Privacy Impact Assessment

The production of a Privacy Impact Assessment (PIA) within any organisation, HMG or private sector, will address the privacy issues regarding a project and visibly demonstrate an organisation's commitment to data protection. Completion of a PIA enables an organisation to decide if a proposal complies with applicable legislation and to identify the wider implications for individual privacy. Proactive consideration of privacy at the development stage can help to save costs and protect reputations, since potential mistakes involving the handling of personal data[1] can be avoided from the outset. Amendments to data protection law, which will impact both public and private organisations, are currently being considered – as detailed below.

Data Protection Reviews

A review of the European data protection regime took place in January 2012 [1] *"....to ensure a holistic approach to compliance, the EU and national regulators, like our Information Commissioner, are planning to introduce an "accountability principle" into data protection law...."* [2]. The accountability principle relies on the concept of 'Privacy by Design', which requires the data controller to identify and minimise the privacy risks at the very beginning of new projects, when they are still on the drawing board. A written compliance programme will need to be put in place to meet the objectives of the data protection principles, including data accuracy and security. One of the key mechanisms in achieving Privacy by Design will be the early completion of a PIA.

Carrying out the PIA process at this stage of a project enables the data controller to address privacy and data protection concerns before a product or service is deployed. Consideration at the design stage benefits both the individual and data controller by avoiding the significant costs and often unsatisfactory solutions that arise from the retrospective addition of privacy features to deployed solutions. The PIA process should be completely transparent and data controllers will be required to maintain records as proof of compliance – records that may be called upon by regulators following an incident or as part of a compliance audit.

In May 2011 the Information Commissioner's Office (ICO) released the Data Sharing Code of Practice on the sharing of personal data [3]. Within which data controllers are advised that it is good practice to carry out a privacy impact assessment before entering into any data sharing arrangement.

Purposes of a PIA

[1] 'Personal data' means any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her identity.

The primary purpose of a PIA is to visibly demonstrate that an organisation acts responsibly in relation to privacy. A key goal of the PIA is to effectively communicate the privacy risks associated with the development of a system to handle and distribute personal data that would not be addressed through standard departmental mechanisms. The PIA is intended to contribute to senior management's ability to make fully informed policy, system design and procurement decisions.

An organisation will undertake a PIA in order to:

- identify and manage areas of risk;
- avoid unnecessary costs;
- prevent the development of inadequate solutions;
- avoid loss of trust and reputation;
- demonstrate appropriate compliance against The Data Protection Act 1998 (DPA) [4], HMG Information Assurance Standard No. 6 (IAS6) [5], ICO guidance and relevant Standards;
- inform citizens and partners of the organisation's communications strategy; and
- meet (or exceed) legal requirements.

The underlying principal of the PIA is to ensure that data sharing is undertaken within a clear legal framework and that intrusion upon an individual's privacy is kept to a minimum. The ICO recommendation for projects already up and running is that they "*are not submitted to a PIA process, but to either a compliance check or a data protection audit*" [6].

The PIA process needs to be clearly distinguished from privacy or data protection audits. PIAs are ideally completed at the design stage of a project, whereas an audit is carried out on a project that has already been implemented. The ultimate focus of a PIA is compliance with the DPA [4]; in the same way, an audit provides confirmation of compliance with privacy laws and highlights areas that need to be addressed.

The aim of a PIA is to prevent problems from arising and thereby avoid additional expense or disruption. Highlighting risks through completion of the PIA process ensures the Senior Information Risk Owner (SIRO) is aware of the issues and can determine how to deal with each risk holistically. Requirements arising out of the PIA process should enable additional processes and procedures to be implemented to manage the risks.

The private sector needs to consider the same factors as public sector organisations when dealing with personal data. For many private sector organisations, privacy poses a risk which needs to be professionally and comprehensively managed in a similar way to other categories of risk. Organisations dealing with personal data need to monitor their ongoing operations when dealing with clients, employees, or the general public. Information security and assurance procedures enable compliance with relevant legislation and recognised standards (DPA [4] and International Standards Organisation (ISO)). However, they do not analyse risk from a privacy perspective by considering "*how to ensure that external privacy concerns are identified and addressed or whether a particular programme is compliant with the broader rights to privacy and confidentiality provided by UK and European law*" [6].

By contrast a PIA will address these issues and any requirements from the stakeholders that may be affected by the project. The PIA is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. It ensures awareness of problems and enables pragmatic solutions to be developed and implemented. The PIA must be viewed as a separate process from compliance checking or data protection audit processes. By utilising recommendations from the ICO PIA Handbook [6], an organisation can produce and implement a PIA that is both relevant and appropriate to their circumstances.

What is privacy?

Privacy, broadly interpreted, is about the integrity of the individual and encompasses many aspects of the individual's social needs. The ICO PIA handbook [6] identifies four aspects of privacy that a PIA could consider:

- the privacy of personal information (data privacy);
- the privacy of the person (bodily privacy);
- the privacy of personal behaviour (observation of what people do); and
- the privacy of personal communications (recording and analysis of communications).

