

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

Section 1: Background

Question 1. Please explain what your interest in information sharing is. If you have an active involvement in personal information sharing, we would be grateful for the following information:

- **what kinds of personal information do you collect, hold and share?**
- **how do you collect, hold and share such personal information?**
- **for what purposes do you collect, hold and share such personal information?**

Comments:

The Serious Organised Crime Agency (SOCA) has the statutory function of, inter alia, gathering, storing, analysing and disseminating information relevant to the prevention, detection, investigation or prosecution of offences, or the reduction of crime in other ways or the mitigation of its consequences.

The disclosure of information by and to SOCA is provided for in Sections 33 and 34 of the Serious Organised Crime and Police Act 2005 (SOCPA 2005). These sections provide for information sharing in support of SOCA's statutory functions. SOCA also maintains the UK's system for managing disclosures by financial institutions of suspicious transactions (known as 'Suspicious Activity Reports') under proceeds of crime legislation, as well as acting by agreement as the UK's central authority for the law enforcement community for issues such as Interpol requests relating to international law enforcement, reports of counterfeit currency

and suspicious transactions of chemicals used in synthetic drugs manufacture.

SOCA collects, holds and shares information on individuals whom we suspect to be involved in serious crime, or closely associated with others so involved, or whose personal information is otherwise required in connection with our duties under statute or international conventions. We also seek information that enables the identification of persons whose activities fall within SOCA's statutory responsibilities.

Information is collected from an extensive range of partners – law enforcement and other public bodies in the UK and abroad, the private sector and individuals, as well as through covert means as provided for by the Regulation of Investigatory Powers Act 2000. Information released by partner agencies to SOCA is typically either in support of requirements to progress specific operations, or more generally volunteered under terms of the National Intelligence Requirement. The latter is a document that SOCA produces and circulates to partners that outlines critical gaps in knowledge about the serious organised crime threat to the UK. In addition, SOCA staff have direct access to certain national databases – the Police National Computer for example - by agreement with the organisations responsible for these. SOCA also collects information from a range of open sources

Some of the information SOCA collects comprises 'bulk' personal data relating, coincidentally, to members of the public more generally where that information contributes to the identification of criminal targets and understanding of criminal activity (for example, airline passenger lists believed to include drug couriers).

We furthermore collect, store and use personal information to maintain records of our staff and contractors.

Information exchange between SOCA and partner agencies, and the sharing of information within SOCA, is essential to ensuring we are able to meet our statutory functions. Information may be shared by SOCA with a wide range of external agencies where a need is identified relevant to those statutory functions. Some of our principal partners in this regard include:

- UK law enforcement agencies, especially the police and other organisations with enforcement powers;
- prosecuting authorities and the courts;
- relevant inspectorates, tribunals and commissioners overseeing aspects of legal compliance;
- foreign law enforcement agencies;
- the UK intelligence agencies;
- government departments and other public agencies, and commercial and private

sector organisations who need to be alert to threats from serious organised crime or who can contribute operationally to combating it.

Information is stored in a combination of electronic and physical records. SOCA has an advanced programme for information management which seeks to set out standard processes and systems for the storing and use of all information necessary for its statutory functions.

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2. What in your view are the key benefits of sharing personal information to a) individuals and b) society? Please provide examples.

Comments:

SOCA's ability to reduce the harm caused by serious organised crime depends on receiving and sharing information with a wide variety of partners. Moreover, the ability to cross reference various sets of data supplied as described in the comment on Q1 above has led, and will continue to lead, to significant benefits in identifying and tackling serious organised crime.

Two recent examples illustrate the power of effective data sharing for SOCA:

- an operation involving cross-matching of data between SOCA internal systems, the Suspicious Activity Reports system and public sector partner systems helped to identify a significant fraud against the UK passport issuing process perpetrated by a serious organised criminal. The outcomes of the operation included the conviction of the organiser, and led to a change in risk management procedures to further protect the integrity of the passport application procedure;
- an operation involved releasing details to public and private sector institutions of information regarding the use in the UK of fraudulent documents received by an international partner. Cross-referencing of information supplied by SOCA by the recipients has led to the recovery of fraudulently obtained tax credits totalling over £750,000, the improvement of fraud prevention measures in financial institutions and enforcement action by a regulatory authority against individuals holding licenses issued by that authority.

SOCA has a number of such data sharing initiatives in hand and we see data sharing as a key innovative tool in helping to tackle serious organised crime, especially aspects involving sophisticated fraud and money laundering. We intend to develop these approaches further.

