



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

Data Protection Officer Conference 10 March 2008

Workshop Outcomes

We held two workshops at the conference. The morning session focussed on security and the afternoon session looked at transparency. Delegates were divided into workshop groups as follows:

Red group: Central government

Yellow group: Health/ NHS/ Other

Green group: Bank/ Credit/ Finance/ Insurance/ Business/ Telecoms

Orange group: Bank/ Credit/ Finance/ Insurance/ Business/ Telecoms

Purple group: Police/ Prison/ Other

Blue group: Local Authorities and Local Government

Key Points

The key points that emerged from the workshops are summarised below. The detailed comments from each group follow on from this:

Workshop 1 – Security

- Everyone should recognise the value of adopting good security measures in relation to personal information.
- Senior management buy-in is key.
- Staff training is essential so that everyone understands their role and responsibilities.
- Security needs to be a 'live' issue and should be checked on an ongoing basis.

Workshop 2 – Transparency

- Ensure you have a legal basis for the processing in question.
- Review the personal information being processed by your organisation to check that sufficient details have been reflected in fair processing notices to customers/ members of the public.
- Consult customers on effective methods of communicating with them.
- Use a variety of methods to communicate information to your audience, appropriate to the individuals you are targeting.
- Keep information succinct and relevant to ensure individuals can understand any processing being undertaken and who they can contact if they have concerns.

2. Detailed Workshop Outcomes

Workshop Session 1 – Security

“Data Protection and Information Security”

Security is a key factor when protecting individual’s personal information. How do data protection officers encourage organisations to adopt appropriate security measures when working with personal information? We asked delegates to discuss the biggest challenges and share ideas on how they could meet these challenges in practice.

1. What approaches do you (DPOs) use in your organisation to ensure the security of personal information; do they work?	
Red	<ol style="list-style-type: none"> 1. People, for example staff training, developing policies and procedures and ensuring ownership and accountability. 2. Physical, for example appropriate technology and physical security. 3. Check it works, for example ensure buy-in and ‘police’ the practice.
Yellow	<ol style="list-style-type: none"> 1. Training, guidance and staff awareness. 2. Senior management buy-in. 3. Robust policies and procedures.
Green	<ol style="list-style-type: none"> 1. Follow industry standards, for example BSI, ISO, SARBOX, and P.C.I. 2. Tailor application to needs of your organisation and on basis of risk and experience.
Orange	<ol style="list-style-type: none"> 1. Training and staff awareness. 2. Ongoing monitoring and auditing. 3. Use of Privacy Impact Assessments in policy work. 4. Use of risk assessment and management. 5. Confidential waste policy. 6. Early engagement in project work to ensure security is considered,
Purple	<ol style="list-style-type: none"> 1. Ensure you have buy-in across the organisation – top to bottom. 2. Ensure that security features in project work.
Blue	<ol style="list-style-type: none"> 1. Staff training. 2. Good use of ICT. 3. Information audits 4. Ensure there is ownership for security. 5. Share good practice. 6. Good policies and approval at Board level. 7. Work within projects to ensure that security is considered early on. 8. Balance resources needed to ensure good security, against the overall savings made through minimising data protection risks.

2. Who are your (DPOs) key partners within the organisation in ensuring the security of personal information?	
Red	<ol style="list-style-type: none"> 1. Experts, for example working with practitioners and influencing other stakeholders. 2. Everyone.
Yellow	<ol style="list-style-type: none"> 1. Frontline staff, IT and senior management. 2. Members of the public, customers and 3rd party bodies.
Green	<ol style="list-style-type: none"> 1. Everyone has a role and responsibility; some will have a particular interest on behalf of a specialist area.