Privacy is protected by overlapping laws; these include The Human Rights Act, The Privacy and Electronic Communication Regulations 2003 and DPA 1998 [4]. A more comprehensive list of relevant areas of law regarding privacy is provided in the ICO PIA Handbook [6] (Part II, Chapter VI).

Why is privacy important?

High-profile losses of personal information have increased the general public's awareness of privacy issues regarding the extent of the collection, storage and use of their personal data. The media has a huge impact on the public's perception of privacy issues and has the capacity to turn a minor issue into a public furore within a few hours. Privacy is a risk factor for many organisations, including the potential impact of a loss of their public reputation and standing.

Serious consequences have resulted from organisations misjudging what the media and the public will accept. The most recent Financial Services Authority (FSA) example was the loss, by Zurich Insurance in August 2008, of an unencrypted back-up tape containing personal financial information belonging to 46,000 individuals. According to the Telegraph [7], this loss resulted in a £2.2m fine being levied on the UK branch of the company (the highest fine imposed to date for data security failings by the FSA). As the ICO press release [8] regarding this incident explains, Zurich Insurance has, since the loss, signed an undertaking with the ICO to ensure that back-up tapes are appropriately secured during transit, in addition to other measures to secure data. The fine was levied for non-compliance with the DPA [4], so the completion of a PIA or a compliance check should have highlighted this risk. If processes to mitigate the risk had been in place, whilst the loss might still have occurred the privacy impact could have been lessened.

When using its regulatory powers, the ICO considers the nature and severity of any breach. The powers the ICO has at its disposal include serving information or enforcement notices, issuing monetary penalties of up to £500,000, conducting audits and prosecution of individuals or organisations who commit criminal offences under the DPA [4]. As of October 2010 numerous undertakings and enforcement notices have been issued by the ICO, but (as yet) no monetary penalties [9].

The PIA process

During the initial assessment phase consultation and analysis takes place, including examining the project, identifying stakeholders and making an initial analysis of privacy risk. This assessment informs the decision on which level of impact assessment is needed: a full-scale PIA, small-scale PIA or no PIA. An essential aspect of the screening process is to identify privacy risks associated with a project. Once the risks have been identified then the necessary management actions can be decided upon. The three options to be considered for each risk are:

- Accept the risk, impacts or liabilities (a record of acceptance is required detailing the reasons for acceptance).
- Identify a way to avoid the risk (i.e. dissipate the risk, perhaps by excluding certain technologies, processes, data or decision criteria in order to avoid particular privacy issues arising).
- Identify a way to mitigate the risk (incorporate one or more features that compensate, in whole or in part, for other privacy-intrusive aspects of the design).

The assessment will help to determine not only the level of work and resources required, but also areas of policy that may demand further, more detailed consideration.

Normally, if a proposal involves the collation of a large quantity of personal data, some of which is sensitive and requires a high level of security protection, the likelihood is that a full-scale PIA will be required. On the other hand if, for example, a change were to be made to the processing of an existing database then a small-scale PIA would probably suffice (unless the analysis suggested any major additional impacts on an individual or their data).

The initial screening questions will focus on and determine the areas of concern and are the same regardless of the level of PIA that is found to be required. The difference lies in the level of work needed to complete a full-scale, as opposed to a small-scale, PIA.

- A full-scale PIA conducts a more in-depth internal assessment of privacy risks and liabilities, analysing privacy risks, consulting widely with stakeholders on privacy concerns and bringing forward solutions to accept, mitigate or avoid these risks.
- A small-scale PIA is similar to a full-scale PIA but it is less formalised and in-depth, necessitating a less exhaustive level of information gathering and analysis. A small-scale PIA is more likely to be used when focusing on a specific aspect of a project.
- If relevant, also conduct a:
- Privacy law compliance check. This focuses on compliance with various "privacy" laws for example Human Rights Act, Regulation of Investigatory Powers Act, Privacy and Electronic Communications Regulations and the DPA [4]. The check examines compliance with the statutory powers, duties and prohibitions in relation to the use and disclosure of personal information.
- Data protection compliance check. This is a checklist for compliance with the DPA [4] that

would usually be completed at a later stage when the project was more developed. (If a PIA assessment were to be initiated further into the project then a Data Protection compliance check could be completed at the same time.)

It should be noted that a PIA does not have to be conducted in order to check that a project is compliant with the DPA [4] and other legal requirements.

Finally, the review stage sets out the timetable for reviewing actions taken as a result of the PIA and examines their effectiveness. New aspects of the project would also be considered and an assessment made to whether they should be subject to a PIA.