Question 3. What in your view are the key risks of sharing personal information to a) individuals and b) society? Please provide examples.

Comments:

A lack of commonly agreed data standards poses a risk. This can lead to the creation of multiple records for one individual, even within one organisation, which means that individuals are unable to be assured that they are able to exercise their rights over data held on them by controllers. Records where there are insufficient personal data to establish a unique identity can be troublesome for authorities processing them, for sharing between agencies with legitimate needs to access the data, for the individual data subjects themselves and for individuals who may be the subject of actions as a result of mistaken identity. Working towards a standard protocol for the storage and formatting of data would greatly improve this situation.

Question 4. As mentioned in the introduction, there are wide variations in the scope and methods of personal information sharing. What scope and methods, in your view, pose the greatest opportunities or risks? Please explain the reasoning behind your response.

Comments:

As illustrated above (Q2), 'bulk' data sharing and cross-matching against suspected criminal data, where targeted appropriately, can have a significant effect on prevention and detection of crime. However, the data must be handled securely and procedures put in place requiring compliance by all involved to avoid data loss or misuse. The use of bulk data for these purposes should clearly satisfy tests of necessity and proportionality with regard to the desired outcomes.

In that context, SOCA has made commitments in its Statement of Information Management Practice (the public document of information governance) about the management of disclosures of bulk data that it receives. These seek to ensure that requests made by SOCA are relevant to its information requirements, that considerations are made in respect of alternative approaches that could lead to the same outcomes, and that bulk data is retained by SOCA for only as long as relevant to SOCA's functions.

We occasionally encounter reluctance to lawful requests for such bulk data matching as the resource implications of processing these are perceived by other organisations to outweigh the benefits of engagement. It is possible that significant opportunities to prevent and detect serious organised crime may be missed as a result of such positions.

Question 5. Please provide examples of where in your view, the public authorities hold too much data or not enough personal information, and the reasoning behind your response.

Comments:

As noted under Q3, a lack of universally applicable data standards may lead to the creation of multiple records for the same individual, with disparate information recorded in each record.

Aside from this, we believe that it would be desirable for some more specific guidance on retention schedules, to supplement that provided in the recently published framework code of practice for sharing personal information. This would help to establish more consistent approaches to retaining and deleting data. The police service is developing such a standardised framework in response to some of the findings of the Bichard enquiry, but the issue extends beyond the law enforcement environment to all data controllers.

Question 6. Please provide examples of where, in your view, private sector organisations hold too much personal information or not enough personal information, and the reasoning behind your response.

Comments:

SOCA has no comment on this.

Question 7. Please provide examples of cases where you believe the sharing of personal information between two or more bodies would be beneficial, but where it is not currently taking place.

Please explain as fully as possible why information is not being shared, detailing what the barriers are to the sharing of personal information are – e.g. legal, cultural, financial, institutional – and how these barriers can be overcome.

Comments:

SOCA has encountered occasional difficulties in assuring information suppliers of the lawfulness of disclosing information under the provisions of SOCPA 2005. We have sought to address this through the publication of our Statement of Information Management Practice. Nevertheless, some difficulty in the application of different legislation is evident, particularly a lack of confidence or understanding of the impact of the permissive gateways in SOCPA 2005 on any legislation potentially restricting the release of information, and how this sits alongside the need to comply at all times with the requirements of the DPA. SOCA has been advised by data controllers, on occasions, that we must obtain a court Production Order before personal data will be released, despite the requests being permitted by both the DPA and SOCPA. Such practice is resource intensive, both within SOCA and in court terms.

We seek to overcome these difficulties through negotiation and agreement with individual suppliers of information. Some guidance was published by the former Department of Constitutional Affairs in November 2003 which sought to clarify such matters for intra-governmental information sharing, but a statement or guidance from the Information Commissioner's Office on the compatibility of such information gateways and the DPA would be welcome.

Question 8. Please provide examples of cases where you believe that personal information is being shared between two or more bodies, but where this should not be taking place.

Comments:

We are concerned at the activities of private investigators in illegally obtaining and processing personal data. The private investigation industry is not, as yet, subject to professional regulation and nor is it constrained like public authorities by the Regulation of Investigatory Powers Act. At its more unscrupulous end, there is clear evidence of elements of the industry obtaining personal data for criminal purposes and being engaged in significant corruption of public officials to secure access to privileged personal data.

Section 3: The legal framework

Question 9. In your view, how well does the DPA work? Please outline the DPA's main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.

