector;
- ensuring a culture of respect for personal information;
- balancing open government and privacy against other public interests;
- helping organisations to achieve compliance with the DPA and the FOI Act;
- fostering an environment where freedom of information and data protection are a natural way of life.

The Data Protection Act 1998

In practice:

- it gives individuals certain rights with regard to information which is held about them. Individuals have the right to find out what information is held about them and what use is being made of that information. This is known as the right of "subject access". If an individual finds that this information is wrong he/she also has the right to have that information corrected or deleted. There are certain exemptions to this right;
- it also says those who record and use personal information must be open about how the information is used.

Who and what is covered by the Act?

The DPA places obligations on those who process data (data controllers) while giving rights to those who are the subject of that data (data subjects). Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual.

The eight principles of good information handling practice

Anyone processing personal data must comply with the eight enforceable principles of good practice.

They say that data must be:

(1) fairly and lawfully processed;
(2) processed for limited purposes;
(3) adequate, relevant and not excessive;
(4) accurate and up to date;
(5) not kept longer than necessary;
(6) processed in accordance with the individual's rights;
(7) secure;
(8) not transferred to countries outside the European Economic Area unless the country has adequate protection for the individual.

The six conditions of processing personal data

Personal data will not be considered to be processed fairly unless at least one of the following conditions are met:

(1) the individual has given his or her consent to the processing;
(2) processing is necessary for the performance of a contract with the individual;
(3) processing is required under a legal obligation (other than one imposed by contract);
(4) processing is necessary to protect the vital interests of the individual;

(5) processing is necessary to carry out public functions, e.g. administration of justice;

(6) processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

Processing sensitive data

The Act makes additional specific provision for sensitive personal data. Sensitive data includes: racial or ethnic origin; political opinions; religious or other beliefs; trade union membership; physical or mental health or condition; sex life; criminal proceedings or convictions.

Sensitive personal information will not be considered to be processed fairly unless at least one of the conditions for processing sensitive personal information is met. These include amongst others:

- having the explicit consent of the individual;
- being required by law to process the data for employment purposes;
- needing to process the information in order to protect the vital interests of the individual or another person;
- dealing with the administration of justice or legal proceedings.

The Data Protection Act 1998 is written in a way that seeks to strike a balance between potentially competing interests. Its provisions do not seek to guarantee personal privacy at all cost but to strike a balance between the rights of individuals and other legitimate interests.

Rights under the Act

The right to subject access

The Act allows individuals to find out what information is held about them on computer and within some paper records. This is known as the right of subject access.

The right to prevent processing

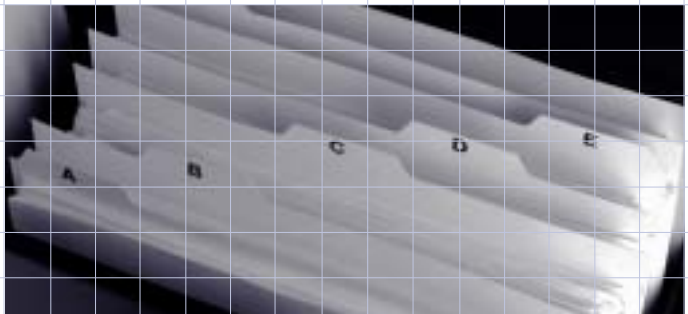
Anyone can ask a data controller to stop or request that they do not begin processing data relating to him or her where it is causing, or is likely to cause, substantial unwarranted damage or substantial unwarranted distress to them or anyone else. However, this right is not available in all cases.

The right to prevent processing for direct marketing

Anyone can ask a data controller to stop or not to begin processing data relating to him or her for direct marketing purposes. This is an absolute right.

Rights in relation to automated decision-taking

An individual can ask a data controller to ensure that no



decision which significantly affects him or her is based solely on processing his or her personal data by automatic means. There are, however, some exemptions to this.

