Data protection

ICO review:

Data sharing between the public and private sector to prevent fraud

Version 1

16 April 2015

Information Commissioner's Office

Contents

Summary

The Serious Crime Act 2007 (SCA) allows public authorities to share information with Specified Anti-Fraud Organisations (SAFO) for the purpose of preventing fraud.

The Information Commissioner's Office (ICO) has the power to audit and inspect data sharing between the public and private sector for the purposes of preventing fraud and a survey was undertaken to review the arrangements in place.

The results suggest disclosures of personal data are necessary and proportionate for the purposes of fraud prevention and that the overall handling of personal data meets the good practice recommendations of the Information Commissioner's statutory Code of Practice on Data Sharing.

A small number of survey responses suggest some opportunities for improvement, including the following good practice reminders for public authorities:

- Ensure data sharing with SAFOs is governed by agreements setting out agreed rules and standards.
- Maintain records of what personal data is shared with SAFOs and why.
- Make privacy notices available to individuals explaining whom personal data may be shared with and why.
- Check that personal data is of sufficient quality prior to disclosure.
- Agree retention periods with SAFOs to ensure personal data is not kept for longer than is necessary.
- Agree secure methods to transfer personal data in transit to SAFOs.
- Periodically review data sharing arrangements with SAFOs to assure compliance with the law and good practice standards.

In addition to the survey, site visits were agreed with selected SAFOs to review their operations, which provided good assurances that the organisations in question have well-designed systems and processes in place to handle the personal data supplied by public authorities in line with the good practice recommendations and other accepted standards.

Introduction

Sections 68 to 72 of the SCA provide public authorities with a legal gateway to disclose information to SAFOs for the purpose of preventing fraud.

The Home Office's Data Sharing for the Prevention of Fraud Code provides guidance for public authorities sharing information via this gateway and

notes that, during the Parliamentary passage of the SCA, the Government gave an undertaking that the ICO would be given access to audit and inspect data sharing arrangements under the legal gateway.

The ICO is committed to using both implied and express audit powers in support of the promotion of good data protection practice, and has undertaken a review of the data sharing arrangements in place between public authorities and SAFOs to determine the type of data sharing and whether it meets good practice recommendations.

Legal context

The legal basis for data sharing was created in response to rising concerns over the extent of fraud and responses to fraud, and the legal impediments to public sector membership of several existing private sector data sharing schemes for the purpose of preventing fraud.

Sections 68 to 72 of the SCA allow that a public authority may disclose information as a member of a SAFO or in accordance with any other arrangements, and that disclosure would not breach any obligation of confidence owed by the public authority or contravene the Data Protection Act 1998 (DPA). In particular, Section 72 of the SCA inserts a new paragraph in Schedule 3 of the DPA to allow the processing of sensitive personal data through a SAFO where necessary for the purpose of fraud prevention.

The data sharing provisions came into force on 1 October 2008 together with an order specifying six anti-fraud organisations. Five more anti-fraud organisations were specified on 21 July 2014. The 11 anti-fraud organisations specified to date are as follows:

- BAE Systems Applied Intelligence Limited
- Callcredit Information Group Limited
- CIFAS
- Dun and Bradstreet Limited
- Equifax Limited
- Experian Limited
- Insurance Fraud Bureau (IFB)
- Insurance Fraud Investigators Group (IFIG)
- N Hunter Limited (National Hunter)
- Synectics Solutions Limited
- Telecommunications United Kingdom Fraud Forum Limited (TUFF)

Two initial surveys undertaken by the former National Fraud Authority and the Home Office concluded that data sharing has been limited although there was good evidence of ongoing discussions and product development between SAFOs and public authorities.

Approach

The objective of the ICO's review is to establish what data sharing arrangements are in place between public authorities and SAFOs and to establish whether any such arrangements meet the good practice recommendations of the ICO's statutory Code of Practice on Data Sharing and the Home Office's Data Sharing for the Prevention of Fraud Code of Practice, as well as the requirements of the DPA.