Summary

The PIA process enables a data controller to address privacy and data protection risks in a comprehensive and systematic manner. The completion of a PIA provides an opportunity to reduce legal uncertainty and to avoid the loss of trust and reputation amongst the public that can all too easily arise if data protection issues are not addressed comprehensively. Although the ideal is to consider privacy as an integral part of the design and to conduct the PIA at a very early stage in a project, there is also benefit to be had from conducting a PIA or compliance check at any stage (provided there are resources available to implement the actions highlighted by the outputs from these processes). A PIA does not have to be conducted in isolation: it can be a very useful tool if used to consider privacy issues in a broader policy context. The requirements of the PIA may overlap work that is already being completed by the project, for example in the areas of information security and assurance. The PIA can be integrated into accreditation documentation to gain accreditation for the system or service, or it can be completed as a standalone requirement.

How Regency IT Consulting can help

Regency IT Consulting firmly believe in a quality, structured and cost-effective approach to Information Security, based on a solid foundation of Risk Assessment and Analysis through a structured methodology. We also recognise that, to be effective, any Security Policy and countermeasure recommendations must be aligned to the requirements of the organisation and have maximum gain versus minimum operational impact, whilst ensuring compliance with relevant legislation and policy.

We have provided organisations with consultants who offer unique information assurance knowledge, advice and guidance, combined with the expertise and resources of the private sector. We are aware of the threats and vulnerabilities that information systems are likely to face, both now and as technology and business needs develop. We have assisted Government departments seeking to bring their networks in line with the requirements of the Security Policy Framework (SPF), implemented International Standards for Information Security Management (ISO 27001) and provided Government standard information assurance advice to the broader public sector (Cabinet Office, Treasury, Ministry of Justice, Home Office, Defence, Police Forces, agencies, NDPBs etc).

Regency IT Consulting employs some of the UK's most experienced Information Security practitioners, including CESG-Listed Advisor Scheme (CLAS) registered consultants well versed in delivering Risk Management and Accreditation Document Sets (RMADS), Business Impact Assessments (BIA) and Technical Risk Assessments (TRA), Information Security Management Systems (ISMS) and business continuity management for multifaceted systems across both the public and private sectors. They are thoroughly familiar with relevant Government policy, standards, legislation and risk management methodologies.

With regard to PIAs specifically, Regency ITC consultants have extensive experience and knowledge of completing the whole process from assessment and development through to production and delivery of both full and small-scale PIAs. The ICO PIA handbook suggests carrying out a screening process to determine the key protection and security issues regarding the privacy of a particular proposal or project. To assist this process Regency ITC has developed a concise document of pre-screening questions to determine the necessary level and depth of the PIA. This pre-screening process feeds into and complements the next stage, which is the in-depth scoping appraisal developed by Regency ITC. Completion of this scoping appraisal ensures that the correct level of information is gathered and enables the Regency ITC consultant to provide a professional, comprehensive and relevant PIA. The structure of the Regency ITC PIA includes data flow analysis, privacy analysis, a privacy risk management plan and a communications/publication strategy. The PIA can be provided as an integral part of an RMADS or as a standalone document. In addition to the PIA, our consultants can complete privacy law and data protection compliance checks, either as part of the PIA process or as separate requirements.

Our consultants can analyse your organisation and assist in the identification of information assets and asset owners, threats, vulnerabilities and associated risks. We can provide recommendations for cost-effective technical and non-technical countermeasures, audit procedures, legislation and personnel education and training requirements. Our analysis will identify existing security features and countermeasures already in place within the organisation, which can then be incorporated into future documentation and compliance evidence, thus providing immediate risk mitigation and ultimately cost savings. The PIA will assist you in achieving Government and International recognised accreditation and/or certification.

References:

[1] European Commission Proposal for a General Data Protection Regulation. Available at: http://bit.ly/QqcxKr

[2] Stewart Room, ComputerWeekly.com – *The only way is tough –the future of data protection law* [online]. Available from: http://www.computerweekly.com/Articles/2010/10/11/243292/The-only-way-is-tough-the-future-of-data-protection.htm

[3] Information Commissioner's Data Sharing Code of Practice. Available at: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx

[4] Data Protection Act 1998 [online]. Available from: http://www.legislation.gov.uk/ukpga/1998/29/contents

[5] CESG, HMG Information Assurance Standard No 6 – Protecting Personal Data and Managing Information Risk [online]. Available to GSI users at: http://www.cesg.gsi.gov.uk/ia-policy-portfolio/hmg-ia-standards.shtml

[6] Information Commissioner's Office, *Privacy Impact Assessment Handbook v2* [online]. Available from: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

[7] Louise Armitstead, Telegraph - *Zurich UK fined record £2.28m for losing customer details* [online]. Available from: http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/insurance/7962642/Zurich-UK-fined-record-2.28m-for-losing-customer-details.html

[8] Information Commissioner's Office Press Release, *Zurich Insurance agrees to improve information security after losing over 46,000 individuals' personal financial information* [online]. Available from: http://www.ico.gov.uk/upload/documents/pressreleases/2010/zurich_insurance_plc_240310.pdf

[9] Information Commissioner's Office, *Taking action* [online]. Available from: http://www.ico.gov.uk/Home/what_we_cover/promoting_data_privacy/taking_action.aspx#notices