The right to compensation

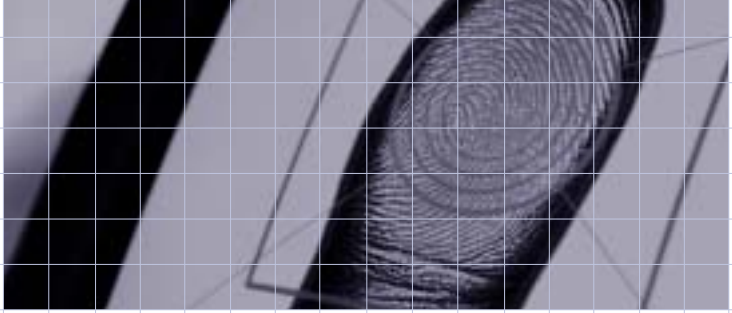
An individual can claim compensation from a data controller for damage or damage and distress caused by any breach of the Act. Compensation for distress alone can only be claimed in limited circumstances.

The right to rectification, blocking, erasure and destruction

The Act allows individuals to apply to the Court to order a data controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.

The right to ask the Commissioner to assess whether the Act has been contravened

Anyone who believes that their personal data has not been processed in accordance with the DPA, and is unable to sort the problem out themselves, can ask the Information Commissioner to make an "assessment" as to whether this is the case. If the Commissioner's assessment is that there has been a breach and the matter cannot be settled informally, then he may decide to serve an enforcement notice on the data controller in question.



Criminal offences

There are a number of criminal offences created by the Act and they include:

- *Notification offences*

  These are committed where processing is being undertaken by a data controller who has not notified the Commissioner either of the processing being undertaken or of any changes that have been made to that processing. Failure to notify is a strict liability offence.

- *Procuring and selling offences*

  It is an offence to knowingly or recklessly procure the disclosure of personal information, without the consent of the data controller. This covers unauthorised access to and disclosure of personal data. There are some exceptions to this, for example, if it was necessary to prevent or detect crime or was required or authorised by law. If a person has obtained personal data illegally it is an offence to offer to sell or to sell personal data.

Other important legislation relevant to the Data Protection Act

EU Data Protection Telecommunications Directive 97/66/EC

The Directive covers telecommunications and reinforces the DPA. This Directive imposes special rules for the processing of personal data in public telecommunications systems, faxes, telephones, and automated calling systems for unsolicited marketing.

Marketing faxes must not be sent to individual subscribers without their prior consent. Also individual subscribers have a statutory right to opt-out of unsolicited telephone marketing either by telling the caller or by registering with the Telephone Preference Service (TPS) on a central stop list. Corporate subscribers cannot opt-out of telephone sales but have the right to opt-out of unsolicited marketing faxes. The prior consent of both corporate and individual subscribers is needed for automated calling systems.

For more information on the Telephone Preference Service contact:

Telephone Preference Service
5th Floor
Haymarket House
1 Oxendon Street
LONDON, SW1Y 4EE

t: 020 7291 3320
e: tps@dma.org.uk
w: www.tpsonline.org.uk

EU Privacy and Electronic Communications Directive 2002/58/EC

The DTI has initiated a consultation exercise inviting comments on how unsolicited commercial email (UCE) colloquially known as "spam" should be regulated. The EU Privacy and Electronic Communications Directive, designed to ensure that rules governing unsolicited marketing communications apply to new technologies, must be enacted into UK law by October 2003. It updates the current directive 97/66/EC known in UK law as the Telecommunications (Data Protection and Privacy) Regulations 1999.

UCE are a major headache for businesses and consumers and the new legislation will mean that they can only be sent when the consumer has "opted-in" to receiving them unless the consumer's email address was obtained in the context of a commercial relationship. Even in the latter case consumers must be offered a chance to opt-out. Similar rules will apply to unsolicited marketing SMS messages. The DTI recognises that legislation is not the complete answer. Consumers and businesses should also look at using technical blocks or filters.

The Information Commissioner will be responsible for enforcing the new legislation though it is not clear exactly what powers he will have to do so at the time of going to print. The DTI consultation also invites views on what enforcement

powers would be appropriate. The Commissioner is calling for stronger powers to allow him to take swifter action where necessary.

The Human Rights Act 1998

The Human Rights Act 1998 introduced for the first time in this country a bill of human rights. The Act details a list of basic human rights that are to be respected and enforced in the UK. The Act ensures that the courts and other public authorities are accountable for their decisions. If an individual feels that their human rights have been ignored in a decision made by an authority it is their right to bring this case to court.