The method comprised a survey of 33 public authorities and the 11 SAFOs. The public authorities selected were among those identified by SAFOs as sharing personal data with them for the purposes of fraud prevention.

Site visits were also agreed with a selection of four SAFOs to review their systems and processes. The SAFOs selected were among those who confirmed that they receive personal data from public authorities for the purposes of fraud prevention.

Results

Twenty-two out of the 33 public authorities contacted completed the survey (see appendix 3 for list). Nine public authorities indicated they share personal data with SAFOs for the purposes of fraud prevention either on a regular or occasional basis.

Ten out of the 11 SAFOs contacted completed the survey (see appendix 3 for list). Five SAFOs indicate that public authorities share personal data with them for the purposes of fraud prevention. The remaining responses included organisations that had only recently (at the time of the survey) been specified as SAFOs since July 2014.

The survey showed a significant difference between the number of public authorities that indicate they share personal data with SAFOs and the number of public authorities identified by SAFOs as data sharers. This could mean that some public authorities are confused as to the identity of SAFOs and what legal basis they are relying on for data sharing.

The ICO intends to keep this area under review through ongoing engagement with public authorities, and further reviews are planned for 2015/16 once the recently specified anti-fraud organisations have had a chance to embed their approach.

The following summarises some of the key findings taken from the surveys and site visits.

Agreements

Public authorities sharing personal data with SAFOs do so as members or in accordance with other arrangements, and membership conditions or data sharing agreements set out agreed rules governing the data sharing arrangements. Four out of nine public authorities indicated they do not have agreements with SAFOs, and one public authority indicated they do not record the volume and frequency of data sharing with SAFOs.

Good practice

The ICO's Code of Practice recommends that organisations have data sharing agreements in place, which could form part of a contract with other organisations, particularly where personal data is to be shared on a large scale or regular basis.

The Home Office's Code of Practice recommends that public authorities prepare data sharing documents with SAFOs that set out mutually agreed rules and incorporate the requirements of the ICO's Code.

Fairness and transparency

The DPA requires that personal data is processed fairly. This means that people should generally be aware of which organisations are sharing their personal data and what it is being used for.

SAFOs make privacy notices available on their websites or other published materials that clearly explain who they are, why they process personal data and with whom it is shared. Of particular note, several SAFOs make layered privacy notices available that provide a simple explanation backed up by a more detailed explanation as recommended by ICO guidance. In addition, several SAFOs require that members make privacy notices available as a condition of membership. Two out of nine public authorities indicated they do not make privacy notices available.

Good practice

The ICO's Code of Practice on Data Sharing notes that the DPA is open as to how, or whether, individuals are provided with a privacy notice but recommends that organisations tell individuals who they are, why they are going to share their personal data, and with whom.

The Home Office's Data Sharing for the Prevention of Fraud Code of Practice recommends that public authorities should, so far as is practicable, ensure that privacy notices are actively provided, or at least made readily available, to individuals.

We recognise that public authorities and SAFOs have legitimate concerns about alerting suspected fraudsters in specific cases but this should not prevent public authorities and SAFOs from being transparent about data sharing in more general terms.

Data standards

The DPA requires that personal data is accurate and, where necessary, kept up-to-date.

SAFOs require that members and other data sharing partners provide personal data in line with agreed data quality requirements, which are determined by the design of the anti-fraud databases hosted by the SAFOs and/or set out in membership conditions or data sharing agreements Two out of nine public authorities indicated they do not check data quality prior to disclosure.

Good practice

ICO's Code of Practice recommends that organisations check from time to time whether the information being shared is of good quality; and, that organisations take steps to check the accuracy of personal data before it is shared, and that procedures are in place for amending data after it has been shared.

The Home Office's Code of Practice recommends that public authorities correct inaccuracies in their records where these are identified, and that any SAFO to whom data has been disclosed should be notified so they can correct their own records; and, that public authorities periodically assure the quality of data that could be shared.

