Data Protection

Manual of Guidance Part 1: Standards

Version 3.0 – Approved by the ACPO Data Protection, Freedom of Information and Records Management Portfolio on 25th February 2010

Replaces Version 2.0 (Approved at the ACPO Data Protection, Freedom of Information and Records Management Portfolio on 26th February 2009)

This manual may be disclosed to the public in its entirety

This manual has been produced by the Association of Chief Police Officers (ACPO) Data Protection, Freedom of Information and Records Management Portfolio Group on behalf of ACPO. It is updated and adapted to reflect decisions made by ACPO, views of the Information Commissioner (where appropriate) and the evolution of the legislation as it is interpreted, challenged or reviewed. All modifications to this manual will be the responsibility of the ACPO Data Protection, Freedom of Information and Records Management Portfolio Group.

All enquiries about this manual should be addressed to the Secretary of the ACPO Data Protection, Freedom of Information and Records Management Portfolio Group.

Acknowledgements

ACPO would like to express its thanks to Andy Begent, Essex Police, and colleagues who have assisted in the creation of this Manual.

ACPO, 1st Floor, 10 Victoria Street, London SW1H 0NN

10 Handling Allegations of Criminal Offences under the Act

10.1 Overview

This chapter provides a summary of the criminal offences contained within the Act, with specific detail on those likely to be of most relevance to the Police.

It describes the procedures that the police and the Information Commissioner will follow when criminal offences under the Act are suspected. It explains that those offences fall within three broad groups:

Offence that is not connected to the Police;

Offence or misconduct identified by, or reported to, the Police relating to police-held personal data;

Offence identified by, or reported to, the Information Commissioner relating to police-held personal data.

The chapter is based on the philosophy that there will be a close working relationship between force data protection officers, Professional Standards Departments and the Information Commissioner in order to help safeguard the public's confidence in the Police's use of personal data.

10.2 The Offences

The following offences within the Act have been enabled:

Section 21(1): Failure to notify the Information Commissioner of the processing of personal data;

Section 21(2): Failure to notify the Information Commissioner of relevant changes to the Notification;

Section 24(4): Failure to provide relevant particulars;

Section 47(1): Failure to comply with a Notice;

Section 47(2): Providing false information in response to a Notice;

Section 55(1), (4) and (5): Unlawful obtaining, disclosing or sale of personal data;

Section 59(3): Unlawful disclosure of personal data by the Information Commissioner;

Schedule 9 para 12 & section 60(3): Obstruction of a warrant or failure to assist re warrant execution;

In addition, an offence within the Freedom of Information Act 2000[64] can also apply to personal data:

Section 77 Freedom of Information Act: Altering, defacing, blocking, erasing, concealing any record to prevent disclosure under section 7 (Subject Access).

The following offences have yet to be enabled:

Section 22(6) & 60(2): Assessable Processing without preliminary notification;

Section 56(5): Enforced Subject Access.

[64] Although Scotland has its own legislation, the Freedom of Information (Scotland) Act 2002, section 77 of the Freedom of Information Act 2000 also has effect across Scotland as it applies to the Data Protection Act 1998, itself a UK-wide piece of legislation.

Breaches of the data protection principles are not criminal offences in themselves (although criminal offences are likely to include breaches of the principles). Breaches of the principles will be reported to the data protection officer and information system owner.

In England and Wales, criminal proceedings may only be instigated by the Information Commissioner, or with the consent of the Director of Public Prosecution (Crown Prosecution Service). In Scotland, criminal proceedings will be brought by the Procurator Fiscal. In Northern Ireland, proceedings can be started by the Information Commissioner or by or with the consent of the Director of Public Prosecutions for Northern Ireland.

All offences, with the exception of those relating to the obstruction of a warrant or failure to assist regarding warrant execution, are 'triable either way offences' which can be tried in England or Wales Summarily in the Magistrates' Court or on Indictment in the Crown Court or in Scotland in the Sheriff Court or High Court of Judiciary on Indictment.

A person found guilty of any of these offences can be sentenced on summary conviction to a fine not exceeding the statutory maximum (currently £5,000), or on conviction on indictment, to an unlimited fine.