	<ol style="list-style-type: none"> Recruitment. Technological staff. Frontline staff, for example in a contact centre.
Orange	<ol style="list-style-type: none"> Management Board, IT partners, Legal, HR, Marketing, Operations, Audit, Fraud and Investigations Department – in effect everybody to different degrees.
Purple	<ol style="list-style-type: none"> Information security (IT) and HR to ensure appropriate staff training.
Blue	<ol style="list-style-type: none"> Senior management. Service heads, for example IT, Audit, Information Management. Involve Heads for areas handling sensitive personal information, for example children's services and HR.

3. What are the main challenges you (DPOs) face in your role when it comes to ensuring the security of personal information (suggest 3), and how do you (DPOs) meet these challenges in practice?

Red	<ol style="list-style-type: none"> Ensuring staff awareness, this influences how successful security can be. Information sharing; data protection is one part of a wider challenge.
Yellow	<ol style="list-style-type: none"> Understanding and prioritising risks (through audit). Ensuring guidance is 'fit for purpose' within an organisation. Technological balance, for example using the right level of security appropriate to the type of information you are handling.
Green	<ol style="list-style-type: none"> How do you measure risk? Senior management buy-in. Getting staff to follow procedures. <p>Ways around the challenge:</p> <ol style="list-style-type: none"> Training and monitoring of compliance.
Orange	<ol style="list-style-type: none"> Ensuring you have buy-in across the organisation - top to bottom. Resources and budget available. Ensuring you are involved at an early stage. Staff understanding, for example the importance of a clear desk policy. Reputation and impact on the organisation if something goes wrong.
Purple	<ol style="list-style-type: none"> Resources and budget available. Ensuring security both internally and externally. Ensuring compliance and effective use of risk management.
Blue	<ol style="list-style-type: none"> Ensuring people understand the need for security. Ensuring that sufficient resources are allocated to security. Managing the culture change. Implementing good security. <p>Ways around the challenge:</p> <ol style="list-style-type: none"> Training Management buy-in. Undertaking a risk assessment. Promoting the benefits of security across the organisation.

Workshop Session 2 – Transparency

“Using Fair Processing Effectively”

Fair processing ensures there is transparency in how personal information is being used. We asked delegates to share experiences of how fair processing worked across their organisations. Specifically, what are the benefits and how can we improve fair processing in practice.

1. How do you (DPOs) work with your organisation to ensure fair processing arrangements are considered?	
Red	<ol style="list-style-type: none"> 1. Corporate awareness. 2. Ensure that the secondary use of personal information is compatible.
Yellow	<ol style="list-style-type: none"> 1. Work with patients and get feedback on how effective the organisation is at communicating. 2. Work in central policy development. 3. Work with legal services.
Green	<ol style="list-style-type: none"> 1. Involvement in product system design. 2. Periodic review of form design. 3. Review of system changes.
Orange	<ol style="list-style-type: none"> 1. Ensure that there is effective e-training; good policies and procedures; good monitoring and audit, and engage with organisational projects. 2. Establish how information is collected by the organisation. 3. Identify the purposes for which it is used. 4. Ensure organisation has the authority to process information. 5. Maintain library of texts to support organisational awareness and understanding. 6. Ensure there is staff training on the Data Protection Act. 7. Ensure there are adequate control functions, approval processes and that key responsibilities and ownership are clearly identified. 8. Ensure there is transparency, and that the organisation communicates in plain English. 9. Use call scripts and pre-recorded information to ensure clear and consistent messages are given.
Purple	<ol style="list-style-type: none"> 1. Be proactive. 2. Consult with information collectors. 3. Review purpose for which information is held. 4. Audit and observe how fair processing is working in practice. 5. Train staff to raise awareness.
Blue	<ol style="list-style-type: none"> 1. Ensure that IT services link to data protection. 2. Train staff. 3. Be pro-active when aware of developments which may have an impact on individual's personal information. 4. Provide guidance with outline templates for the organisation to use. 5. Ad hoc involvement in organisational projects on request to ensure data protection advice is given.

