Information Commissioner's Office

ICO response to Law Commission:Data Sharing Between Public Bodies consultation.

December 2013

Information Commissioner's Office

Contents

About the ICO

The ICO's mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

The ICO is the UK's independent public authority set up to uphold information rights. We do this by promoting good practice, ruling on complaints providing information to individuals and organisations and taking appropriate action where the law is broken.

The ICO enforces and oversees the Freedom of Information Act, the Environmental Information Regulations, the Data Protection Act and the Privacy and Electronic Communication Regulations.

Introduction

The ICO welcomes the opportunity to take part in the Law Commission's consultation. Data sharing – within the public sector and beyond it – is a major issue for us. We hope that our expertise in this area will help the Law Society to inform its own approach to the development of the legal framework that should surround data sharing.

Clarity and certainty of the law

5.3 The law surrounding data sharing is complex. It has been suggested that complexity and lack of clarity are hindrances to data sharing.

5.4 Question 1: Do you think that the current law on data sharing is sufficiently clear and certain? If not, please explain which parts of the law you find unclear or uncertain, and if possible please give examples of any problems that the lack of clarity or certainty causes.

The current system of data protection law, human rights principles, common law powers and statutory gateways is complex. As your consultation document explains very clearly though, given the origins and nature of our public authorities and their now complex relationship with the private and third sectors, to some extent this is perhaps inevitable. The ICO has issued clear, authoritative guidance on data sharing and has done a great deal to promote our guidance. However we still receive fairly frequent requests for advice from practitioners and policy makers who are clearly confused about what the law does - or does not - allow them to do in terms of sharing personal data. In particular, the relationship between data protection and other elements of the law, such as statutory gateways, seems to be fairly widely mis-understood. Whilst a statutory gateway provides legal certainty when a public authority shares personal data, the data protection principles would allow the sharing anyway, provided it is done in compliance with the data protection principles - and provided that the sharing is necessary for the public authority's or government department's statutory or common law purposes and is not therefore ultra vires. The first data protection principle requires that the processing (e.g. sharing) of personal data be lawful. Given our legal system, this does not mean though that the sharing has to be expressly provided for in law. If this was better understood, then perhaps a more flexible, imaginative and less risk-averse approach to data sharing could be developed – supported, and sometimes limited, by data protection requirements of fairness, transparency, data standards and so forth.

In terms of the general public, we have no doubt that the circumstances in which – and the basis on which – the information they provide to their public authorities can be shared is not well understood. Many members of the public will not be interested in this, provided they receive the services they expect from their public authorities. However, public authorities should try to improve the way they explain their sharing of personal data to citizens. We are

sceptical as to whether longer, more detailed privacy policies are the best way to do inform citizens. We note the accessible, imaginative means some online service providers – in particular – are developing to explain very complex information systems to 'ordinary' citizens. The public sector should learn from this. See, for example, the animations, videos and 'layered notices' that some online service providers and telecoms companies have developed to explain their own use of information to the public.

As part of its work on data sharing, we urge the Law Commission to give particular attention to the relationship between data protection and other elements of the law. In our view the data protection principles have all the necessary features to protect citizens' privacy and to provide a positive framework for organisations to share personal data in a fair and lawful way for a defined purpose or purposes. We understand the relevance of other elements of the law, but perhaps a more prominent place for data protection law would help to simplify the very confusing legal landscape surrounding data sharing. We believe that the current system of establishing 'gateways' for particular data sharing activity is confusing for practitioners. We wonder what the consequences would be if instead of relying on a gateway, data sharing were to take place in a more principle-based way, relying on the tests of fairness, necessity etc. that lie at the heart of data protection law. The ICO is not making a particular recommendation in respect of statutory data-sharing gateways. However, we do hope the Law Commission will consider this issue as part of its work – a more principle based approach might facilitate the imaginative and flexible use of personal data that policy makers would like to see, whilst safeguarding – and indeed strengthening - individuals' information rights. A possible model might be to build on the statutory Data Sharing Code of Practice that the ICO issued in 2011. Although it probably needs updating, and will be reviewed in due course, this could usefully become a central source of authoritative guidance on data sharing. It could also be used as source material for other organisations wishing to produce their own organisation or sector-specific guidance, going into more detail than the ICO's code could do. (Arguably there is too much guidance in circulation and perhaps the corpus of materials available needs to be rationalised and made more coherent.) We can also see the advantage of a revamped statutory code on data sharing – linked to incentives for organisations to follow it – perhaps as part of an accreditation scheme.

