

# STATEMENT OF INFORMATION MANAGEMENT PRACTICE

SECOND EDITION, MAY 2007

**SOCA**  
SERIOUS ORGANISED CRIME AGENCY



## PURPOSES OF THIS STATEMENT OF PRACTICE

### INTRODUCTION

1. The publication of this statement of practice serves two purposes:
  - a. an explanatory purpose, to help established and potential information partners to understand the legal basis for SOCA's acquisition, storage and use of personal or other sensitive information. The statement therefore emphasises the lawfulness of disclosure of information to SOCA by all government departments, other public authorities, private organisations, and individuals who may hold information relevant to tackling serious criminals and the harm they cause;
  - b. a codification purpose, to make clear to SOCA's staff and information partners the procedural standards and safeguards that will be observed by SOCA in its acquisition, storage and further disclosure of information.
2. This statement of practice concerns all information received or generated by SOCA. It covers information shared voluntarily with SOCA by virtue of the information gateways created by the Serious Organised Crime and Police Act 2005 in order to facilitate operational activity against serious criminality and the harm it causes. It also covers information provided to SOCA under non-discretionary regimes, such as the suspicious activity report regime required by primary UK legislation including the Proceeds of Crime Act 2002, and as a result of international conventions such as the European Mutual Legal Assistance Convention.
3. All of SOCA's information relationships, whether voluntary or non-discretionary, are underpinned by policies that set out the agreed standards, procedures, and safeguards.

## SOCA'S FUNCTIONS - THE LAW ON INFORMATION GATHERING AND DISCLOSURE

### THE STATUTORY FUNCTIONS OF SOCA

4. The legal basis for SOCA's information activity is clearly set out in the Serious Organised Crime and Police Act 2005. The Act contains strong provisions for SOCA's information functions. The intention of Parliament in enacting these provisions was vigorously to promote the sharing of information between government departments, other public authorities, private organisations, individuals and SOCA in the cause of the prevention and detection of crime and the mitigation of the harm it causes. In introducing the Bill the Home Secretary acknowledged the need for improvement in this area and noted, "...how difficult it has been, even with good will, to exchange the necessary intelligence information and to link investigation, intelligence and prosecution. The added value of the Serious Organised Crime Agency will be measured by its ability to do just that". It was, he said, necessary, "... to ensure that that the Agency is not subject to those problems".<sup>1</sup>
5. By virtue of S2 (1) SOCA has the statutory functions of:
  - a. preventing and detecting serious organised crime, and
  - b. contributing to the reduction of such crime in other ways and to the mitigation of its consequences.
6. SOCA's information activity extends beyond serious organised crime, however, to include more general information support for law enforcement and harm reduction. By virtue of S3 (1), SOCA has the statutory function of gathering, storing, analysing and disseminating information relevant to –
  - a. the prevention, detection, investigation or prosecution of offences, or
  - b. the reduction of crime in other ways or the mitigation of its consequences.

<sup>1</sup> Hansard 7/12/04 Columns 1046, 1049.

## DISCLOSURE OF INFORMATION TO SOCA

7. By virtue of S34 (1) any person is permitted to disclose information to SOCA if the disclosure is made for the purpose of the exercise by SOCA of any of its functions.
8. S34 (2) provides that the disclosure of information to SOCA in such circumstances does not breach any restriction on the disclosure of the information however imposed. For example, the following restrictions will not apply:
  - a. any common law restriction, as in an obligation of confidence;
  - b. any statutory restriction (other than that imposed by Part 1 of the Regulation of Investigatory Powers Act 2000 or the Data Protection Act 1998 – see below);
  - c. any contractual restriction.
9. S34 (3) requires that any disclosure of personal data must not contravene the provisions of the Data Protection Act 1998 (DPA). S29 of the DPA creates powerful exemptions from many of these provisions where personal data are disclosed for purposes related to the prevention and detection of crime. In particular, personal data are exempt from the non disclosure provisions of the DPA, as set out in S27 (3) of the Act, where the disclosure is necessary for the exercise of any functions conferred on any person by an enactment and where non disclosure in the particular case would be likely to prejudice the purposes of the prevention and detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty or of any imposition of a similar nature.
10. In the case of disclosures to SOCA:
  - a. the functions conferred by an enactment include the gathering, storing, analysis and dissemination of information, which necessarily depend upon the disclosure of information to SOCA;
  - b. SOCA's ability to prevent and detect crime, a feature of which is the mitigation of the harm caused by crime, would necessarily be prejudiced if personal data were not disclosed to the agency;

- c. the provision of information to SOCA in any particular case is likely to be both necessary and proportionate where it is provided for the purposes of the prevention and detection of crime as set out in the DPA;
- d. further exemptions apply under S28 of the DPA to disclosures for the purpose of safeguarding national security. This will be relevant where, for example, SOCA is acting in support of the Security and Intelligence Agencies.

