

Data Sharing Review

Richard Thomas and Dr Mark Walport

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.

Comments: CIFAS is the UK's Fraud Prevention Service with 270 Members spread across banking, credit cards, asset finance, retail credit, mail order, insurance, savings and investments, telecommunications, factoring and share dealing.

Members of CIFAS share information about identified frauds in the fight to prevent further fraud.

CIFAS also offers its Protective Registration Service to protect the name and address of individuals who are at particular risk of identity fraud.

CIFAS Members are currently private sector organisations. It is hoped that, when the relevant clauses of the Serious Crime Act are brought into force, public sector organisations may also choose to become Members.

CIFAS has always worked closely with the ICO to ensure compliance with the letter and spirit of the DPA.

What kinds of personal information does CIFAS collect, hold and share?

CIFAS collects personal data relating to fraud cases. This includes names and

addresses supplied by fraudsters when applying fraudulently for financial services or other services or facilities.

How does CIFAS collect, hold and share such personal information? CIFAS Members collect the data, in accordance with a set of standards. Compliance with the standards is audited annually. The data is held securely on the CIFAS database. Access is carefully controlled by means of digital certificate and other security measures. Only suitably trained and authorised users may access the database.

For what purposes does CIFAS collect, hold and share such personal information? For fraud prevention purposes.

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

Question 2.

Comments: In answering this question, CIFAS will confine its answer to the sharing of personal data for fraud prevention purposes.

The key benefits to individuals and society as a whole of CIFAS sharing personal information for fraud prevention are threefold. First, the Protective Registration Service helps to protect those who are at particular risk of identity fraud, and who wish to protect themselves from further incidences. Second, the more fraud that is prevented, the better for individuals (as well as organisations and society as a whole) as, ultimately, it is the genuine customer who foots the bill for fraud. Third, fraud prevention is essential to the integrity of the UK's banking system, which itself is the largest component of the UK economy. During 2007, CIFAS Members have reported savings of nearly £1 billion by sharing fraud data through CIFAS.

Question 3.

Comments: Taking a wider view in responding to this question, CIFAS views the key risks to individuals and society of sharing personal information include:

- the possibility of the kind of mass data breaches which have recently claimed the headlines, making those whose data is lost particularly vulnerable to identity fraud.
- the possibility of incorrect information about an individual causing damage to that individual.
- surveillance 'creep' .
- inadequate safeguards and controls, and inappropriate access to sensitive data that, in the wrong hands, could be damaging.

Question 4.

Comments: The methods that pose the greatest risks include: cold calling; canvassing in the street; surveys about shopping habits; the sale of lists; personal data being held overseas where the regime is less rigorous and the sanctions less severe; collecting more data than is actually needed; fair processing notices that have insufficient detail; and cross matching entire databases when only a limited

number of fields would have been necessary to fulfil the purpose of the cross matching

Opportunities include: bringing together tax and benefits data to ensure that those on low incomes are awarded the benefits to which they are entitled, especially the elderly who are reluctant to claim. In addition, pilots have demonstrated beyond doubt the financial benefits that would accrue from the reciprocal sharing of public sector and private sector fraud data to combat fraud.

Please also see our answer to Question 14.

Question 5.

Comments: The holding of personal data by public authorities should be limited to that necessary to undertake the public function concerned. What is critical, however, is the security of that data, the way in which it is accessed by staff (which should also be done securely), and the way it is transmitted between departments, for example, for the National Fraud Initiative.

CIFAS notes from slide 21 of an Audit Commission presentation - see http://www.wao.gov.uk/assets/englishdocuments/NFI_200607_trainingnorth.ppt - that the National Fraud Initiative lists under "future developments/current restrictions" (i) payroll information from the private sector and (ii) bank and building society mortgage information. While the National Fraud Initiative has achieved excellent results, it would be interesting to know more about the plans to extend it to include private sector information. If this extension does take place, it will be essential for such public/private sector data sharing to be reciprocal and for Fair Processing Notices to make clear to the data subjects that this is an intended use of their data.