On conviction of an offender, the Court may order any data apparently connected with the crime to be forfeited, destroyed or erased. Anyone other than the offender who claims to own the material may apply to the Court that such an order should not be made.

The two offences most relevant to the Police are likely to be those under section 55 and, section 77 of the Freedom of Information Act 2000 (see 10.2.1 and 10.2.2).

10.2.1 Section 55

Under section 55(1) a criminal offence is committed if an individual knowingly or recklessly, obtains or discloses personal data, or the information contained in personal data, or procures the disclosure to another person of the information contained in personal data, without the consent of the data controller (chief officer for police forces).

This does not apply where it can be shown that any of the provisions, outlined under section 55(2) shown below, are satisfied:

> That the obtaining, disclosing or procuring of the information was either, (i) necessary for the purpose of preventing or detecting crime, or (ii) required or authorised by or under any enactment, by any rule of law, or by the order of a court.
>
> That the individual acted in the reasonable belief that he/she had in law the right to obtain or disclose the data, or to procure the disclosure to the other person.
>
> That the individual acted in the reasonable belief that the data controller (chief officer would have consented if he had known of the obtaining, disclosing or procuring, and the circumstances of it.
>
> That in the particular circumstances, the obtaining, disclosing or procuring was justified as being in the public interest.

Section 78 of the Criminal Justice and Immigration Act 2008 inserts a new defence into section 55 of the Data Protection Act 1998. The defence applies when a person acts for journalistic, literary or artistic purposes with a view to the publication of journalistic, literary or artistic material and in the reasonable belief that their actions were justified as being in the public interest.

Where those working for, or on behalf of, the Police have authority to obtain and disclose personal data in the course of their duties, they will commit section 55 offences if they use their position to obtain, disclose, or procure disclosure of personal data for their own purposes.

In addition to the section 55(1) offence there are further offences under section 55(4) and (5) committed through the selling of personal data - specifically, when a person sells or offers to sell personal data where it has been obtained in contravention of section 55(1). An advertisement indicating that personal data is or may be for sale is an offer to sell. Personal data includes information extracted from personal data for the purposes of these offences.

There are no section 55 offences if the personal data in question falls within the national security exemption (Section 28), or if the personal data is 'category (e) unstructured personal data' as defined by section 68(2) of the Freedom of Information Act 2000[65].

Section 77 of the Criminal Justice and Immigration Act 2008 confers a power on the Secretary of State to make an order altering the maximum penalty for an offence under section 55 of the Data Protection Act 1998. No order has yet been made.

10.2.2 Section 77 FOI Act

Under section 77 of the Freedom of Information Act it is an offence to alter, deface, block, erase, destroy or conceal information and personal data sought under the Subject Access and Freedom of Information Act processes if it is done so with the intention of preventing the disclosure of all or part of the information and personal data sought.

This is a summary offence and is punishable by a fine. A prosecution may be instituted by the Information Commissioner or by the Director of Public Prosecutions (or the Director of Public Prosecutions for Northern Ireland where appropriate).

10.3 Process to be followed

Offences fall within three broad groups and will be handled as described in the following paragraphs.

10.3.1 Offence not connected to the Police

Where a police force receives a complaint that a member of the public or another organisation may have committed or be committing a criminal offence under the Act, the allegation will be recorded by the police force in accordance with the National Crime Recording Standard and associated procedures[66].

Examples of section 55 offences include:

A debt collector impersonating a customer to procure the address of a debtor from a bank;

A call centre operative selling a list of a famous customer's 'friends and family' phone numbers to a journalist.

Where an allegation is made the officer in the case will notify the case to the Head of Investigations at the Information Commissioner:

Address:
The Head of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane

---

[65] The Freedom of Information (Scotland) Act 2002 (Consequential Modifications) Order 2004 creates an equivalent in Scotland to the new class of personal data created by section 68 of the Freedom of Information Act 2000 in the rest of the UK.

[66] The 'National Crime Recording Standard' (NCRS) should not be confused with the term 'recordable offences'. The NCRS was introduced in 2002 to help ensure consistency between forces as to what crimes are recorded. Section 55 (and section 77 FOIA) offences are not 'recordable offences' (i.e. they are not recorded on the Police National Computer under The National Police Records (Recordable Offences) Regulations 2000 as amended).