2. What methods of fair processing do you (DPOs) recommend to your organisation?

Red	<ol style="list-style-type: none"> 1. Encourage use of web based information. 2. Encourage organisations to raise age requirements in terms of ensuring awareness and understanding of fair processing information.
Yellow	<ol style="list-style-type: none"> 1. Use good communication channels, such as leaflets, websites, staff training, letters etc. Use a layered approach. 2. Use face to face updates as appropriate. 3. Use public consultations, for example PALS and public forums. 4. Notification to the Commissioner is a form of fair processing.
Green	<ol style="list-style-type: none"> 1. Communicate simply and clearly. 2. Remind customers at key times (in terms of what you are doing with their information). 3. Consider fair processing particularly carefully when advising customers as they are often more focussed on buying something rather than considering their privacy issues.
Orange	<ol style="list-style-type: none"> 1. Ensure clear statements on data protection. 2. Publicise a privacy policy. 3. Put key messages on staff computers, for example screen savers. 4. Ensure fair processing is considered in any data collection exercise.
Purple	<ol style="list-style-type: none"> 1. Take a layered approach to raising awareness in your own organisation. 2. Publish plans setting out what you're going to do, to a wide audience, 3. Websites, leaflets and forms should include relevant fair processing information. 4. Call scripts should include fair processing information, 5. Reception areas and custody suites should have fair processing information available. 6. There should be contracts/ information sharing agreements in place.
Blue	<ol style="list-style-type: none"> 1. Verbal messages backed up by paper and web information. 2. Use council tax bills and council publications. 3. Use the website as this enables changes to be made to messages at appropriate stages over time.

3. What are the main challenges in ensuring that fair processing requirements are met by your organisation (suggest 3), and how do you (DPOs) meet these challenges in practice?

Red	<ol style="list-style-type: none"> 1. Clearly identifying the data controller or processor. 2. Ensuring that the right balance of information is provided – not providing too much/ too little. 3. Raising organisational knowledge and awareness of the importance of fair processing.
Yellow	<ol style="list-style-type: none"> 1. Getting the messages across in plain English whilst ensuring that individuals are aware of any legal framework. 2. How do you provide services where no consent is given? 3. Possible staff and patient confusion, for example too little information too late, or consent versus ensuring 'awareness'. 4. Ensuring consent is appropriate, for example complete, implied or 'awareness' only. 5. Ensuring that consent is obtained at the appropriate time, for example point of treatment or consultation.

	<ol style="list-style-type: none"> 6. Use of violent markers, for example having an effective 'flagging' system and ensuring it is reviewed and up to date.
Green	<ol style="list-style-type: none"> 1. Difficult to judge a 'reasonable expectation' of the processing being undertaken as often customers don't take it in when they sign up for services etc. 2. Considering what is a compatible secondary use of personal information. <p>Ways around the challenge:</p> <ol style="list-style-type: none"> 1. Clear statements on websites and in paper based communications. 2. Possible 'one stop shop' for industry fair processing information. 3. Check practices to ensure they are consistent with fair processing information provided to customers.
Orange	<ol style="list-style-type: none"> 1. Keeping information up to date. 2. Ensuring notification is up to date. 3. Ensuring information is kept clear and succinct. 4. How to communicate fair processing information which affects 'everyone'. 5. Using marketing effectively. 6. Incorporating IT support.
Purple	<ol style="list-style-type: none"> 1. Defining what is fair and reasonable; a code of practice would assist here. 2. There is a loss of control when you share information. 3. Keeping notices up to date and simple. 4. Identifying new processing. 5. Tailoring fair processing information.
Blue	<ol style="list-style-type: none"> 1. Making people aware and ensuring they know their rights in relation to how an organisation is processing their personal information. 2. Using easy language. 3. Ensuring effective fair processing information is given – using the website, publications, pamphlets, radio and TV as appropriate. 4. 3rd party processing arrangements and agreements. Ensuring there is a balance between the use of information by the 3rd party and the individuals being made aware that the processing is taking place.