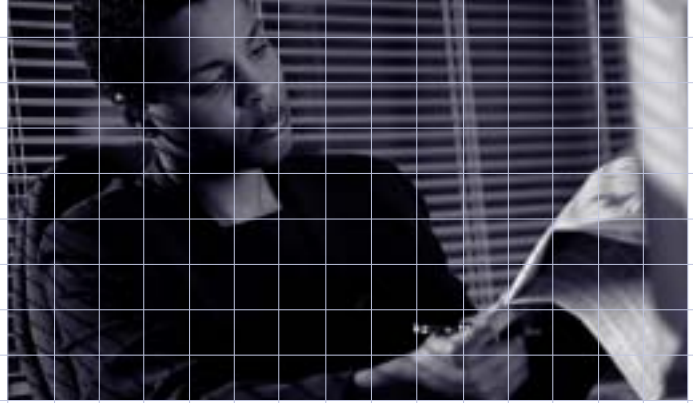
Whenever exercising his discretion in accordance with the DPA, the Commissioner will always have regard to competing interests under the Human Rights Act.

For more information regarding human rights, please visit: www.humanrights.gov.uk

Anti-Terrorism and Security Act 2001

Following the events of 11 September 2001, the Government revised the Anti-Terrorism Act which has implications on the Human Rights Act, DPA and the FOI Act.

The Anti-Terrorism Crime and Security Act impacts on the DPA in two particular areas.



Part 3 provides a lawful basis for the disclosure of personal information held by a range of public authorities where the disclosure is for the purposes of any criminal investigation or proceedings. Any public authority intending to disclose personal data must still satisfy data protection requirements.

Part 11 deals with the 'retention' of communications data by communications providers. At the time of going to print, arrangements are included for a voluntary code under which providers can retain personal data, where this is necessary for safeguarding national security or related matters. Before issuing any code the Secretary of State has to undertake a public consultation. Before publishing his draft for public consultation the Secretary of State must first consult with both the Information Commissioner and communications providers.

Freedom of Information Act 2000

In summary:

- it allows individuals access to information held by a public authority;
- public authorities and anyone who provides services to them must adopt and maintain a publication scheme setting out how they intend to publish the different classes of information they hold, and whether there is a charge for the information.

Who is covered by the Act?

The Act applies to public authorities and those providing services for them. A detailed list of public authorities is contained in Schedule 1 of the Act.

This includes amongst others:

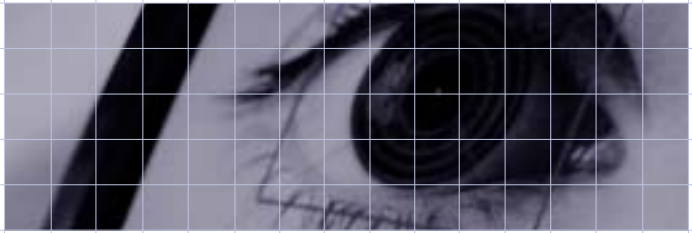
- government departments;
- local authorities;

- NHS bodies (such as hospitals, as well as doctors, dentists, pharmacists and opticians);
- schools, colleges and universities;
- the police;
- organisations such as the National Gallery and Parole Board;
- the House of Commons and the House of Lords;
- the Northern Ireland Assembly, and
- the National Assembly for Wales.

There is provision in the Act for other authorities to be named later and for private sector organisations to be named as public authorities for relevant parts of their work.

The Act in brief

Any person who makes a written request (satisfying certain conditions) to a public authority for information, must be told whether the public authority holds that information and if so, that information must normally be supplied. However, the public authority will not be obliged to confirm or deny the existence of information or provide all or part of the information requested if an exemption applies or the request is vexatious, similar to a recent previous request or the cost of compliance would exceed the "appropriate limit". Usually, in the majority of cases where an exemption applies, the public authority will then have to consider whether the information must be released in the public interest.



New rights for individuals

As far as public authorities are concerned, freedom of information will extend the rights of individuals to obtain access to most types of information held, whether personal or non-personal.

This may include information about third parties, although a public authority will have to take account of the DPA before releasing any personal information.

Where possible, the authority must provide the information in the manner requested by the applicant. This may be in the form of a copy or summary, or the applicant may ask to inspect the record.

It is important to note that applicants will not be able to exercise most of their rights of access under the FOI Act until 1 January 2005. However, the Act will be fully retrospective, as regards the information covered.

New responsibilities for public authorities

a) Publication schemes

The Act places a duty on public authorities to adopt and maintain a publication scheme which must be approved by the Information Commissioner. The scheme must set out the type of information the authority has, how it is made available and whether a charge is made for it.