Knowledge and application of the law

5.5 Question 2: Do those responsible for data sharing in your organisation have a good understanding of the law? If not, to what do you attribute this?

The ICO is perhaps in an unusual situation here because so much of our corporate expertise centres on understanding the law surrounding data sharing and related issues. However, we do engage in data sharing to carry out our own statutory functions – including investigations for example. We believe that our own good understanding of the data protection principles gives us the knowledge and confidence to share personal data in a way that is fair, reasonable and would be defensible in the face of any legal challenge.

5.6 Question 3: Do you think that those responsible for data sharing are given enough leeway to exercise judgement or, in contrast, that there should not be as much flexibility when it comes to comply with the law?

In our opinion there needs to be both flexibility and a clear understanding of when data sharing is not acceptable. Again, the data protection principles provide a basis for sharing personal data within reasonable parameters. Depending on the type of sharing, there may be a need for professional judgement based on the circumstances of the case. It is unrealistic to expect the system of express data sharing powers and statutory gateways to always be so detailed and comprehensive as to rule out the need for individual decision-making. There needs to a better understanding of what proportionality means in practice.

It might be useful to draw a distinction here between different types of data sharing. Large scale, routine, 'structural' data sharing might best take place on an express statutory basis. Whilst this would enable the sharing, it could also place limits on it – so that only certain data items could be shared between specified bodies for a particular purpose. An example might be disclosures between DWP and local authorities for the purpose of working out housing benefit claims. Here, in reality, there is very little need for individual judgement as the data sharing is routine, the data sets defined and the arrangements for sharing them well-established.

A second form of data sharing can depend more on individual judgement – but exercised within a statutory framework. This might be the case where a local authority is under a general statutory duty to, for example, promote the social well-being of its area. Clearly this is a very wide duty and the data sharing needed to fulfil this aim could take a variety of forms. This means that individual judgement could play a much greater role, depending on the type of sharing. For example, in order to combat teenage alcohol abuse the local authority's parks and leisure department might decide to share certain information about particular children caught drinking in local parks with its child welfare officers – so that health advice and counselling can be targeted at them. Clearly this involves a larger degree of judgement based on the circumstances of the case: which information should be shared about which children? Should the children or their parents be told about the sharing, and so forth? In cases like this principles of fairness, necessity, reasonableness etc. come into play much more than in the first type of data sharing. Although a data sharing agreement can set the rules relating to sharing in cases like this, we very much doubt whether the relevant law could be drafted in such a way as to rule out the need for flexibility and professional judgement. Indeed, in drafting legislation such as the Local Government Act 2000 policy makers seemed to be opening the way for local authorities to be freer to use their judgement and to be more flexible in terms of the way they improve their areas. If this policy approach is to continue then the 'gaps' left by the broad drafting of the relevant law need to be filled by principles that help the relevant professionals to share personal data in a way that is fair, proportionate and reasonable – and hopefully publicly acceptable.

The point is that there are different types of data sharing and in some cases the sharing depends largely or entirely on the exercise of individual judgement, in other cases this plays a minimal role, where detailed rules are set out in statute and in the relevant corporate policies.

We believe that a diversity of approach to data sharing will always be necessary. We should accept this and recognise that a move to put all data sharing on an express legal basis could stifle the innovative use of citizens' personal data. A better establishment of the principles of good practice in data sharing will provide for flexibility whilst protecting citizens against the unnecessary or inappropriate use of their personal data.

Balancing data sharing and the rights of individuals

5.7 Some public bodies may feel that sharing information is too onerous and should be streamlined. However, there are also potential risks of data sharing alongside its benefits.
5.8 Question 4: If you think that there are inappropriate obstacles to data sharing between public bodies, please say what these are and where you have encountered them.