### **DISCLOSURE OF INFORMATION BY SOCA**

11. SOCA may, by virtue of S3 (2) disseminate information which it has gathered, stored and analysed to police forces, law enforcement agencies, or such other persons as it considers appropriate in connection with any of the matters in S3 (1) (a) and (b), namely: the prevention, detection, investigation or prosecution of offences, or the reduction of crime in other ways or the mitigation of its consequences.
12. S32 of the Act enables information obtained by SOCA in connection with the exercise of any of its functions to be used by SOCA in connection with any of its other functions, and S33 (1) enables SOCA to disclose information obtained in connection with the exercise of any of its functions where the disclosure is for a 'permitted purpose'. The definition of 'permitted purpose' effectively extends the scope of S3 (2) to permit disclosure of information for the purpose of prevention, detection, investigation or prosecution of criminal offences or the prevention, detection or investigation of conduct for which penalties other than criminal penalties are provided (whether the criminal offences or conduct are alleged to have taken place in the UK or elsewhere). Disclosure is also permitted to enable SOCA to respond to requests for support from law enforcement agencies and to support the work of the intelligence services in the exercise of their functions. Further disclosure by SOCA of information supplied by HM Revenue and Customs will be made in accordance with the consents provided by the Commissioners.
13. In order to discharge its functions SOCA seeks productive information relationships with a wide range of government departments, other public authorities, and private organisations.

## ECHR, DPA, STANDARDS AND SAFEGUARDS

**SCOPE, NECESSITY AND PROPORTIONALITY OF SOCA'S INFORMATION REQUIREMENTS**

14. SOCA will not gather or disclose information for any purposes other than to carry out its statutory or other legal functions. Any disclosure to or by SOCA must be considered in the light of the Human Rights Act 1998 and, in particular, Article 8(1) of the European Convention on Human Rights (ECHR) which applies, *inter alia*, to the use and disclosure of personal data. However, a disclosure of personal data is permitted which is:
  - a. necessary in the interests of public safety, the protection of public order, health or morals, or for the protection of the rights and freedoms of others;
  - b. in accordance with the law;
  - c. proportionate.
15. It is highly likely that any disclosures of personal data which are made within the terms of S29 (3) DPA will fully comply with the disclosing person's obligations under the Human Rights Act (if any – unlike public authorities, most private sector bodies are not governed by the Human Rights Act and are not therefore bound by the requirements of the ECHR, including Article 8(1) as it relates to the disclosure of personal data).
16. In order further to secure its observance of Article 8 and the DPA, SOCA has put in place standards for the identification of its information requirements and for its handling, storage, processing and dissemination of data. Those standards are set out below at paragraph 23 *et seq.*

**SOCA'S INFORMATION REQUIREMENTS**

17. SOCA is the UK's main source of intelligence assessments of the threat to the United Kingdom from serious organised crime. A proper appreciation of the threat is vital to the effective shaping and execution of the government's strategic aim to reduce the harm caused by serious organised crime. This requires the closest cooperation by all those

government departments and agencies, and other bodies, who hold or may acquire information that sheds light on the activities of organised criminals and the harm they cause.

18. In order to facilitate this cooperation, SOCA has produced the National Intelligence Requirement in respect of serious organised crime. The intelligence requirement is endorsed by the Cabinet Sub-Committee on Organised Crime. This ministerial endorsement underlines the importance of SOCA receiving the information it needs in order to fulfil its statutory functions, and is relevant to any considerations of proportionality on the part of the owner of the information.
19. The information required by SOCA for the purpose of its functions relating to serious organised crime falls within the scope of the ministerially endorsed National Intelligence Requirement.

## **CATEGORIES OF INFORMATION**

20. SOCA will seek access to information in the possession of another body only where it believes that the other body holds or is likely to hold relevant information.
21. SOCA generally seeks information in three broad categories:
  - a. 'personal' information on individuals whom SOCA suspects to be involved in or closely associated with others involved in serious crime, or whose personal information is required in connection with SOCA's duties under statute or international conventions;
  - b. information that enables the identification and profiling of persons whose activities fall within SOCA's statutory responsibilities. Such information may include 'bulk' personal data relating, coincidentally, to members of the public where that information contributes to the gaining of an understanding of criminal business methods or the identification of criminal targets – for example passenger lists believed to include drug couriers. Further considerations in respect of SOCA's access to 'bulk data' are set out in paragraph 28 *et seq.*;

- c. other information of strategic and policy importance relating to the extent of, and changes in the nature of, the harm caused by serious organised crime. This category includes information relevant to SOCA's responsibility to assist public and private sector partners in reducing opportunities for crime. Data in this category may contain some personal information relating to those affected by serious organised criminal activity, or may contain material that needs to be handled with sensitivity, such as that which relates to particular communities or ethnic groups or which is commercially sensitive.
22. SOCA will seek such information in electronic or other formats depending upon need and the technical capability of SOCA and its information partners. SOCA's practice standards apply equally to transactions in all media.

