ICO Scotland Conference 2014

Question & Answer session

The Question Time panel was:

- Ken Macdonald, ICO
- Iain Bourne, ICO
- Blythe Robertson, Scottish Government
- Paul Comley, WithScotland

Do I always need to get consent? Surely fair processing notices are enough.
No - the DPA provides alternatives to consent as the legal basis for processing personal data. However, seeking and obtaining consent to share their personal data can empower individuals and develop trust. If you are relying on consent, then you need to be prepared to stop sharing an individual's personal data if they revoke their consent. Whether or not you are relying on consent, the general rule is that you need to be transparent in respect of your data sharing, and a properly drafted privacy notice can deliver transparency. There are exceptions to the transparency rule, for example where telling someone that you are sharing their personal data would amount to a 'tip off' and prejudice the purposes of crime prevention.

Does there need to be specific legislation to enable data-sharing? Such as a Data Sharing Act?
It is the prerogative of governments to introduce legislation if there is evidence that data sharing is being improperly prevented. However, in the ICO's view the DPA does allow data sharing where this is a necessary and appropriate response to a particular issue. We remain to be convinced that a general data sharing act is necessary.

Is there consideration to be given to the DPA in respect of vexatious requests?
Unlike in Freedom of Information, the DPA does not contain a specific provision relating to vexatious requests. However an organisation does not need to comply with requests that are made unreasonably frequently. The ICO places great importance of the right of subject access but where there is clear and very strong evidence that a SAR is designed to inconvenience or annoy, it may choose not to take regulatory action against the data controller.

Data sharing initiatives aren't new. Has the Scottish Government identified the lessons to be learned from previous initiatives to inform current projects?

The Scottish Government has considered what worked well and what could be improved on from previous projects and identified some 'keys to success'. These are:

- Local decision making and proximity to the front line of service delivery gets results.
- Joint practice leadership ensures service wide adoption and "fit for purpose".
- Alignment to improvement planning processes and workforce development to gain collective support.
- Focus on incremental IT convergence agenda reduces complexity and provides opportunities.

It's also important to have the right governance arrangements in place for the particular project. For example, the Information Sharing Board is important in providing strategic oversight of information sharing issues in the Government's health and social care agenda.

Does the special purposes exemption allow for disclosure of third party data e.g. CCTV showing a missing person? Can you show footage of third parties?

The special purposes exemption could allow the disclosure of CCTV footage if this is being done for the purposes of journalism, for example. The exemption contains a public interest test, and the importance of finding a missing person would be a relevant factor in assessing whether the exemption applies.

Normally the identities of third parties should be disguised, for example through pixilation, but this depends on context and on the sensitivity of the information.

How can financial institutions play their part if they identify an adult at risk? Who do they notify?

It will depend on the nature of the risk and who is most appropriately placed to intervene in that person's best interests.

The ICO, the Scottish Government, adult protection committees and financial institutions will be working together over the coming year to look in more detail about how we can ensure effective data-sharing to safeguard adults at risk of financial harm. Part of that project will look at communication issues.

When there are joint data controllers, does one of the controllers have responsibility to pass SARs to the other?

We would expect them to do so as a matter of good practice, in order to ensure the information is made available to the requester as fully as possible. When a controller discloses personal data to another controller each has full data protection responsibility because both parties will exercise control over the purposes for which and the manner in which the data is processed. Where the sharing is systemic, large-scale or particularly risky, then both parties should sign up to a data sharing agreement, covering for example how the data can be used and whether it can be further disclosed. In other cases, where the sharing is a 'one off', is small scale and low-risk, then a more informal approach can be adopted (see our Data sharing code of practice for more information about this).

A data sharing agreement could provide for the controller that holds most of the personal data to be responsible for the practical elements of compliance. For example, if a number of organisations – each data controllers in their own right – are working together in a child protection initiative it would be acceptable for one of the organisations to take responsibility for giving individuals subject access to the personal data held by all the organisations involved.

If there is an agreement in place about who will deal with the various aspects of compliance, for example dealing with subject access requests, then the ICO will only seek to take action against the data controller with accountability for that aspect of compliance. However, the ICO may find that the other data controllers have failed in their obligations if:

- the allocation of responsibilities is unreasonable;
- the other data controllers are at fault for the non-compliance; or
- one of the other data controllers received the subject access request but failed to pass it to the controller responsible for handling requests.

In regard to adult protection, can I share concerns about likely risk to harm even although I have no consent for an intervention?

Yes, you can. However, it is not a case of sharing everything with everyone all of the time. It is very much about proportionality and appropriateness. If a professional practitioner has a genuine concern about a risk to anyone, the Data Protection Act 1998 is not a barrier to sharing as much of the concern as is proportionate, to an appropriate person/body in order to achieve the desired purpose. That purpose might be to get advice or to alert the body to a person's needs to provide some support or just to be aware of their situation.

What is SASPI?

The Scottish Accord on the Sharing of Personal Information (SASPI) provides a framework to enable organisations to share personal information in a manner compliant with the Data Protection Act. It is designed for organisations which provide services relating to health, education, safety, crime prevention and social wellbeing and, in particular, concerns those organisations that hold information about individuals and who may consider it appropriate or necessary to share that information with others.

SASPI is based upon the Wales Accord on the Sharing of Personal Information (WASPI) which acts as a single information sharing framework for Wales.