Wilmslow
Cheshire
SK9 5AF

Telephone: 01625 545708

Email: investigations@ico.gsi.gov.uk

Where the offence relates solely to data protection matters, the Information Commissioner will deal with the investigation and prosecution.

In the event of offences under the Act being discovered by the Police in the course of their investigations into other matters (e.g. a fraud investigation) it is important that all evidence relating to data protection matters is secured. In such circumstances the Information Commissioner will provide advice as necessary and assist in the preparation of the case file, with regard to any data protection offences.

Where the circumstances of an offence committed under section 55 of the Data Protection Act 1998 may also constitute an offence under the Official Secrets Act 1989, the Police will investigate the matter and submit a file to the Director of Public Prosecution via the Crown Prosecution Service.

The Information Commissioner and/or the OIC will notify the data protection officer of the outcome of the investigation.

10.3.2 Offence or misconduct identified by, or reported to, the Police relating to Police-held personal data

This section concerns the misuse of police-held personal data by those working for or on behalf of a police force.

Examples of section 55 offences include:

A Police Officer carrying out a PNC check on his/her daughter's new boyfriend to help assess his 'suitability';

A member of Police Staff offering to sell police intelligence to a member of a criminal gang;

A cleaner removing computer printouts from the confidential waste and showing them to family members;

A member of Police Staff viewing the custody record of a famous person in custody;

A Police Officer procuring personal data from a bank, using a 'Section 29.3 Form', for his/her own purposes.

In these circumstances, details of the allegation must be forwarded to the police force's Professional Standards Department (PSD).

The PSD will assess the circumstances of the case and identify a proportionate response to the allegation. The assessment will include consideration of all relevant factors including:

The motive of the offender – was it a case of curiosity, was it for personal gain, was it for another person's gain?;

The nature of the personal data – what quantity was involved, what it related to, its sensitivity, and so on;

The harm and/or distress, potential or otherwise, caused to the person to whom the personal data related and others;

The level of intrusion or breach of privacy suffered;

Previous misconduct or criminal breaches by the offender;

Whether the offender was one of many;

The wider public interest.

Where necessary (for example, confirmation that an offence has occurred), the PSD will seek the views of the data protection officer. The Information Commissioner may also be in a position to provide advice. In all cases the data protection officer should be regularly appraised by the PSD of the progress of any investigation and prosecution into offences under the Act.

Having carried out the assessment, the PSD will be in a position to determine the seriousness of the offence. Although it is not possible to draw up definitive criteria to assess that seriousness, the scale of an offence will be apparent.

Those offences deemed to be low-level in nature - for example, a member of staff browsing a record containing a minimal amount of personal data out of curiosity, where there was little prospect of harm or distress – may be dealt with under misconduct only and will not necessarily require a criminal investigation. Each case will need to be assessed against the above criteria.

Those of a more serious nature – for example, a member of staff selling the names and addresses of witnesses in a forthcoming criminal trial to associates of the person charged – are likely to be considered high-level in nature and would be likely to merit a criminal investigation and prosecution.

Where a prosecution is anticipated the PSD will inform the Head of Investigations at the Information Commissioner' Office who will provide guidance and assistance as necessary, though the police force will retain primacy.

A decision by the Crown Prosecution Service not to proceed with a prosecution under the Act should not preclude notification of the case to the Information Commissioner.

The Information Commissioner is particularly keen on pursuing those who procure the disclosure or sale of Police-held personal data.

PSD will notify the data protection officer of the outcome of the case in order that any necessary remedial action can be identified and undertaken by the force.

10.3.3 Offence identified by, or reported to, the Information Commissioner relating to Police-held personal data.

On occasion the Information Commissioner is likely to receive allegations that a police force or individuals working on its behalf have committed offences under the Act.

In such circumstances, the Information Commissioner will take primacy for the investigation and will notify the force's Head of PSD of the complaint. This will allow the police force to consider running a misconduct investigation parallel to or in conjunction with the Information Commissioner's criminal investigation[67].

Where the offender is a senior police officer of ACC or above the Information Commissioner will notify the Chairman of the Police Authority rather than the Head of PSD (or other appropriate authority as per statute).