Question 6.

Comments: Examples of situations where private sector organisations hold too much personal information are Internet shopping, where there are mandatory fields for personal data that are not relevant to the purchase being made, or where an individual is required to set up an account (with full personal details, including bank details) even for a one-off purchase.

Question 7.

Comments: Public/private sector data sharing for fraud prevention. Progress towards this has been helped by the Serious Crime Act (which removed the legal barriers). CIFAS is keen to make this a reality and will be applying to the Home Office to become a specified anti-fraud organisation when the appropriate framework is in place. The potential savings to the public purse are considerable, not least because those who commit fraud against the private sector also defraud the public sector and vice versa. The only other barriers that remain are cultural and institutional, and these will resolve themselves over time.

Please also see our answer to Question 14.

Question 8.

Comments: N/A

Section 3: The legal framework

Question 9.

Comments: CIFAS considers that the DPA works well, in general, and that its implementation has been assisted by the various guidance leaflets produced by the ICO. The main problem tends to be with the way in which the DPA is perceived or misunderstood, for example when it inhibits data sharing because of the way that individual organisations "hide behind it" to use it as an excuse not to share data, when in fact such data sharing would be perfectly legitimate. The most obvious example of this was the elderly couple who died of hypothermia because the gas company did not feel they could share data with any of the authorities who might have helped them. CIFAS is aware that the ICO took action to rectify such instances but, in CIFAS' experience, too many organisations still use the DPA as an excuse to be obstructive (for example, organisations whose deliberate policy is to blame the DPA in order not to resource certain activities or requests). CIFAS is also aware that some organisations are genuinely confused about the DPA and fearful of breaking the law, and in such cases decline to do something entirely permissible under the Act rather than take guidance (or take what they perceive to be a risk). Education and encouragement to use the helpline both have a role to play.

Question 10.

Comments: It is CIFAS' firm view that the second principle of the DPA is fundamental to the Act. Without it, the 'surveillance creep' would be far worse than it is already.

Question 11.

Comments: Please see our answer to question 9. In addition, the legal definition of filing systems changed as a result of the Durant case so that, where it was once usual for individuals to receive copies of papers from paper files (for example in answer to a subject access request), some organisations now file them in such a way that they are not obliged to disclose them. CIFAS therefore suggests that the ICO could do more to enable individuals to obtain copies of paper documents. CIFAS also recommends that it should be possible for an individual, where he or she knows that a particular document exists that contains personal data about him or her, to ask for that specific document, rather than repeatedly having to make a subject access request, and thereby requiring an organisation to send perhaps a whole sheaf or box of documents, where one sheet would have sufficed.

Question 12.

Comments: CIFAS has a great deal of experience of the use of Fair Processing Notices by our Members, and we see very clearly the difficulties that they face when changes are required to FPNs. For example, it can be very challenging for them to secure an internal commitment, proper priority, and the resources necessary to change an FPN across a large organisation's suite of documents. CIFAS would suggest as a further sanction the introduction of automatic civil fines for persistent Fair Processing Notice or other DPA failures. This would help to secure the priority that such changes require.

CIFAS welcomes the inclusion in the Criminal Justice and Immigration Bill of a new penalty for unlawfully obtaining personal data.

Question 13.

Comments: The different interpretation of the EC Directive by Member States impacts negatively on data sharing for fraud prevention purposes across the EEA. There are moves towards a single market, but not in data protection. Each Member State would have to be approached individually to enable organisations to share fraud information across their borders - and some Member States do not allow the private sector to process fraud related data even within their borders. The fraudster knows no geographical boundaries, so a vital fraud prevention tool is not available to society.

Please also see our response to Question 26.

Question 14.