Once approved, it will be up to the public authority to review it periodically and to ensure that it publishes information in accordance with its scheme.

The Commissioner may also approve model publication schemes. These schemes would be suitable for groups of similar bodies which hold and publish similar information. For example, parish councils, hospital trusts and primary schools.

The Information Commissioner is working with representatives of public authorities to identify what should be included in model publication schemes.

b) Responding to requests:

- in general, public authorities will have to respond to requests within 20 working days. There are exceptions where the public authority is considering whether the disclosure of exempt information would be in the public interest;
- public authorities may charge a fee for complying with a

request for information;

- in cases where a qualified exemption applies, the public authority must apply the public interest test and make a decision whether to release the information 'within a reasonable time';
- authorities will have a duty to provide advice and assistance to applicants;
- where possible, authorities must provide the information in the form requested by the applicant.
- where an authority has grounds not to release the information requested, it must give reasons for its decision and must inform the applicant of its complaints procedure and his/her right to complain to the Information Commissioner.

The public interest

Public authorities are not required to disclose any information which is covered by one or more of the exemptions (these are dealt with in the next section). However, in the majority of cases where an exemption applies, the public authority will then have to consider whether the information must nevertheless be released in the public interest. This public interest test involves considering the circumstances of each particular case and the exemption that covers the information. The information may only be withheld if the public interest in withholding it is greater than the public interest in releasing it.

The exemptions

There are 23 exemptions in the FOI Act.

The exemptions can be divided into:

a) those which apply to a whole category (or class) of information, for example:

- information relating to investigations and proceedings conducted by public authorities;
- court records; and
- trade secrets.

and

b) those which are subject to a prejudice test, for example, where disclosure would, or would be likely to prejudice:

- the interests of the United Kingdom abroad; or
- the prevention or detection of crime.

Information only becomes exempt if disclosing it would, or would be likely to prejudice the activity or interest described in the exemption.

The public interest test applies to most of the exemptions. Those to which the test does not apply are called the 'absolute exemptions'.

Exemptions for personal information

Where a request to a public authority is for personal information relating to the applicant, the information will become exempt under the FOI Act. This request will be treated

as a 'subject access request' made under the Data Protection Act 1998. Where a request is for personal information relating to a third party, release of the information will have to be determined by reference to the DPA.

Enforcement of the Act

A person who has made a request for information may apply to the Information Commissioner for a decision as to whether the request has been dealt with according to the Act. In response, the Information Commissioner may serve a decision notice on the public authority and applicant setting out any steps which are required in order to comply.

The Commissioner will also have the power to serve information notices and enforcement notices on public authorities. The Information Commissioner may issue a decision or enforcement notice requiring disclosure of information where he believes that the public authority has incorrectly claimed that an exemption applies. If such a notice is served upon a government department, the National Assembly for Wales or any authority designated for these purposes by an order of the Lord Chancellor, it may be subject to an 'Executive Override'. In such a case the public authority will have 20 days from receipt of the notice to obtain a signed certificate from a Cabinet Minister overriding the Information Commissioner's notice. All notices may be appealed to the independent Information Tribunal.

Is there potential conflict between the DPA and FOI Act with regard to personal information?

The issues are complex, however there must be a distinction between information relating to an individual in a personal capacity (covered by the DPA) and information relating to an individual in an official capacity. So where an individual is appointed to a senior post in public office and is taking decisions which are of public importance, in the interests of transparency and accountability, personal information which relates directly to the discharge of public functions may need to be disclosed publicly.

Glossary

Data controller (DPA)

A person who determines the purposes for which, and the manner in which, personal data are, or are to be, processed. This may be an individual or an organisation, and the processing may be carried out jointly or in common with other persons.

Data processor (DPA)

A person, who processes data on behalf of a data controller. Anyone responsible for the disposal of confidential waste is also included under this definition.

Data subject (DPA)

This is the living individual who is the subject of the personal information (data).

Enforcement notice (DPA)

The Information Commissioner has the power to serve an enforcement notice if he is satisfied that a public authority has failed to respond properly to a request for information under the Act. The notice must set out the steps that the authority must take in order to comply with the relevant requirements of the Act. An appeal against a notice may be made to the Information Tribunal which may confirm, amend or overturn the notice. However, in the absence of an appeal, if the authority fails to comply with a notice, then the Commissioner may apply to a court which will deal with the matter as a contempt of court.