The Law Commission's paper has made a good job of setting out the legal and cultural, actual and perceived, obstacles to data sharing. There have been several attempts – for example by the (former) Department for Constitutional Affairs – to find compelling examples of the law preventing data sharing that would otherwise be reasonable and in the public interest. As far as we are aware there is still very little evidence of this. However, there does still seem to be a fairly widely held belief that data sharing is being prevented by a defect in the law. However, our experience suggests that the problems are generally cultural, based on a misunderstanding of what the law does allow or the result of inter-organisational distrust, budgetary restraints, incompatible IT systems and so forth. If the Law Commission does find genuine examples of a legal obstacle to data sharing then we urge it to carry out a thorough analysis of how the relevant provision came to be in place, whether it is being applied properly and whether a change to the law is necessary or desirable. It could be the case that if there is a legal obstacle to data sharing, there is a good reason for this; it is wrong to assume that data sharing should *always* be allowed. (An interesting case study might be Local Authorities' approaches to the use of information obtained for council tax purposes under the Schedule 2 of the Local Government and Finance Act 1992; there is great divergence of approach here yet clearly all Local Authorities are working to the same piece of legislation.)

One problem area issue is the prohibition on certain public authorities from using personal data in their possession to produce even anonymised data - if the resultant data are not to be used for the authority's own statutory purposes. We believe that this is overly restrictive and – provided the information is anonymised to a satisfactory standard – public authorities should normally be allowed to share and publish anonymised information derived from the personal data they hold. This is an area where there does

seem to be an artificial and unnecessary restriction on the sharing and publication of information.

5.9 Question 5: If you think there should be more checks on data sharing, please say why (and indicate what those checks should be). If possible, please provide examples of sharing that is currently allowed that you think should not be.

Speaking as the regulator for the Data Protection Act 1998, we believe that the proper application of the law does strike the right balance between the ability to share data and the need to protect the privacy of the people the information is about. Where personal data is shared in a way that is unfair, or where the sharing is unnecessary, the ICO would be able to stop this. It is worth noting that the ICO receives relatively few complaints about excessive data sharing – and the ones we do receive tend to be about individual cases rather than systematic data sharing arrangements. (See though our recent blog on information sharing within the police service at: http://www.ico.org.uk/news/blog/2013/police-collaboration-unit-failings-should-act-as-a-warning-to-all)

It is very important for organisations to review their data sharing arrangements periodically. It could well be the case that the justification for data sharing disappears over time – we provide advice about this in our Data Sharing Code of Practice. This also begs the question of whether some statutory gateways, once opened, should eventually be closed. As far as we are aware, cases of primary or secondary data sharing legislation being repealed are few. This suggests that once a gateway has been established it generally remains open.

The ICO's powers of compulsory audit should be extended to cover local government and the NHS. We believe that this would provide more effective regulation of data sharing in these sectors.

5.10 Question 6: Do you think that the current law strikes the right balance between the ability of public bodies to share data and the need to protect privacy or other rights of data subjects? If not, please say why.

It is interesting that data sharing legislation tends to stipulate the datasets that particular organisations can share for particular purposes. It tends not to contain bespoke safeguards for individuals. Rights for the individuals whose data is being shared largely emanate from data protection law – transparency and access rights for example. It would be a good idea for the Law Commission to consider whether major data sharing legislation should always contain specific safeguards for individuals or whether it is sufficient to rely on the safeguards in data protection law. (One of the problems with the data sharing provisions of the Coroners and Justice Act was – we understand – the perceived weakness of the safeguards on the face of the legislation.) Either way, we do think it is important that the 'recipe' for data sharing safeguards –

security, transparency, Privacy Impact Assessments and so forth – is broadly consistent and provides coherent, meaningful safeguards for individuals.

Public attitudes to data sharing

5.11 Public bodies may encounter difficulties when collecting or sharing data about individuals due to the reluctance of individuals to allow their data to be shared. Public bodies themselves may also be reluctant to share data due to a lack of public trust in the ability of public bodies to handle their data.
5.12 Question 7: Does the reluctance of individuals to have their data shared by public bodies have an effect on data sharing? If possible, please provide examples.