Comments: Once the relevant clauses of the Serious Crime Act are implemented, it will be possible for public authorities to share data for crime prevention purposes with the private sector. This reciprocity will have proven benefits for both parties. In addition, CIFAS considers that, to help the public and private sectors combat identity fraud and other types of fraud, there should be online access - for verification purposes only - to passport records, DVLA records, NHS numbers, National Insurance numbers and bank account numbers. This online access would obviously require appropriate strict controls, both over organisations entitled to access and over individual users, and would be purely for fraud prevention.

Question 15.

Comments: When responding to subject access requests, where the amount of documentation that needs to be sent out may be considerable, the statutory fee of £10 does not cover postage costs (or, indeed, courier costs where normal post might not be advisable for security reasons).

Section 4: Consent and transparency

Question 16.

Comments: Because of the nature of CIFAS' business, we have worked closely with the ICO to ensure compliance in these respects. For other businesses, however, who deal only rarely with the ICO, the situation may be less clear. The ICO help lines should help to ensure that such organisations have easy access to advice, provided that the organisations are aware of when and how to contact them. Public bodies are particularly bad at explaining why certain personal data is required and how the information will be used. Examples are the DWP's benefit claim forms and the Royal Mail re-direction forms. Micro-businesses (and particularly new businesses) should be particular target audiences for the ICO, and continued dialogue with relevant trade associations will help to achieve increased awareness.

Question 17.

Comments: Data sharing for fraud prevention would be totally undermined if a requirement were to be introduced that required explicit consent by each individual to sharing information about him/her (rather than reliance on a transparent FPN,

for example). A fraudster would refuse to give explicit consent to the sharing of whatever personal data he provided on an application form (whether they were his own, or whether they were the data of whomever he was impersonating) .

Question 18.

Comments: It is the firm view of CIFAS that the current arrangements are sufficiently transparent and that no strengthened access rights are necessary other than those outlined in our answer to question 11.

Question 19.

Comments: CIFAS suggests that this can best be achieved by continuing to consult on changes and developments. Additional transparency could be achieved by emailing details of any new consultation to all of those who have responded to consultations in the past, and also to sending hard copies where costs permit.

CIFAS supports the production of documents such as the Framework Code of Practice for Sharing Personal Information, as it is helpful to have such documents for reference purposes, especially for those who are not familiar with the legislation.

Section 5: Technology

Question 20.

Comments: Technological advances have made the sharing of personal data easier and cheaper, but at the same time have increased the ability to protect data. Example protections include the use of digital certificates to access internet based databases and whole disk/filesystem level encryption.

Unfortunately, in some cases (e.g. in some call centres) personal data on databases can be accessible to all staff in the call centre. There are obvious dangers when personal data is too accessible, and guidelines to cover such circumstances would be helpful.

Question 21.

Comments: CIFAS can see strong arguments for a legal requirement to encrypt personal information held on portable devices to a particular standard. However, such requirements should be flexible enough to reflect the rapidly changing nature of computer security best practice, particularly with regard to the comparatively slower pace of legislative change.

Question 22.

Comments: N/A

Section 6: International comparisons

Question 23.

Comments: N/A

Question 24.

Comments: CIFAS is viewed by other countries as setting the international standard for fraud prevention data sharing.

Question 25.

Comments: N/A

Question 26.

Comments: CIFAS participates in the pan-European Fraud Prevention Expert Group (FPEG) and, in answer to this question, would draw attention to the two following extracts from the Group's draft 2007 Report on Identity Fraud:

“National data protection legislations seem to differ significantly from country to country, leading to different access levels to verifiable data in relation to identities. This makes it almost impossible for a financial institution to conduct a consistent prevention policy across Europe. In addition to the segmentation effect, another problem relates to the types of personal data that can be processed without infringing the law. There is no potential for the financial institutions to keep data on suspected identities or individuals, further than the (limited) possibilities offered by the anti money laundering legislation.”

“Some stakeholders claim that in some EU countries the balance in favour of personal data protection is undermining attempts to combat identity abuses [identity fraud].”

Please also see our response to Question 13.

Section 7: Additional questions

Question 27.

Comments: N/A

Question 28.

Comments: N/A