Information Padlock/Signpost (DPA)

The symbol (designed by the Information Commissioner and the National Consumer Council) acts as a signpost, so that data subjects can tell at a glance that personal data about them is being collected and processed.

Information notice (DPA + FOI)

An information notice is a written notice from the Information Commissioner to a data controller seeking information the Commissioner needs to carry out his functions. Failure to comply with an information notice is an offence.

Information Tribunal (DPA + FOI)

The Information Tribunal hears appeals by data controllers against notices issued by the Information Commissioner under the DPA and appeals made by a public authority against enforcement notices and information notices under the FOI Act from 1 January 2005. It will also hear appeals from decision notices made by a complainant or a public authority.

Mail Preference Service (DPA)

The Mail Preference Service (MPS) is a non-profit making body set up by the direct marketing industry to assist those people who do not wish to receive so called 'junk' mail.

When an individual provides their surname and address to the MPS they will place the information on their consumer file which is then made available to those members of the direct marketing industry who subscribe to the MPS scheme. They undertake to ensure that the mailing lists they use and supply are 'cleaned' of any names and addresses which appear on the MPS file, the result being that an individual should not, in future, receive their mailings.

Notification (DPA)

Notification is the process by which a data controller's processing details are added to a register. Under the DPA every data controller who is processing personal data needs to notify unless they are exempt. Failure to notify is a criminal offence.

Even if a data controller is exempt from notification, they must still comply with the principles.

The Commissioner maintains a public register of data controllers available at www.dpr.gov.uk. A register entry only shows what a data controller has told the Commissioner about the type of data being processed. It doesn't name the people they hold information about.

Personal data (DPA)

Data which relates to a living individual who can be identified

- from those data, or
- from those data and other information which is in the possession of, or likely to come into the possession of the data controller.

It 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 (DPA)

Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data.

Public authority (FOI)

Any body, any person, or the holder of any office listed in the FOI Act, or designated by order and publicly owned companies. Examples of some of the public authorities covered by the scheme are:- government departments, local authorities, NHS bodies (hospitals, doctors, dentists, pharmacists and opticians), schools, colleges and universities, the police, the House of Commons and the House of Lords, the Northern Ireland Assembly, the National Assembly for Wales.

Publication schemes (FOI)

The FOI Act places a duty on public authorities to adopt and maintain a publication scheme that must be approved by the Information Commissioner. The scheme lists and defines the classes of information that will be published, indicates the manner in which information is or is intended to be published and states whether charges are applied for the information.

Subject access request (DPA)

Under the DPA, individuals can see the information about themselves that is held on computer and in some paper records. If an individual wants more information on the personal data held about them, they can write to the person or organisation that they believe is processing the data.

A subject access request must be made in writing and must be accompanied by the appropriate fee. In the majority of cases, the maximum fee will be £10, but this will vary, particularly if the information requested is for health or educational records. If a subject access request is made to a credit reference agency, then the fee is £2, and the information must be provided within 7 working days.

A request must include sufficient information to enable the person or organisation to whom the subject is writing, to satisfy itself as to the identity and to locate the information.

A reply must be received within 40 days as long as the necessary fee has been paid. A data controller should act promptly in requesting the fee or any further information necessary to fulfil the request. If a data controller is not processing personal information of which this individual is the data subject the data controller must reply to that effect.

Telephone Preference Service & Fax Preference Service (DPA)

Similar schemes to the MPS exist for the Telephone Preference Service (TPS) and Fax Preference Service (FPS) which were set up on behalf of the Director General of Telecommunications. Organisations that engage in unsolicited direct marketing by telephone and fax must not contact individuals who have registered with these opt-out schemes. Registration with the TPS and FPS can therefore help people to reduce the number of unwanted telephone sales calls or marketing faxes they receive.

Publication request

t: 0870 600 8100

Media

t: 020 7535 9770
f: 020 7535 9998
e: icopressoffice@citigatec.co.uk
w: informationcommissioner.gov.uk

Our contact details

If you would like to arrange an interview or be placed on our mailing list please contact our Press Office or visit 'Media Services' at the above web address.

Information Commissioner,
Wycliffe House, Water Lane,
Wilmslow, Cheshire, SK9 5AF

IC/MB/0503/5k

Information Commissioner