## **STORAGE AND DISCLOSURE OF INFORMATION – STANDARDS AND SAFEGUARDS**

23. The standards and safeguards for storage and disclosure of SOCA's information, as set out in this statement of practice, are compatible with those contained in the *Code of Practice for the Management of Police Information (2005)* applied by the Home Secretary to police forces in England and Wales.
24. SOCA fully embraces the principles set out in ISO/IEC27001 relating to information security management, and is working towards full compliance with this internationally recognised standard.
25. SOCA will observe, in the relevant areas of its information activity, the standards set out in the *Code of Practice on Legal Admissibility and Evidential Weight of Information Stored Electronically (BSI BIP0008:2004)*. In addition to these specific standards, SOCA will:
  - a. apply appropriate Government Protective Marking Scheme (GPMS) classifications to its information, and will manage its information accordingly;

- b. maintain a secure communications capability and use it to transmit and receive all protectively marked material as required by the assigned classification;
- c. maintain criteria ('recording categories') which will be used to test the relevance of all information received or generated by SOCA to SOCA's purpose and functions, and to ensure that information disclosed to SOCA which is not relevant is rejected. The relevance and reliability of information will be evaluated before it is permanently recorded in SOCA's intelligence systems;
- d. pay due regard to any restrictions placed upon the recording, disclosure, or further use of information disclosed to SOCA by others;
- e. before permanent inclusion of information into systems, assess the risks to the data subject or source, arising from use of the information (whether received from either public sector or private sector sources), or from the likely result of disclosure of the information;
- f. protect intellectual property and commercially sensitive information provided by others, taking into account any expressed requirements concerning the maintenance of commercial confidentiality in its storage and use of information received from private sector sources;
- g. disclose information to private sector bodies only where the recipient's use of the information supports the discharge of SOCA's statutory functions, and where SOCA is satisfied on reasonable grounds that the recipient is able to handle the information securely and observe any restrictions imposed on the use or further disclosure of the information;
- h. restrict access to its information systems to authorised personnel. Persons permitted access to information will access and use it only in connection with their official business.

26. Where appropriate, SOCA will enter into written information sharing agreements with its principal information partners the terms of which may specify the standards to be observed in the transmission, storage, use and retention of personal or other sensitive information.
27. SOCA will determine retention criteria for all classes of information. Systems will be subject to periodic review in line with the criteria, in order to ensure the continuing accuracy and relevance to SOCA's functions of the information held.

### **BULK DATA MANAGEMENT – STANDARDS AND SAFEGUARDS**

28. SOCA recognises that particular concerns may arise for information partners where 'bulk data access' is sought. In certain instances it may not be possible to separate relevant and irrelevant information, for example where serious organised criminals set out deliberately to conceal their criminal activity by 'losing' it within large scale legitimate activity. In such cases the success of an investigation and prosecution may depend upon the retention of sufficient contextual material to prove the criminal business methodology used, and the disclosure of large quantities of data, including personal data, may be essential to SOCA's functions.
29. Whilst disclosure of personal data should never be unthinking or routine<sup>2</sup>, the disclosure of bulk personal data complies with the provisions of the DPA if it is done for the prevention or detection of crime and where the disclosure of bulk personal data is necessary to achieve these objectives. The requirement that disclosure be considered on a case by case basis does not mean that the disclosure of each portion of data must be separately considered, but that, taken as a whole, the bulk disclosure is necessary and proportionate.

<sup>2</sup> *Department for Constitutional Affairs "Public Sector Data Sharing: Guidance on the Law November 2003" para. 6.30*

30. To this end:
- a. SOCA will not seek disclosure of personal data where the personal details are not relevant to its requirements. SOCA will seek disclosure of bulk personal data in order to fulfil its statutory functions relating to serious organised crime, and will consider in each case whether any alternative form of disclosure that contains less risk of collateral intrusion would be sufficient for the purpose;
  - b. subject to the requirements of the Criminal Procedure and Investigations Act 1996, following research and analysis, SOCA will retain only such elements of collateral material as remain relevant to the functions of SOCA and only for so long as relevance continues;
  - c. access to collaterally intrusive material within SOCA will be restricted to authorised staff;
  - d. notwithstanding the effect of the statutory information gateways contained in the Serious Organised Crime and Police Act and Ss 28 and 29 of the Data Protection Act, SOCA will, where necessary, put in place written agreements with partner agencies concerning the terms and conditions attaching to 'bulk data access'.

### **COMPLIANCE WITH STANDARDS AND REVIEW OF THIS STATEMENT OF PRACTICE**

31. SOCA will put in place policies and procedures to ensure high standards of compliance and integrity in the management of its information. SOCA's information management policies and practice are subject to Board level scrutiny and to independent inspection by, *inter alia*, Her Majesty's Inspectorate of Constabulary and the Office of the Surveillance Commissioner.
32. This statement of practice will be subject to regular review and revision as necessary.

**SOCA**  
SERIOUS ORGANISED CRIME AGENCY