Comments:

SOCA is of the view that the data protection principles are well-understood, but also believes that the structure of the DPA is highly complex and that this hinders application of its requirements by non-specialists who process personal data on a daily basis. We believe that some clarity and amendment to the Act and ICO guidance could usefully be considered, as set out below:

- we rely on the exemptions under Section 29 (and, to an extent, 28) for much of our operational business. We believe that greater prominence and clarity for guidance on these exemptions would be helpful, to assist potential information suppliers to understand what precisely these exemptions permit in practice, and their compatibility with legal gateways such as those in SOCPA 2005. Some additional guidance on the formulation of responses to subject access requests where SOCA (and other appropriate agencies) invoke the S29 exemption would also be helpful;
- the requirement to assess whether information sought under S29 is properly required for the prevention or detection of crime may place an onus on data controllers that may be unreasonable. There is a risk that some data controllers may prejudice the prevention and detection of crime by failing to release data through lack of understanding of law enforcement decision-making. It may be worth considering an amendment to the effect that data controllers may release information necessary for the prevention and detection of crime on the basis of certification from recognised law enforcement agencies, including SOCA, that the information is so required. The responsibility for the legality of the request would thus transfer to the requesting data controller rather than the provider;
- SOCA devotes significant effort to non-fiscal fraud, where the use of aliases and

fraudulently obtained documents by many serious organised criminals is commonplace. Some clarity on the extent to which “personal data” in fraudulently obtained documents (including aliases, false and stolen identities) constitutes personal data as intended by the DPA would be useful;

- some guidance on the applicability of the exemptions under Section 31 to SOCA would be welcome, especially when we are investigating complaints on behalf of or under the supervision of the Independent Police Complaints Commission. Also in this context, SOCA has internal processes to ensure that staff abide by a set of standards and policies regulating their conduct. Misconduct by staff may not constitute criminal behaviour, but may undermine the integrity of the organisation and threaten our fitness to function effectively as a law enforcement agency. Investigating such conduct in SOCA is a high priority and may on occasions require the use of techniques whose disclosure in subject access requests would be prejudicial to current and future investigations. Some guidance on the extent to which exemptions may apply, either under sections 29 or 31, would be helpful;

Question 10. In your view, how well do public authorities and private organisations adhere to the second principle of the DPA? How valuable do you believe the second principle is? Please provide examples and the reasoning behind your response.

Comments:

SOCA is permitted by virtue of S32 of SOCPA 2005 to use information obtained in connection with the exercise of any of its functions for any of its other functions. SOCA does not view this as incompatible with the DPA, given that the majority of our functions are directly connected with the prevention and detection of crime.

Question 11. What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Please provide examples.

Comments:

SOCA has no further on comment on this question.

Question 12. What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA.

Comments:

Please see the comments at Q9.

Question 13. Are there any other aspects of UK law or EU law (such as EU Directive 95/46/EC) that impact positively or negatively on data sharing or data protection? Please provide examples.

Comments:

There is a risk that the European Data Protection Framework Decision may impact on SOCA's ability to share information with organisations outside the UK. This may conflict with our general crime prevention and harm reduction functions, which frequently have an international dimension. SOCA has made representations to the Ministry of Justice on this issue. This issue has the potential to increase significantly the complexity of assessing the data protection issues surrounding the release of data overseas to some organisations for law enforcement purposes.

Question 14. Are there any statutory powers unavailable that would enable better and more secure sharing of personal information – for example for identity authentication purposes – between a) public authorities and b) public authorities and private organisations? If so, what are they?

Comments:

We believe that the National Identity Scheme might offer opportunities for better and more secure sharing of personal information and are monitoring the development of the scheme with relevant stakeholders.

Question 15. Are there any parts of the legal framework that place an unreasonable burden on business? Please provide examples.

Comments:

Guidance would be welcome from the ICO on the practice by some information suppliers of imposing charges on requests for personal data.

Section 4: Consent and transparency

Question 16. Is it clear whether and when you need individuals' consent to share information about them? Are you clear about the form that consent should take? Please provide examples.

Comments:

We believe that the position on obtaining consent from individuals is clear. SOCA frequently uses the S29 exemptions to share information about the subjects of its operations when it is necessary to do so for the prevention and detection of crime.

Question 17. What, if any, barriers would a requirement for gaining consent create to the sharing of personal information? Please explain your reasoning.

Comments:

A universally applicable requirement for gaining consent (without appropriate exemptions) to share personal information would prevent SOCA almost entirely from being able to carry out its statutory functions.