The DPA requires that personal data shall not be kept for longer than is necessary.

SAFOs keep personal data in line with agreed retention requirements to ensure that personal data is not kept for longer than is necessary for the purposes of fraud prevention. One out of nine public authorities indicated they have not agreed retention periods with SAFOs.

Good practice

The ICO's Code of Practice recommends that if personal data is no longer needed for the purpose it was shared, then all organisations with whom it was shared should delete it.

The Home Office's Code of Practice states that public authorities and SAFOs should agree a maximum period of time for which information shared under their arrangements can be held.

Individuals' rights

The DPA requires that personal data is processed in accordance with the rights of individuals, which includes the right to access personal data.

SAFOs have processes in place to recognise and respond to subject access requests in line with the requirements of the DPA, and all public authorities indicate they have a process in place to manage requests.

Good practice

The ICO's Code of Practice provides advice and guidance to organisations sharing personal data on how to manage subject access requests in compliance with DPA.

The Home Office's Code of Practice states that public authorities must ensure that there are members of staff who are nominated to handle subject access requests, enquiries and complaints from individuals.

Security

The DPA requires that appropriate technical and organisational measures are taken to ensure the security of personal data.

SAFOs have appropriate technical and organisational measures in place to ensure the security of personal data. This includes independent reviews of information systems and processes to ensure security measures conform to accepted standards (for example, ISO/IEC 27001). Several SAFOs undertake regular audits of their members to ensure they comply with membership rules, including compliance with the DPA.

One out of nine public authorities indicated they have not agreed secure methods to transfer personal data to SAFOs, and three out of nine public authorities indicated they do not review the security of data sharing arrangements with SAFOs.

Good practice

Both the ICO and Home Office codes of practice provide general advice and guidance on security measures, which should be appropriate to the confidentiality or sensitive nature of the personal data in question. This

includes protecting data in transit from unauthorised access, and monitoring and auditing security arrangements to ensure these are adequate and effective.

Appendix 1: Public authority survey questionnaire

Organisation:	
Name/role:	
Date:	

Objective:	To ensure data sharing arrangements between public authorities and Specified Anti-Fraud Organisations (SAFO) comply with the Data Protection Act 1998 (DPA) and the Information Commissioner Office's (ICO) statutory code of practice on data sharing.

Q1. Do you routinely share personal data with SAFOs for the purposes of fraud prevention?
Yes ☐
No ☐
Comments: *Please list the SAFOs in question.*

Q2. What types of personal data do you share and in what format?
Comments:

Q3. Please indicate the volume and frequency of sharing with SAFOs.
Comments:

Q4. Do you have agreed information sharing agreements in place with SAFOs?
Yes ☐
No ☐
Comments: *Please provide copies.*

Q5. Do you make privacy notices available for individuals whose personal data has or may be shared?
Yes ☐
No ☐
Comments:

Q6. Do you have a process to routinely check the quality (that is, the adequacy and accuracy) of personal data shared with SAFOs?
Yes ☐
No ☐
Comments:

Q7. Where notified, do you have a process to update inaccurate personal data held in your records?
Yes ☐
No ☐
Comments:

Q8. Do you have a process to inform any SAFOs of inaccuracies in shared personal data so they can update their records accordingly?
Yes ☐
No ☐
Comments:

Q9. Have you agreed retention periods to ensure personal data that has or may be shared is held for no longer than is necessary?
Yes ☐
No ☐
Comments:

Q10. Do you have a process to securely discard, delete or otherwise render irretrievable personal data that has or may be shared?
Comments:

Q11. Do you have a process to recognise and respond to individual requests under the DPA to access personal data that has or may be shared?
Yes ☐
No ☐
Comments:

Q12. What physical and logical security measures are in place to ensure access to equipment and systems holding personal data that has or may be shared is controlled and restricted to authorised personnel?
Comments:

Q13. Do you provide data protection training for personnel with access to personal data that has or may be shared?
Yes ☐
No ☐
Comments:

Q14. Do you regularly back-up personal data that may be shared?
Yes ☐
No ☐
Comments:

Q15. Have you agreed secure methods with SAFOs for the transfer of personal data?
Yes ☐
No ☐
Comments:

Q16. Is any personal data transferred outside the European Economic Area?
Yes ☐
No ☐
Comments:

Q17. Do you undertake periodic audits of the security of information sharing

arrangements?
Yes ☐
No ☐
Comments:

Q18. Do you have a process to report and recover from security incidents involving shared personal data?
Yes ☐
No ☐
Comments:

Appendix 2: SAFO survey questionnaire

Organisation:	
Name/role:	
Date:	

Objective:	To ensure data sharing arrangements between public authorities and Specified Anti-Fraud Organisations (SAFO) comply with the Data Protection Act 1998 (DPA) and the Information Commissioner Office's (ICO) statutory code of practice on data sharing.

Q1. Do public authorities routinely share personal data with you for the purposes of fraud prevention?
Yes ☐
No ☐
Comments: *Please list the public authorities in question.*

Q2. What types of personal data do public authorities share with you, and in what format?
Comments:

Q3. Do you have agreed information sharing agreements in place with public authorities?
Yes ☐
No ☐
Comments: *Please provide copies.*

Q4. Do you make privacy notices available for individuals whose personal data has or may be shared with you by public authorities?
Yes ☐
No ☐
Comments:

Q5. Where notified, do you have a process to update inaccurate personal data held in your records?
Yes ☐
No ☐
Comments:

Q6. Have you agreed retention periods for shared personal data to ensure it is held for no longer than is necessary?
Yes ☐
No ☐
Comments:

Q7. Do you have a process to securely discard, delete or otherwise render irretrievable shared personal data?
Yes ☐

No ☐
Comments:

Q8. Do you have a process to recognise and respond to individual requests under the DPA to access shared personal data?
Yes ☐
No ☐
Comments:

Q9. What physical and logical security measures are in place to ensure access to equipment and systems holding shared personal data is controlled and restricted to authorised personnel?
Comments:

Q10. Do you provide data protection training for personnel with access to shared personal data?
Yes ☐
No ☐
Comments:

Q11. Do you regularly back-up shared personal data?
Yes ☐
No ☐
Comments:

Q12. Have you agreed secure methods with public authorities for the transfer of personal data?
Yes ☐
No ☐
Comments:

Q13. Is any shared personal data transferred outside the European Economic Area?
Yes ☐
No ☐
Comments:

Q14. Do you undertake periodic audits of the security of information sharing arrangements?
Yes ☐
No ☐
Comments:

Q15. Do you have a process to report and recover from security incidents involving shared personal data?
Yes ☐
No ☐
Comments:

Appendix 3: list of survey participants

Key

Response to survey provided
Response to survey not received
Response to survey indicates data sharing between public authority and SAFO

SAFO

BAE Systems Applied Intelligence Limited*
Callcredit Information Group Limited*
CIFAS**
Dun and Bradstreet Limited*
Equifax Limited*
Experian Limited
Insurance Fraud Bureau**
Insurance Fraud Investigators Group**
N Hunter Limited**
Synectics Solutions Limited*
Telecommunications United Kingdom Fraud Forum Limited

* Specified by Order effective from 21 July 2014
** Site visits arranged

Public authority

Association of Chief Police Officers
Avon and Somerset Police
Big Lottery Fund
Birmingham City Council
British Transport Authority
Caerphilly County Council
National Fraud Intelligence Bureau - City of London Police
Cumbria Police
Department for Work and Pensions
Derbyshire Police
Devon and Cornwall Police
Dorset Police
Financial Conduct Authority
HM Revenue and Customs
Lancashire Police
London Borough of Lambeth
Ministry of Justice
National Crime Agency
Norfolk and Suffolk Police
North Yorkshire Police
Northumbria Police
Police Scotland