Our experience suggests that public attitudes to data sharing are complex, and that individuals are not necessarily reluctant for their data to be shared – particularly where there is an obvious benefit to them. A good example might be the sharing of data between the Passport Office and DVLA, allowing drivers' identities to be verified without the inconvenience of sending sensitive documents through the post – a service that we understand has proved very popular with drivers. Recent research carried out by the Scottish Government seems to suggest that individuals are willing for their data to be shared for altruistic purposes such as medical research but less willing for it to be shared with pharmaceutical companies for private gain, for example. Data breaches will also damage the public's trust in data sharing. Some data sharing, for example between a person's GP and their hospital care team is well-established and accepted by the public. We think it is too simplistic to conclude that individuals are generally reluctant for their data to be shared. Organisations should, though, get better at explaining the risks and benefits of data sharing to individuals, allowing them to make better informed choices. (Of course in much public sector data sharing individuals have no choice over the data sharing so their reluctance – or not – is not so much of an issue.)

We suspect that there is a link between the sensitivity of individuals' personal data and their willingness for it to be shared. There can be a tendency to see all personal data as being sensitive and confidential. It might be worth the Law Society considering how the sensitivity and privacy impact of sharing personal data is evaluated by practitioners and how this is fed into data sharing practice. Whilst we do not think a simple binary sensitive / non-sensitive approach to data sharing is viable, an evaluation of sensitivity can form an important component of a risk-based approach to data sharing.

5.13 Question 8: Do you think that there is a lack of public trust in public bodies which has an effect on data sharing? If so, is this because the public have a poor understanding of data sharing, or are they right to question sharing?

It is very difficult to say, and as far as we are aware no substantive research on public trust in relation to data sharing has been carried out. We do think though that, in general, standards of transparency in relation to data sharing can be improved – although it is wrong to assume that more transparency

necessarily means more trust. It will work best when the transparency is consistent over time and is genuinely meaningful. In terms of the public questioning data sharing, one problem is that it is not always clear how much control individuals do – or should – have over the sharing of their personal data. This is a major issue in data sharing policy. Clearly some sharing will never be voluntary – for example for taxation or policing purposes. In other cases individual control is much more viable – for example data sharing for research purposes. We do suspect that the public are confused as to the degree of control they can exercise over the sharing of their personal data. Organisations should explain to the public as clearly as possible whether the sharing of their personal data is voluntary or mandatory – this is an important element of the 'fairness' requirement of data protection law. We would encourage the Law Commission to give due consideration to extent to which individuals should be able to exercise control over the sharing of their personal data. We suspect that this is a major source of uncertainty amongst policy makers and practitioners.

Availability of powers to share data
5.14 Question 9: Do you think that you, or your organisation, have sufficient powers to share the information you want to share with other organisations? If possible, please provide examples

As far as we are aware we have never encountered any problems in terms of our own power to share data.

5.15 Question 10: Do you think that others, who you think should disclose data to you, have sufficient powers to do so? If possible, please provide examples.

We have never encountered this as a problem, and where necessary we have the power to require organisations to provide information to us – for example as part of an investigation.

Misuse of data

5.16 There have been a number of high profile examples of data loss or the unauthorised disclosure of data.
5.17 Question 11: Do you think that the adverse consequences of unauthorised disclosure, including reputational damage or formal sanctioning, have an adverse effect on data sharing? If so, what sorts of consequences are most significant? If possible, please provide examples of each.

It is difficult to say – organisations that have been involved in a data breach would be best placed to answer this. We suspect that, yes, organisations may be less willing to share data where there has been a breach. However, we also suspect that a data breach can have a positive impact in terms of ensuring proper governance is put in place to minimise the risk of future breaches. Anecdotally, we have certainly been told that a data breach - and subsequent ICO enforcement action - has led to increased resources for information governance and to an improvement in standards. (The ICO intends to carry

out research into the effect of Civil Monetary Penalties on post-breach data protection practice.)

Other legal restrictions on the use of data

5.18 Public bodies' use of data can also be subject to private law rights, such as contractual, employment and intellectual property rights.
5.19 Question 12: What obstacles to data sharing, if any, does the existence of private law rights create, and are those obstacles appropriate? If possible, please give examples.

