The requirements are subject to various safeguards, such as protection against repeated requests and how to respond to a request which may involve the disclosure of data relating to other data subjects, or which might constitute a 'tipping off' offence under the Proceeds of Crime Act 2002. Investigators should seek specialist legal advice before responding to any data access requests.

EXEMPTIONS

There are exemptions (within the Act and in Statutory Instruments) to certain of the Act's provisions in certain circumstances. It is important to note that these exemptions have different effects, in that some exemptions work to restrict nearly all of the Act's provisions, whilst others are limited in their scope and restrict only certain parts of the Act.

We cannot set out all the relevant provisions here, but the most significant for investigators is the 'Crime & Taxation' exemption (section 29 of the Act), which provides exemption from:

- the first data protection principle (save the need to establish a legitimate purpose for the processing); and
- data subject access requests

for processing for the purpose of the prevention or detection of crime, or the apprehension or prosecution of offenders. Investigators should study the detail of the exemptions, consult guidance or seek legal advice.

It should be noted that the exemption relating to legal proceedings (including prospective legal proceedings), the obtaining of legal advice or establishing, exercising or defending legal rights (section 35 of the Act) applies only to the disclosure of data, and not to the obligation on controllers to comply with the other provisions of the Act set out above.

INFORMATION COMMISSIONER'S POWERS

Although not yet in force, the Information Commissioner has been granted new powers to impose monetary penalties in cases of serious, and deliberate or reckless contravention of the data protection principles likely to cause substantial damage or distress. The Information Commissioner also has power to issue enforcement notices to bring controllers into compliance.

As data controllers, investigators must therefore be in full compliance with their obligations under the Act or risk regulatory intervention from the ICO.

INFORMATION COMMISSIONER'S OFFICE

The Information Commissioner's Office has said that it 'welcomes this sensible practical advice which should help investigators understand their data protection responsibilities'.

FURTHER INFORMATION

Other leaflets in this series include *Issues to consider when determining whether investigators are data controllers or data processors*; *Issues to consider when obtaining and sharing data*; *Summary of published guidance*; and *Keeping personal data secure*. All are available from the Fraud Advisory Panel website.

Other sources of information:

- **European Commission**
  http://ec.europa.eu/justice_home/fsj/privacy
- **Fraud Advisory Panel**
  www.fraudadvisorypanel.org
- **Information Commissioner's Office**
  www.ico.gov.uk
- **Office of Public Sector Information**
  www.opsi.gov.uk

Fraud Advisory Panel
Chartered Accountants' Hall, PO Box 433,
Moorgate Place, London, EC2P 2BJ
Tel: 020 7920 8721
Fax: 020 7920 8545
Email: info@fraudadvisorypanel.org
Or visit: www.fraudadvisorypanel.org
Registered Charity No. 1108863

OTHPLN8293 4/09

Fraud Advisory Panel

DATA PROTECTION AND THE INVESTIGATOR

Complying with Data Protection Act 1998 Obligations

May 2009

INTRODUCTION

The Data Protection Act 1998 ('the Act') applies to all individuals and businesses 'processing' data in the UK: 'processing' means any activity carried out with data relating to living individuals, including storing, consulting, retrieving and disclosing it.

The Act requires those processing data to have legitimate grounds for so doing, for example:

- it is necessary for compliance with a legal obligation (other than contractual); or
- it is necessary on the grounds of legitimate interests and does not cause unwarranted prejudice to the rights and freedoms or legitimate interests of the subjects of the data.

If 'sensitive data' is to be processed (which includes data about physical or mental health, sexual life and the commission or alleged commission of any offence), additional purposes must be established before processing can take place. They include, but are not limited to:

- the processing is necessary for the purpose of, or in connection with, current or prospective legal proceedings;
- the processing is necessary for the purpose of obtaining legal advice; or
- the processing is necessary for the purpose of establishing, exercising or defending legal rights.

Assuming that the investigator and his/her client have legitimate grounds for the processing to take place, the Act imposes obligations on those concerned in the processing.

REGISTRATION

The primary obligation imposed on data controllers is to register with the Information Commissioner's Office (ICO). Data controllers are those who determine the 'manner' in which and 'purpose' of the processing. In the majority of cases this definition will include both the investigator and his/her client; see the earlier leaflet in this series *Data Controller or Data Processor? Issues to consider when determining whether investigators are data controllers or data processors* for further detail.

The ICO maintains a register of data controllers which is open to the public to consult through its website: www.ico.gov.uk. Registration may be completed online, by post or by telephone and registration must be renewed annually. The current annual cost of registration is £35. Failure to register is a criminal offence punishable with a fine.

THE DATA PROTECTION PRINCIPLES

Once registered, data controllers must comply with the eight 'Data Protection Principles' set out at Schedule 1 to the Act:

1. Personal data shall be processed fairly and lawfully: this is one of the most complex of the principles, covering issues such as the right of data subjects to be told what data any controller processes about them and why. The 'lawfulness' requirement relates to other legal issues, such as theft of data or trespass. Investigators need to be clear about the circumstances in which data is obtained and the applicability of exemptions to the general rule that data subjects should be informed when their data is processed (see 'Exemptions' below).

2. Personal data shall be obtained for only one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with those purposes: data obtained for one purpose cannot then be processed for another incompatible purpose.

3. Personal data shall be adequate, relevant and not excessive: investigators need to limit the data they process to that which is necessary.

4. Personal data shall be accurate and where necessary, kept up to date: investigators need to review the data they hold and keep it updated.

5. Personal data shall not be kept for longer than necessary: there are no absolute time limits, but investigators will need to be able to justify the period for which they retain data.

6. Personal data shall be processed in accordance with the rights of data subjects: see below.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing, accidental loss or destruction, and damage: see the earlier leaflet in this series *Data Security: Keeping personal data secure* for practical guidance on this issue.

8. Personal data shall not be transferred to countries outside the European Economic Area: this is a complex provision. Investigators should seek specialist advice if they are transferring data to countries other than those in the European Economic Area.

THE RIGHTS OF DATA SUBJECTS

As the sixth data protection principle requires, controllers shall process data in accordance with the rights of data subjects (the people the data is about). Investigators therefore need to ensure that what they do does not infringe those rights, which include:

- The right of data subjects to access the data any controller processes about them.
- Data subjects have a right to prevent processing that is likely to cause unwarranted damage or distress: the data subject may serve a written notice requiring the processing to stop, and the controller must respond. If agreement cannot be reached the data subject may apply to a court for an order to stop the processing.
- Rectification, blocking, erasure and destruction: a data subject may apply to a court for an order that data which is inaccurate is rectified, blocked, erased or destroyed.
- Direct marketing and automated decision-taking: although unlikely to be applicable to the work of investigators, data subjects can serve notices requiring the cessation of such processing, with recourse to the courts if necessary.

SUBJECT ACCESS REQUESTS

As mentioned above, a key right of data subjects is the right to be told, in response to a written request, if a data controller:

- processes data relating to them; and
- if so, to be told what that data is, the purpose of the processing and to whom the data is or may be disclosed.

The data subject is also entitled to a copy of any such data in an intelligible form.

If data controllers receive such a written request they must respond 'promptly', but in any event within 40 days of receiving the request and any fee which may be required by the data controller (the current maximum chargeable for most data controllers is £10).