provided guidance, which although published prior to the enactment of POCA is still valid: www.hm-treasury.gov.uk/d/money_laundering.pdf

It states that where compliance with the data subject's rights under the Act would disclose a SAR and this would 'be likely to prejudice any investigation' this would constitute a 'tipping off' offence and in these circumstances the section 29 exemption will apply. However, where disclosure of a SAR to the data subject would not be likely to prejudice an investigation, no 'tipping off' offence would have been committed. It follows that in these circumstances the section 29 exemption would not be available to data controllers. For example, where the existence and contents of a SAR have been revealed in the course of criminal proceedings, it is unlikely that any prejudice would be caused by the subsequent disclosure of the SAR to the individual concerned. Therefore, the data subject rights and the section 29 exemption must be considered on a case by case basis. Investigators should nonetheless take particular care with regard to the identity of the author of a SAR because of the potential risk of reprisal.

HM Treasury guidance emphasises that even when relying upon an exemption, investigators should provide as much information as they can in response to a 'Data Subject Access Request' made under section 7 of the Act. However, where an investigator withholds a piece of information in reliance on the section 29 exemption, he/she is not obliged to tell the individual that any information has been withheld.

It should not be assumed that the section 29 exemption applies automatically to SARs. However, where an organisation is in doubt as to whether disclosure would be likely to prejudice an investigation or potential investigation, it should approach SOCA for guidance. An investigator should also bear in mind the legal guidance issued by the Information Commissioner on the practical application of section 29. If challenged, either in front of the Information Commissioner or in court, then a data controller must be prepared to defend the decision made. To comply with the legal guidance, the decision to rely on section 29 should therefore be taken at a senior level within an organisation and the reasons for that decision should be documented.

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; Keeping personal data secure;* and *Complying with Data Protection Act 1998 obligations.* 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
- **HM Treasury**
  www.hm-treasury.gov.uk
- **Information Commissioner's Office**
  www.ico.gov.uk
- **Office of Public Sector Information**
  www.opsi.gov.uk
- **Serious Organised Crime Agency**
  www.soca.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

OTHPLN8537 7/09

Fraud Advisory Panel

DATA PROTECTION AND THE INVESTIGATOR

Anti-Money Laundering and Data Protection

July 2009

INTRODUCTION

UK anti-money laundering legislation can be found in the Proceeds of Crime Act 2002 ('POCA') and the Terrorism Act 2000 ('TA') (together, 'the anti-money laundering legislation'). Both pieces of legislation create a disclosure regime, imposing the following obligations:

- to disclose knowledge or suspicion of money laundering/terrorist financing;
- to obtain consent to transact in appropriate circumstances; and
- not to 'tip off' an individual about whom a money laundering disclosure has been made or who is being investigated.

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.

Under the Act, 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.

Data subjects (the people that the data is about) have a right under the Act to access the personal data that is held about them.

There is therefore a potential conflict between the obligations under the Act to allow a data subject to access his/her personal data and the obligations imposed under the anti-money laundering legislation not to 'tip off' an individual about whom a money laundering disclosure has been made.

DUTY TO REPORT SUSPICIONS

The POCA imposes an obligation on individuals in the 'regulated sector' to disclose suspicions of money laundering as soon as is practicable. Businesses in the regulated sector include, but are not limited to, financial institutions, law firms and estate agencies. Investigators should seek specialist legal advice if they are in any doubt as to whether their business falls within the regulated sector and whether, on a case by case basis, they are obliged to make a disclosure.

The TA imposes an identical obligation of disclosure where a person has suspicions of the provision of monetary support for terrorist activities. The obligation is imposed on businesses in the non-regulated sector.

Disclosures must be made to the Serious Organised Crime Agency ('SOCA') by way of a Suspicious Activity Report ('SAR'). Failure to do so is a criminal offence and carries a custodial sentence.

TIPPING OFF

In order to prevent individuals from warning those about whom they have made a disclosure, the anti-money laundering legislation also criminalises 'tipping off'.

The POCA and the TA both provide that where a person in the regulated sector knows or suspects that a SAR has been made to law enforcement authorities, other than in certain strictly defined circumstances it is an offence for him/her to make any disclosure which is likely to prejudice any investigation which might be conducted following the making of the SAR. The most obvious example of a disclosure likely to prejudice an investigation is letting the individual know that the authorities are interested in him/her so that he/she has time to destroy evidence.

Where a person (whether or not in the regulated sector) knows or suspects an investigation has begun or is pending, he/she commits an offence if he/she makes any disclosure likely to prejudice it.

Note that in each case the offence is committed where disclosure would be 'likely' to prejudice an investigation. There is no requirement that the investigation suffer actual prejudice for the offence to be committed.

The 'tipping off' offences under the POCA and the TA carry custodial sentences.

THE DATA PROTECTION ACT 1998

Under the Act, data controllers must comply with the 'Data Protection Principles' set out in Schedule 1 to the Act. The sixth data protection principle (relevant to the issue in this paper) provides that 'personal data shall be processed in accordance with the rights of the data subjects'.

Investigators need to ensure that they do not infringe those rights. This includes the right of data subjects 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 the 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 'Data Subject Access Request' under section 7 of the Act they must respond 'promptly', but in any event within 40 days of receiving the request.

POTENTIAL CONFLICT BETWEEN THE DATA PROTECTION ACT 1998 AND THE ANTI-MONEY LAUNDERING LEGISLATION

There is clearly a potential concern regarding the interrelationship between the 'tipping off' provisions under the anti-money laundering legislation and data subject access provisions under section 7 of the Act. If an investigator makes a disclosure to SOCA regarding an individual about whom he/she has suspicions of money laundering, the data processed about this individual will contain material which reveals that a SAR has been made. At first blush it may appear that if, in order to avoid a 'tipping off' offence, the investigator refuses to comply with the 'Data Subject Access Request' and provide that individual with access to the data which had been processed about him/her, he/she would be in breach of the Act.

However, the Act provides certain exemptions to the rights of data subjects to access the data any controller processes about them. Section 29 of the Act is the most relevant exemption in the present context. This provides that data controllers are exempt from the provisions pertaining to the rights of data subjects to access the data any controller processes about them if the application of those provisions would be likely to prejudice the prevention or detection of crime or the apprehension or the prosecution of offenders. However, it is important to note that the exemption applies only 'to the extent to which' prejudice is likely; there may be some information which can be disclosed without prejudicing those purposes. HM Treasury has