The most significant element of private law is probably the common law duty of confidentiality. This has been a particular issue where data are being shared in health and social services contexts. This is a complex area of the law where legal and ethical concerns converge and we suspect that much data sharing is prevented by confidentiality concerns – rightly so in many cases. (A good example of the complexity here is the GMC's guidance on confidentiality for doctors – this strikes a careful balance between the doctor's need to protect patient confidentiality and the need to share patient data with the police, for example where a patient's injury is indicative of involvement in serious crime.)

(Although this is not our area of expertise, we note that issues to do with property rights and the 'ownership' of personal data seem to be playing a more prominent role in the current debate about data sharing, big data and open data. We have heard it argued that if, for example, NHS patients' records are being anonymised, published and used by private companies to make profit, then the patients involved should also benefit financially from this. This debate also touches on the wider issue of who 'owns' an individual's personal data.)

5.20 Question 13: What benefits, if any, to data collection and sharing do these rights afford? If possible, please give examples.

We think it is worth reiterating our point that it is right that both private and public law does place restrictions on – and sometimes prevents – data sharing. Both elements of the law must continue to protect individuals from excessive, unnecessary or disproportionately intrusive data sharing. Confidentiality rules, for example, are in place for a good reason.

5.21 Question 14: Do you use strategies to manage the effect, if any, of private law rights on data sharing? If possible, please give examples.

n/a

Lack of incentives or motivation to share

5.22 Data collection and sharing can require a large investment in terms of resources and time. A public body able to collect and share

data may not consider data sharing to be a high priority to allow it to carry out its functions. Other public bodies may lack the resources to share data that would improve their ability to carry out their public functions. A public body may fail to share information because it does not have the necessary resources, in terms of staff, finance or time. We are interested in learning whether the distribution of those resources creates a lack of incentives to share data and what role managerial and organisational priorities and attitudes have on motivation to share data.

5.23 Question 15: Do you think that data sharing is prevented because public bodies lack the practical capacity or resources (lack of staff, money, time) to process and share data? If possible, please provide examples.

This is really for organisations with day to day involvement in data sharing to answer, and for the Information Sharing Centre of Excellence when it is launched next year. However, there is no doubt that if data sharing is to be done properly then this inevitably incurs costs – for example in terms of sorting out databases to make sure the right records are linked where data is recorded in different formats. However, clearly the costs are lower where information resources are already in good order.

The stronger mandating of open standards could have a positive effect here – ultimately making the interoperability of systems easier and cheaper. ICO has been supportive of the Cabinet Office's work in this area. (Please see the information governance section of the ICO's Data Sharing Code of Practice for more information about the 'nuts and bolts' issues surrounding data sharing.)

In terms of changing corporate behaviour in respect of data sharing, there needs to be a clear articulation of the benefit of data sharing for the organisations involved – for example in terms of providing a better service to the public or saving money – for example by re-using information that another organisation has already collected rather than re-collecting it. Although perhaps less of an issue than it used to be, we believe that organisations can feel under political or other pressure to share data without the benefits of this being articulated clearly enough. The data protection 'discipline' of having a clear purpose or objective for data sharing and designing the sharing with a set objective in mind is useful here.

ICO does not think that problems with motivation to share personal data, or lack of incentives for this, should be countered through mandated data sharing unless there is a very clear and specific, compelling public interest. We are not supportive of general clauses mandating data sharing.

5.24 Question 16: What role does a lack of incentives or motivation play in failure to share appropriately? If possible, please provide examples.

n/a

Concerns about security

5.25 Public bodies holding relevant information may not be willing to share it due to concerns about their own security systems, the security system of the prospective recipient body or the security of the process of communicating data. A number of cases of data loss have resulted from security issues and have increased security concerns.

5.26 Question 17: What role do you think security concerns play in public bodies' reluctance to share data? If possible, please provide examples.