Question 18.

Do you have any suggestions on how to make the sharing of information more transparent? For example, should individuals be given strengthened access rights? And if so, how? Should organisations be expected to do more to explain their use and sharing of personal information to the public? And if so, how?

Comments:

SOCA has sought to explain its requirement for and use of information by publishing its Statement of Information Management Practice. The SIMP has the dual purposes of explaining the legal basis for SOCA's acquisition, storage and use of information in view of the gateways created in SOCPA 2005, and a codification purposes setting out standards and safeguards which SOCA will observe in its information management.

SOCA makes the SIMP available through its public website, in exchanges with partners and it is used in internal training. The SIMP is kept under review to ensure it remains fit for purpose.

Question 19. How can we best ensure that information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability? For example, in your view how valuable is the Information Commissioner's recently published Framework code of practice for sharing personal information? In your view, how valuable are privacy impact assessments announced by the Information Commissioner on 11 December?

Comments:

SOCA welcomes the publication of the framework code of practice for sharing personal information and is reviewing its internal policies and procedures for compatibility with the code.

In common with many other agencies, we are in the initial stages of exploring the use of Privacy Impact Assessments and are determining the contexts in which SOCA may seek to adopt the PIA process.

Section 5: Technology

Question 20. What impact in your view have technological advances had on the sharing and protection of personal information? Please provide examples.

Comments:

Technology facilitates the accrual of large aggregations of personal data, and makes it easier for large amounts of data to be transmitted to third parties. The ease and convenience of e-mail in particular can lead to safeguards and good practice around personal data processing being overlooked, or even ignored. There are also high risks surrounding the transport of large amounts of data on compact removable media. We recognise that these advances may increase the risks to information we disclose to our partners and accordingly we look to manage risks through evaluation of processes, agreements with partners and strict adherence to security rules surrounding transport of information assets.

The Government Protective Marking System, and the Manual of Protective Security which supports it, do not give clear guidance on how to handle large aggregations of personal data where the sensitivity and potential national damage arising from loss or compromise of the whole may be very much greater than that pertaining to any one item in the aggregation. This may lead routinely to inappropriate protection being given to such aggregations..

Question 21. Should the law mandate specific technical safeguards for protecting personal information? For example, should there be an explicit requirement that all personal information held on portable devices be encrypted to a particular standard?

Comments:

In our view, while technical safeguards may be helpful, they are only as reliable as the people operating them. People factors are almost always the weakest link in any security system. Standards of personal behaviour and reliability must be established and maintained if technical safeguards are to function as intended. However, it is clear that more routine application of encryption to the "aggregation" problem identified above would be helpful.

Question 22. How, in your view, could 'privacy enhancing techniques', such as the anonymisation or pseudonymisation of personal information, help safeguard personal privacy, whilst facilitating activities such as performing medical research? Is sufficient advice about the deployment of such techniques available? Are you confident about using them? What are the barriers to using them?

Comments:

This is not really relevant to SOCA's functions, although we would be concerned if routine anonymisation and pseudonymisation of personal information allowed criminals to derive some inadvertent benefit from such techniques.

Section 6: International comparisons

Question 23. Are you aware of any jurisdictions whose legal framework for sharing and protecting personal information contains features that could be useful in a UK context? Please provide examples.

Comments:

We have no comment at this stage.

Question 24. Do you have any international examples of good practice in the sharing of personal information that could or should be adopted by the UK?

Comments:

We have no comment at this stage.

Question 25. Do you have any knowledge of jurisdictions that have adopted a particularly permissive or restrictive approach to sharing personal information? What have the consequences of this been?

Comments:

We have no comment at this stage.

Question 26. Are you aware of significant differences in public attitudes to the sharing of personal information in other countries? Please provide examples and an explanation for why you believe this to be the case.

Comments:

We have no comment at this stage.

Section 7: Additional questions

Question 27. Are there any additional issues on the sharing of personal information and protection of personal information that this review should be considering. Do any of these apply specifically to your sector?

Comments:

As we hope is evident from this response, SOCA has a high degree of interest in this topic. We are keen to ensure that an environment prevails which enables us to continue with effective data sharing activities to support our functions under law in countering serious crime, while appreciating and taking into account the potential areas of public concern around data sharing generally. We would welcome the opportunity to meet and discuss issues raised in the consultation with Mr Thomas and Dr Walcott and their staff.

Question 28. Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.

Comments:

