

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.

The ABI represents the interests of its members on data protection issues. The ABI has a standing Data Protection Panel whose objective is to seek proportionate UK and EU regulatory regimes that do not hinder insurers' innovation and anti-fraud initiatives, whilst safeguarding customers' right to privacy. The Panel's remit is:

- To address insurance-specific privacy and freedom of information issues of practical importance for ABI members, including the preparation of industry guidance, the promotion of effective information sharing and the preparation of responses to consultations;
- To promote an effective dialogue with the UK Information Commissioners, the FSA, the Ministry of Justice and the Home Office;
- To engage actively with the CEA (the pan-European insurance trade association) informing its responses to EU data protection matters, including those initiated by the European Commission's Article 29 Working Party.

The ABI has a number of other Committees that have an interest in information sharing. The Financial Crime Committee and the GI Anti-Fraud Committee, for example, implement

strategies for reducing the impact of financial crime and the incidence of fraud on insurers' businesses.

Our members will hold personal data pertaining to employees (for HR purposes) and customers in relation to the provision of a wide range of products in the market place. Customer data will be personal (for example, to process simple insurance contracts) and sensitive (for example, medical data to assess underwriting requirements or pay claims in relation to health and protection insurance). Data will also be held on third parties, for example, third party claimants and witnesses in road traffic accidents.

Customer data will be collected by a variety of means. This may be by paper, electronically and electronically but distributed manually. Both paper-based and electronic data may be held on-site and off-site (for example, electronic data may be held by service providers who arrange medicals).

Data might be shared with other insurers (and the police) for fraud prevention purposes (often via databases such as the Claims & Underwriting Exchange); joint data controllers (e.g. business partners such as IFAs; reinsurers); data processors for outsourced functions (service providers); and government departments to satisfy statutory obligations (for example, tax data sent to HM Revenue and Customs [HMRC]).

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

Question 2.

(a) The benefits of sharing information with individuals include:

- protecting genuine customers and their assets and discovering identity theft;
- improving fraud prevention capability by helping to identify known fraudsters;

Where information relating to policyholders and others is shared amongst insurers, this can make the application and claims processes more streamlined for customers (e.g. where information relating to claims history is provided by a previous insurer).

(b) There do not appear to be any obvious benefits from sharing personal information with society at large, though information shared under the Freedom of Information Act (FOIA) can help engender transparency, openness and trust.

The sharing of information (on fraudulent applications and claims) with relevant Government agencies provides more effective tools to combat fraud and can facilitate a swift response to organised crime. But information sharing is largely one-way (i.e. from industry to Government) and would benefit from a more reciprocal approach.

Question 3.

- (a) The key risk is that data could be lost or stolen and subsequently used inappropriately (whether accidentally, opportunistically or via targeted organised crime), for example, to steal someone's identity.

There are also problems caused by data mismatch on insurers' customer databases e.g. where the details of two similar sounding customers become confused. Information (including mailshots) is then sent in error to the wrong person. This might also occur where a customer has failed to pass on new details, such as change of address. These events can ultimately lead to a loss of customer confidence in a firm or sector.

- (b) We see no merit in sharing personal information with society – this would merely create the notion of the emergence of a 'nanny' state. The risks associated with information disclosed under the FOIA include information being put in the public domain that should be regarded as commercially sensitive and/or confidential. This could, for example, undermine the degree of openness and trust between private bodies and public bodies (subject to the FOIA) to whom information is provided. In other words, private bodies might be reticent to provide certain information if they thought it might be published.

Question 4.

A key benefit of sharing personal information is that it helps to prevent fraud, making the UK a less attractive target for opportunistic fraudsters and organised criminals. This helps to ensure that policyholders do not have to subsidise fraud by paying a certain percentage of their premiums to offset fraud costs.

The greatest opportunities are perhaps presented by technological advances, including the internet, which are seen as efficient and user-friendly means of communication.

Significant risks (including identity theft) are presented by sharing personal information where there are insufficient security measures in place.

Question 5.

Comments: None.

Question 6.

Some of our members are of the opinion that – in order to ensure compliance with the data protection principles - insurers are not permitted to hold enough personal data relating to policyholders. This puts them at a disadvantage vis-à-vis organised criminals who do not of course respect the Act and use a variety of means to obtain data by deception.

Some simple insurance products do not require very much data relating to the policyholder. However, this means that the insurer has little information on which to conduct identification verification checks against people claiming to be the policyholder. This can expose the insurer to fraud.

The insurer has to consider the length of time that it might need to hold customer data. Some customers might take the view that data is held for too long. But, for evidential purposes, in line with the Limitation Act 1980, it is prudent to hold data for 6 years following the cancellation of the policy or repudiation of the claim.

One area where it is important for insurers to get the balance right is in relation to the use of private investigators (PIs), for example, to check whether or not a claim is genuine. Insurance fraud is a problem that costs the industry's customers around £1.6 billion a year. In July 2007, the ABI published guidelines on the instruction and use of private investigators (PIs) and tracing agents. This aims to ensure that a PI is only employed where there is reasonable suspicion that the claim might be fraudulent and the information a PI can obtain is necessary to dispute it.

Question 7.

Police road traffic collision reports

The police are required to attend road collisions where a person has been killed or injured, the road is obstructed, or there are allegations of offences. The attending police officer will record information about the collision – including driver, vehicle and victim details, the circumstances of the collision, and the contact details of any witnesses.

Police road traffic collision (RTC) reports are a vital tool in helping motor insurers reach a decision where liability is in doubt, and therefore play a crucial role in resolving difficult claims as quickly as possible. Insurers want to pay timely compensation to claimants; this is in line with the Ministry of Justice's own commitment to making the personal injury claims process more efficient and cost effective to the benefit of claimants.

In the past, RTC reports were made available to insurers at a standard price, dispatched fairly promptly, and generally contained all the required material. Unfortunately, that is no longer the case. Today, vital information is often redacted. Data protection and human rights concerns are behind police refusals to supply full information. These concerns are we believe misplaced and should not override the broader interest of promoting access to justice.

We believe that a sensible way forward would be to develop a Memorandum of Understanding (MoU), setting out appropriate timeframes, content and pricing for RTC reports. We began developing a MoU in 2005; but unfortunately discussions with the Association of Chief Police Officers stalled and no progress has been made since.

It may be that some guidance from the Information Commissioner on this will enable those discussions to reach a satisfactory conclusion.

Notification of No Claims Bonus (NCB)

At present, the disclosure of NCBs by one insurer to another is only permissible where the consent of the customer has been obtained. This is unwieldy and should be reviewed.

Motor Insurance Database (MID)

The MID, which is overseen by the Motor Insurers' Information Centre (MIIC), is used primarily to identify uninsured drivers. It has been suggested that it has the capability to perform additional functions, such as advising motor service providers in real time whether replacement windscreen cover exists.

Question 8.

We suggest that one area that might be worth exploring is the responsibilities of joint data controllers. For example, an insurer might be a joint data controller with an independent financial adviser (IFA). In practice, this means that the IFA can request a download of a policy and other personal data held on their clients. There should be more onus on each data controller to maintain their own personal data store and not rely on the other data controller to provide the information. While it obviously makes sense for the other data controller to be informed when common data changes are made, we believe that some joint data controllers are under the impression that it is the responsibility of the other to maintain both sets of data. This can prove administratively burdensome for insurers.

Section 3: The legal framework

Question 9.

The main strength of the Act is perhaps the heightened profile that data protection issues have received of late, albeit in unfortunate circumstances following the media splash created by several losses of data by government departments and agencies.

But the Act is not always 'black and white'. It is often not clear how a firm should act in response to a given scenario (e.g. sharing data regarding a third party insurance claimant suspected of fraud when they have not been issued with a fair processing notice [FPN]). We fully acknowledge that it is not always appropriate to prescribe rules – this can hinder a firm's ability to achieve the best outcome for its customers. But more guidance from the ICO would be useful.

A key weakness of the DPA is the inadequacy of sanctions available to the Information Commissioner when the Act is breached (see our comments in response to Q 12). There is little incentive for the data controller to proactively seek to comply with the Act. So it often falls to a firm's data protection officer (DPO) to emphasise the importance of compliance – from a reputational, as well as a strictly legal, standpoint – in order to create the right culture within the firm and, consequently, a robust compliance policy.

Having said that, it is important that the ICO takes a proportionate approach to enforcement. It should focus on systemic issues, for example, persistent security breaches rather than one-off breakdowns concerning, say, marketing activity. We welcome the approach outlined in the ICO's proposed data protection strategy consultation (see our comments in response to Q 11).

Turning to definitions, the ICO has still not clarified the question of what amounts to 'personal data'. There is still some confusion regarding the definition, particularly in relation to subject access rights. The ICO often regards data as 'personal data' even when it does not identify the subject (this is on the basis that it is possible to match the data with other data to identify a living individual – even though there is no intention on the part of the controller to do so). By way of example, telematics data can identify the location of a device at a given time (e.g. a black box in a vehicle). But this does not prove that a particular individual was driving the vehicle at a particular time. Therefore, we consider that such data should not be deemed to be 'personal data', although the indications from the ICO are to the contrary.

In terms of changes to the DPA, we have the following suggestions:

Investigation of fraud: Data controllers need to exercise a great deal of care to ensure that their fraud prevention initiatives do not conflict with the general requirement to be open and transparent when processing personal information. Under Section 29 DPA, data processed for the purposes of the prevention or detection of fraud may be exempt from the First Principle (fair obtaining and lawful processing). Section 29(3) exempts such data from disclosure, if the investigation is likely to be prejudiced. But section 29 is applied on a case by case basis e.g. when the data controller is contemplating legal action against an alleged offender, and where it would be detrimental to that particular legal action if the normal rules of transparency were to apply.

We believe that the ability of organisations to detect and prevent fraud would be enhanced if the section 29(3) exemption were to be applied more broadly, for example, to allow the interrogation of databases to identify and trace patterns for organised crime.

Subject access requests: The fee should be proportionate to the actual costs incurred by the data controller (see Question 15).

Sub-contractors: Organisations should be allowed to sub-contract without a requirement to have to notify data subjects, as long as data protection requirements are addressed adequately in the contract between the organisation and the sub-contractor.

Question 10.

Our members effect various measures to ensure compliance with the second principle. These include conducting periodical inventories of data and regular checks that the firm's notification remains accurate.

But whilst firms will comply, there is some unease that the principle does not sit comfortably with traditional business practice. It can be very restrictive – business objectives change and a matter that may have been irrelevant at the start of the relationship may become relevant later (e.g. marketing). If the 'new' purpose is reasonable, then the firm should be able to continue with it.

Question 11.

It can be very costly for firms to amend old systems to ensure they are DP compliant. New technologies, such as the upsurge in email activity, also present challenges to firms in developing security solutions. More widely, firms are under increasing pressure from shareholders to lower operating costs, so businesses need to look for the most cost-effective ways of achieving their objectives.

There is some frustration amongst insurers at the disproportionate amount of time spent on handling individual complaints – in many cases, there has been no actual harm to the individual. It would be in the public interest for firms to spend more time on matters aimed at reducing the risk to many, by improving privacy and security measures.

So we welcome the ICO's intention to adopt a risk-based approach going forward, focusing its priorities on areas where there is a real danger of serious harm to the individual or society at large. We particularly welcome the intention to take a practical down-to-earth approach, making things easier for compliant firms, and tougher for those who don't comply. This approach is in line with good regulatory practice. It is also in line with the approach of our members.

Public understanding of actual and perceived risks of data loss or misuse often appear to drive the political (and media) agenda. The ICO states that it must work with the media to deliver clear and consistent messages about the purposes and benefits of data protection. We would add that the ICO should be fair – and seen to be fair – in its dealings with the media. We suggest that sensationalist headlines are more likely to scaremonger and undermine public confidence in data protection, rather than underpin it.

Question 12.

The ICO requires more teeth. So we support recent moves by the ICO to have custodial sanctions introduced to deter the wilful and deliberate misuse of data; increased powers to conduct mandatory audits; to require breach reporting; and security declaration in report and accounts. The level of fines currently administered by the ICO is very low when compared to, say, the Financial Services Authority.

There would also be merit in exploring whether there should be a requirement for firms (falling within defined parameters) to have a Data Protection Officer, as occurs within some other EU states.

Question 13.

We believe that the Privacy and Electronic Communications Regulations interact well with the DPA.

We consider that the ICO and the FSA may have different approaches to the sharing of information for fraud prevention purposes. Whereas the FSA has a statutory objective of reducing financial crime, the ICO is concerned primarily with the protection of privacy. This can create confusion and conflicting obligations for financial services providers.

Question 14.

- (a) More cross-referencing between public authorities to detect suspicious activity would improve effectiveness of fraud detection.
- (b) Financial services firms should have an easier means for verifying that someone making a request for information is actually from the police, HMRC etc. The ability to verify identity documents electronically with public authorities would also help to reduce identity fraud. Further, financial services firms creating direct debits should have the ability to verify the name of the individual with the holding bank.

Question 15.

Subject Access Requests

The public has an expectation that all data connected to their relationship with a data controller is personal data and should be supplied to them. We believe the ICO should do more via the media to manage the expectations of the public so that they are made aware that there are limitations on the release of data under the subject access request (SAR) provisions.

Further, the Act does not provide the ICO with any teeth to prevent individuals from causing significant nuisance through the SAR process. Our members are seeing an increasing trend of the SAR route being used to cause significant disruption and cost to firms where the individual has no real desire to be provided with 'all' personal data. This might, for example, involve requesting details of every recorded phone call (which may cover numerous hours of conversations over several years) when the real issue is, say, a disagreement over the current insurance claim and the amount to be paid. It should be acceptable for the firm to supply only data that is relevant in the circumstances.

The SAR fee is often out-of-kilter with the actual costs incurred. The fee should be increased so that it is more proportional to the actual costs incurred. This might, for example, be a flat fee per A4 sheet of paper and a fee for recorded telephone conversations and CCTV based on the length of the recording.

Handling of sensitive data

It is burdensome and very costly for our members to have to write to a large number of individuals, for example, to seek consent to use data for a new purpose where a Schedule 3 condition cannot be readily relied upon. The firm will often implement new practices to capture responses to the request for consent, only to then find that no responses are forthcoming. It would be helpful if firms could, instead, seek the prior agreement of the ICO to undertake the new initiative.

Similarly, where a firm has a proposal approved by the FSA and there is no consumer detriment involved, this should be acceptable to the ICO.

Example

An insurer set up a new legal entity. This involved the transfer of personal data – which had been approved by the FSA. While customers had been informed of the new arrangements, they had not been asked to provide their explicit consent, as this was not practicable (and would have involved policies having to be cancelled and re-issued). However, the ICO upheld a complaint and prevented the firm from relying on the Schedule 3 condition. But, in effect, the transfer was really just a change of name as everything else stayed the same (e.g. data was handled by the same staff). The customer did not suffer any harm (and chose not to cancel the policy).

Consideration should be given to the introduction of a further Schedule 3 condition (similar to Schedule 2) along the lines of 'where it is in the interests of the data subject'. Alternatively, a wider interpretation of the 'vital interests' condition should be considered.

Notifications

It would be very helpful if notification was permitted at Group level, rather than for every legal entity – this would then simplify transfers of data between firms within the same group. We suggest that this matter is addressed when the ICO reviews the notification process.

DP status of data subjects

There should be a distinction drawn between dealings with individuals in their private and professional capacities. This would enable the firm to determine whether it is dealing with a private individual or an employee.

The ICO should also consider whether to discard the view that sole traders and partnerships are to be treated as individuals under the Act.

Section 4: Consent and transparency

Question 16.

Much data processing performed by insurers is based on consent. But it can be difficult to balance the need to provide good customer service with data protection obligations. By way of example, insurers will receive requests for details of the insured from, say, the driver of the other car in an RTA or from individuals wanting to act on behalf of an elderly relative. The refusal of the insurer to disclose such details can cause ill feeling and gives the DPA a bad name. In some circumstances, it seems unreasonable to deny people - the ICO should provide firms with more latitude to assess a situation on its merits and respond accordingly. It should be possible, for example, to consider the rights of two or more individuals in tandem, as it may be unreasonable that one person may use the Act to block a legitimate request made by another.

It can sometimes be difficult for an insurer to obtain informed consent. For example, a customer may request details of the consent communication by email, without realising the risk of interception.

It is not always clear when data can be shared in the claims environment, for example, the sharing of data relating to a third party (both internally within a group and externally via a database) who has not been provided with a FPN (see Q 9).

An example of an initiative within the insurance that is based on consent is the provision of medical information relating to a policyholder by a General Practitioner to an insurer.

Question 17.

Often difficulties will be encountered after the relationship has started and the firm seeks to make purpose and/or processing changes - for example, move a business to another data controller, use different anti-fraud databases and market to new customers.

Firms will often have millions of customers and it is very costly to write to each individual customer. Moreover, many will simply not respond, leaving the firm to decide how they will deal with customers who have failed to provide further consent. We recommend that the ICO makes it clear that data controllers are able to rely on implied consent (including in respect of the processing of sensitive data). In other words, the firm may inform the customer of the new processing giving them the opportunity to contact the firm should they wish to object.

Question 18.

The sharing of information could be made more transparent by more widespread use of layered privacy notices. But despite a lot of initial noise about the introduction of such notices, we have not seen much come out from the ICO. Our members would welcome guidance from the ICO.

ICO research (January 2007) found that while people care about what happens to their data, they pay little attention to FPNs and learn little from them. But they would pay more attention to better designed FPNs. This must strike the right balance between enough detail and information overload.

We do not think that subject access rights should be strengthened. As is borne out in our responses to previous questions, we believe that the balance of access rights is currently tipped in favour of the data subject.

Question 19.

We believe that the Framework Code is likely to be most appropriate for public authorities. Within the insurance sector, it is probably of most relevance for information sharing in order to combat fraud or to assess risk for underwriting purposes. The ICO should, however, recognise the costs associated with IT changes, particularly in relation to legacy systems. The Code might also be used by insurers as a checklist to evaluate current procedures in order to assess whether they remain good practice.

We note that the ICO plans further work and acknowledges demand for practical examples and templates. We suggest practical examples highlighting the circumstances in which consent may be withdrawn would aid transparency.

Section 5: Technology

Question 20.

Technological advances facilitate greater data sharing possibilities. But they also pose a greater exposure to mass data compromise from one source. While technology has made data sharing and transfer far easier, it appears that security measures have not as yet caught up. For example, spyware (software that can be downloaded from the internet) can log and transmit information without the user's knowledge.

Once data security management matures, and security measures are tightened, the risks will be managed more readily. But this might take between 3-5 years. In the meantime, the risks of data loss are significant (as has been evidenced by the loss of data by HMRC). The huge costs of IT systems means that it can be difficult to fit protective measures retrospectively.

There is a growing trend towards home working and it is now very easy to send an entire database to a home address for downloading. While this is very convenient for the employee, it does enhance the risk of data security breaches and loss (particularly where, say, a wireless internet connection is used).

The trend towards outsourcing processing operations to third world countries has given rise to a perceived risk of low paid workers selling data illegally. There are, however, very good incentives for outsourcing firms to control data loss effectively in order to maintain confidence in their business model.

Question 21.

We can understand why this issue is being raised, given the recent high profile losses/thefts of laptops containing personal information.

But, as technology changes quickly, the danger is that the type of encryption would become outmoded. Moreover, any legislation passed could similarly become outmoded with the result that the law would continually be chasing technology.

We note from the recent ICO communication 'Our approach to encryption' that the Commissioner has formed the view that in future, where losses involving portable devices occur, and where encryption has not been used to protect the data, enforcement action will be taken. Given the likelihood of technology outstripping legislation, this might continue to be the most sensible option going forward.

While the ICO has issued a Good Practice Note on security of personal information, it has been suggested that there should be more specific guidance for firms on what amounts to appropriate security. It would be useful for the ICO to interact with the security functions within firms to agree best practice so that it is clearer what constitutes a security breach; what action should a firm take to notify a breach; and which regulator might take action (e.g. the ICO or the FSA).

Question 22.

We do not think there exists sufficient information or advice about anonymisation. This is an area that the ICO could become more involved in. While this is a useful tool it is costly and it

can take time for the firm to tailor the solution to its specific needs and run it against the firms' databases. It has also been suggested that there is a danger that anonymisation could actually weaken identification controls and undermine fraud prevention capability.

Section 6: International comparisons

Question 23.

No.

Question 24.

No.

Question 25.

Some states have different local requirements for data. (e.g. Luxembourg). Others, including Spain, restrict the export of data unless approved.

Question 26.

No.

Section 7: Additional questions

Question 27.

The review could address the merits of providing information by secure email rather than hard copy (in the post). We suggest that the view of the ICO that plain text email is as vulnerable as information sent by postcard is over-cautious - an email has to be specifically hacked into before it can be read.

Question 28.

We welcome the ICO's commitment – as set out in its data protection strategy – to engage more closely with its stakeholders, including those organisations it regulates and the data protection officers working within those organisations.

We believe that relationships with individual firms would be enhanced if the ICO gave more recognition to the positive aspects of a firm's data protection practices, rather than simply focusing on any problems that come to light.