This is a real issue and there is clearly a tension between the need to keep personal data secure and the desire to share it. This can be a particular problem when two or more organisations with different levels of security want to share data. A good example was the construction of the Contact Point database of children. Although this was eventually scrapped, we understand that the different levels of security between health, social services and the other organisations involved in the project was a major problem when preparing to share data. Whilst a 'higher common denominator' approach to security is the best one, it can be very expensive to implement and the challenges of changing long-established security cultures should not be underestimated. However, data protection law is perfectly clear, and when personal data is being shared all the organisations involved must afford it an appropriate level of security. Privacy by design approaches are relevant here because if implemented properly they mean that only minimal amounts of personal data, or data that has been anonymised are shared or matched, perhaps momentarily with no need for the various parties involved to retain copies of the data for any significant amount of time. This brings down costs and reduces privacy risk. The ICO has been very active in developing this approach – for example when working with counter-fraud bodies.

Quality issues

5.27 Problems with the quality of data, such as incomplete, out of date or inconsistent data, may be an obstacle to the transfer and linkage of data.
5.28 Question 18: What role do you think quality concerns play in public bodies' ability to share data? If possible, please provide examples.

Organisations should address poor data quality regardless of whether they intend to share it. However, data sharing brings data quality issues into sharp relief. Again, please see our data sharing code of practice for more information about data quality and related issues. It is worth noting that when public authorities were established their databases were often not designed with data sharing in mind. This means that even within the health service, for example, there are many different ways of recording dates of birth, different abbreviations are used for 'no fixed abode', names are transcribed into Latin characters in different ways and so forth. Ensuring data is recorded in a compatible format is a major issue and can be time-consuming and expensive

to sort out. We also suspect – but have no evidence to support this – that one barrier to data sharing can be the risk of exposing bad-quality data to external scrutiny and criticism.

Other possible causes

5.29 Question 19: Do you, or your organisation, find it difficult to secure the data you want because the holder of the information is unwilling to divulge it for other reasons? If so, what are the reasons? If possible, please provide examples.

n/a

5.30 Question 20: Are you, or your organisation, unwilling to divulge information for other reasons? If so, what are the reasons? If possible, please provide examples.

The Information Commissioner and his staff are subject to a strict statutory confidentiality provision in section 59 of the Data Protection Act, which can only be overridden in specific circumstances. Whilst we understand the reasons for this, there can be a tension between confidentiality and our desire to publicise our work for public accountability and other reasons, such as deterrence. This is a good example of a tension that runs through all data sharing – the desire to share information or make it publicly available versus the need to maintain personal privacy and confidentiality.

The use of shared data by public bodies

5.31 We are interested in the use of shared data by public bodies. This includes what information public bodies require and disclose, and from which and to which other public bodies. It also includes the purpose of sharing that data and the types of data that are shared, such as personal, sensitive personal, anonymised or deidentified data. We are also interested in consultees' views on the magnitude of the problems encountered in data sharing, for example, whether any difficulties in data sharing affect the possibility of sharing, cause delay or render sharing more onerous.

5.32 Question 21: Please describe the information you want or disclose, and the other public bodies concerned. For what purposes is the data required or disclosed? What types of data are concerned by this sharing? Through what process is it shared?

n/a

5.33 Question 22: Please describe the magnitude of any problem encountered in data sharing and the effects of such problems on data sharing.

The ICO is not a major 'data sharer' but we do share personal data and other information to carry out our statutory functions. However, rather than sharing

information we are more likely to ask or require another organisation to provide information to us – typically as part of an investigation or to handle an individual's complaint. (Note that much of what is described as 'data sharing' isn't sharing in the true sense of the word, but rather the provision of information by one organisation to another, often in a non-reciprocal arrangement.) We have not experienced any particular problems here and we hope that this is because when we ask organisations to 'share' information with us we frame our request in clear terms, only ask for relevant information to be provided to us and are clear as to the basis on which we are requesting the information.

We hope the ICO's responses have been of use. We will of course offer the Law Society any assistance we can as its work in this very important area continues.

[Law Commission: Data Sharing Between Public Bodies]

For further information on this submission, please contact ICO, Policy Delivery, casework@ico.org.uk

If you would like to contact us please call 0303 123 1113.

www.ico.gov.uk

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF

Information Commissioner's Office