Police Service of Northern Ireland
Security Industry Authority
Serious Fraud Office
Shropshire Fire and Rescue Service
South Wales Fire and Rescue Service
South Yorkshire Police
Staffordshire Police
Sussex Police
Swansea City and County Council
Thames Valley Police
West Mercia Police*

* Completed survey screened out as file could not be read

Appendix 4: summary of public authority survey responses

The following provides a summary of responses to closed questions, which were captured between June and October 2014.

Public authority survey response	
Total sampling frame	33
Total returns	22
Response rate	64%
*Rejected or screened surveys	13
Final sample	9

*Responses that indicate the public authority does not share data with SAFOs for the purposes of fraud prevention have been screened

Q4. Do you have agreed information sharing agreements in place with SAFOs?	
Yes	6
No	3
Q5. Do you make privacy notices available for individuals whose personal data has or may be shared?	
Yes	7
No	2
Q6. Do you have a process to routinely check the quality (that is, the adequacy and accuracy) of personal data shared with SAFOs?	
Yes	7
No	2
Q7. Where notified, do you have a process to update inaccurate personal data held in your records?	
Yes	9
No	0
Q8. Do you have a process to inform any SAFOs of inaccuracies in shared personal data so they can update their records accordingly?	
Yes	6
No	3
Q9. Have you agreed retention periods to ensure personal data that has or may be shared is held for no longer than is necessary?	
Yes	8
No	1
Q11. Do you have a process to recognise and respond to individual requests under the DPA to access personal data that has or may be shared?	
Yes	9

No	0
Q13. Do you provide data protection training for personnel with access to personal data that has or may be shared?	
Yes	9
No	0
Q14. Do you regularly back-up personal data that may be shared?	
Yes	9
No	0
Q15. Have you agreed secure methods with SAFOs for the transfer of personal data?	
Yes	8
No	1
Q16. Is any personal data transferred outside the European Economic Area?	
Yes	2
No	7
Q17. Do you undertake periodic audits of the security of information sharing arrangements?	
Yes	7
No	2
Q18. Do you have a process to report and recover from security incidents involving shared personal data?	
Yes	9
No	0

Appendix 5: summary of SAFO survey responses

The following provide a summary of responses to closed questions, which were captured between June and October 2014.

SAFO survey response	
Total sampling frame	11
Total returns	10
Response rate	91%
*Rejected or screened surveys	5
Final sample	5

*Responses that indicate the SAFO does not receive data from public authorities for the purposes of fraud prevention have been screened

Q3. Do you have agreed information sharing agreements in place with public authorities?	
Yes	5
No	0
Q4. Do you make privacy notices available for individuals whose personal data has or may be shared with you by public authorities?	
Yes	5
No	0
Q5. Where notified, do you have a process to update inaccurate personal data held in your records?	
Yes	5
No	0
Q6. Have you agreed retention periods for shared personal data to ensure it is held for no longer than is necessary?	
Yes	5
No	0
Q7. Do you have a process to securely discard, delete or otherwise render irretrievable shared personal data?	
Yes	5
No	0
Q8. Do you have a process to recognise and respond to individual requests under the DPA to access shared personal data?	
Yes	5
No	0
Q10. Do you provide data protection training for personnel with access to shared personal data?	

Yes	5
No	0
Q11. Do you regularly back-up shared personal data?	
Yes	5
No	0
Q12. Have you agreed secure methods with public authorities for the transfer of personal data?	
Yes	5
No	0
Q13. Is any shared personal data transferred outside the European Economic Area?	
Yes	3
No	2
Q14. Do you undertake periodic audits of the security of information sharing arrangements?	
Yes	5
No	0
Q15. Do you have a process to report and recover from security incidents involving shared personal data?	
Yes	5
No	0