10.4 The Role of the Information Commissioner's Head of Investigations

[67] In the case of the Police Service of Northern Ireland such allegations should be dealt with by the Ombudsman and Information Commissioner rather than the Force and Information Commissioner.

The Information Commissioner's Head of Investigations' role can be summarised as follows:

To receive from police forces details of offences that are not connected to the Police;

To advise the relevant Head of PSD (or Police Authority in certain circumstances) when the Information Commissioner identifies or receives an allegation of an offence relating to police-held personal data;

To advise the relevant Head of PSD of any Information Commissioner activity or investigation where there is any suspicion there is police officer or police staff involvement. This is to ensure no conflict with Police activity;

To provide the ACPO Data Protection and Freedom of Information Portfolio Holder with statistics and other information relating to all cases referred to the Information Commissioner by police forces.

10.5 Related Offences

The following are related offences that will be considered when dealing with offences under the Act:

Computer Misuse Act 1990, sections 1-3;
Malfeasance in a Public Office (Common Law);
Conspiracy (Section 1(1) Criminal Law Act 1977);
Conspiracy to Pervert the Course of Justice (Section 1(1) Criminal Law Act 1977;
Breach of Confidence (Common Law);
Freedom of Information Act 2000, section 77;
Fraud Act 2006, sections 2 and 4.

10.6 'Victim Care'

Police forces will take appropriate action within their powers and capabilities to mitigate any damage or distress caused to an individual by virtue of any offence under the Act.

10.7 Standards

Standard	Source
Police force has effective procedures in place to ensure that breaches of data protection principles are reported to the data protection officer and information system owner.	10.2
Police force has effective procedures in place to ensure that the Information Commissioner's Head of Investigations is informed of allegations of criminal breaches of the Act as prescribed.	10.3.1
Police force has effective measures in place which ensure that the data protection officer is appraised of the progress of and outcome of all allegations and investigations regarding criminal breaches of the Act.	10.3.2
Police force has procedures in place to ensure that the police force conducts a process to identify any 'lessons learned' at the conclusion of an enquiry in order to identify measures that will be adopted to prevent re-occurrence.	10.3.2
Police force handles allegations of S55 offences by those working for on behalf of a police force in accordance with the procedures described in the MoG.	10.3.2 – 10.6

11 Disclosure of Personal Data by the Police

11.1 Overview

This chapter focuses on the disclosure of personal data by the police to external organisations and individuals. It provides a methodology which data protection officers may follow when considering the data protection aspects of such disclosures (see 11.2 to 11.3).

'Disclosure' may involve the provision of personal data by any means, including; verbally (either at meetings or via the telephone), electronically (email, text, internet, fax) and by the supply of hard copy-documents (letters, memoranda, reports and 'print-outs'). The term 'disclosure' in this chapter should not be confused with the rules for disclosure as provided by the Criminal Proceedings Investigations Act 1996 (CPIA) or the Civil Procedures Rules.

The chapter examines requests by the police for the disclosure of personal data from other bodies and organisations using a standard form and the exemption under section 29.3 of the Act (see 11.5). A brief examination of disclosures required by law can be found at 10.6, while 10.7 introduces forthcoming work to produce an A-Z reference of disclosure/information sharing for the police service. Standards relating to disclosure can be found at 10.8.

Related guidance on 'information sharing' may be found in section 6 of the MoPI Guidance.

11.2 Introduction

Disclosures of personal data can be divided into various types based upon the legal basis underlying them as shown in the diagram below. The whole diagram represents all disclosures by the police. The second 'row' on the diagram shows that those disclosures can be divided into those under statute (yellow side) and those under common law (green side). The third 'row' shows that the statutory disclosures can be further divided into those where there is an obligation or compulsion to disclose and those where there is a power to disclose, but not an obligation. Finally, the bottom row provides some examples of disclosures in the three categories.

All Disclosures		
Statutory		**Common law**
Obligation Requires disclosure	**Power** Gives the option/discretion (i.e. the power) to disclose, but does not compel	where there is a pressing social need and it is necessary and proportionate to do so for policing purposes – public interest test
e.g.	e.g.	e.g.
Child Support Agency Subject Access Court Order	Statutory partners [Section 115 Crime and Disorder Act 1998] CRB [Part V Police Act 1997]	Crimewatch, any individual or body, And, currently for: notifiable occupations