PIA Handbook
Contents

Version 1.0, 31 October 2007

PIA Handbook - Preface

[This draft text indicates the topics that it is envisaged the Preface will address]

[To the extent that any aspect mentioned here is omitted from the published Preface, a check needs to be performed to ensure that the point is made elsewhere, most likely in Intro.html]

A key function of the Information Commissioner's Office is the promotion of good data protection practice, in particular through the provision of guidance to business and government.

Developments in information technology continue apace, and there is legitimate public concern about the impact on privacy, including data privacy. This concern translates into risks for business and government, because the effectiveness and efficiency of their activities depends on adoption and appropriate use of information technology.

These risks can be much better managed if they are understood. Organisations use various risk management techniques to achieve this. The particular form of risk management technique that is relevant in this context is commonly referred to as 'Privacy Impact Assessment', or PIA.

The Office has commissioned the development of this Handbook to provide guidance to organisations when they conduct PIAs. All aspects of the Handbook are expressed as advice. There are currently no circumstances in which the conduct of a PIA is mandatory, and no aspect of this document gives rise to legal obligations that do not already exist.

The Office commends the document to executives and managers throughout the public and private sectors.

Data Protection Act s.51

(1) **It shall be the duty of the Commissioner to promote the following of good practice by data controllers** and, in particular, so to perform his functions under this Act as to promote the observance of the requirements of this Act by data controllers.

(2) The Commissioner shall arrange for the dissemination in such form and manner as he considers appropriate of such information as it may appear to him expedient to give to the

public about the operation of this Act, about good practice, and about other matters within the scope of his functions under this Act, and may give advice to any person as to any of those matters.

Up to the Contents Page Introduction ==>>

Version 1.0, 31 October 2007

PIA Handbook - Introduction

The Nature of Privacy Impact Assessment

Projects that involve personal information or intrusive technologies inevitably give rise to privacy concerns. The cumulative effect of many such initiatives during recent decades has resulted in harm to public trust and to the reputations of corporations and government agencies alike.

Where the success of a project depends on people accepting, adopting and using a new system, process or program, privacy concerns can be a significant risk factor that threatens return on the organisation's investment. In order to address this risk, it is advisable to undertake a particular risk management technique commonly referred to as Privacy Impact Assessment (PIA).

The scale of effort that is appropriate to invest in a PIA depends on the circumstances. A project with large inherent risks warrants much more investment than one with limited privacy impacts. Other projects may merely need a check of their compliance with privacy laws, and in particular with the provisions of the Data Protection Act.

A PIA is best conducted early in the life-cycle of a project. Compliance Checks, on the other hand, are usually performed at a later stage, after business processes and business rules have been specified sufficiently that they can be assessed for their compliance with the law.

A PIA may be conducted as a separate process, in parallel with the project that gives rise to the privacy concerns. Alternatively, organisations are likely to find it more effective to integrate the PIA within the project plan as a whole, or within broader risk assessment and risk management activities.

The Nature of This Handbook

Organisations vary greatly in their size, the extent to which their activities intrude on privacy, and their experience in dealing with privacy issues. It is therefore simply not feasible to write a 'one size fits all' guide. The purpose of this Handbook is to be comprehensive. So for each project that it is applied to, some parts will not be relevant.

The Handbook may appear to repeat information already provided in another segment. The reason this was done is to make the segments more readily understandable by people who read them separately rather than reading the whole document sequentially.

It is of course necessary to ensure compliance with privacy laws. On the other hand, there is no legal obligation to undertake a PIA, and hence none of the information about PIAs is mandated. The information is provided purely as guidance to organisations, to assist them in making their own judgements for each project that they undertake that has potential privacy impacts. Each organisation is encouraged to use the Handbook to devise and implement a PIA process that is appropriate to their particular circumstances.

The Handbook's structure, which is outlined below and provided in detail in the Table of Contents, is intended to enable a reader who is knowledgeable about privacy to start working on the PIA quickly. For readers who would like some general information prior to plunging into the advice relating to the PIA process, background information on privacy and PIAs is provided.

The Structure of This Handbook

In order to determine whether a PIA is required, and, if so, how substantial it needs to be, a short, preliminary study is recommended. In this Handbook, that study is referred to as a 'Screening Process'.

Part I of the Handbook provides straightforward guidance on how to prepare for and conduct that Screening Process. It involves assessing the project against four sets of criteria.

After the Screening Process is completed, it should be clear whether a Full-Scale PIA is warranted (addressed in Part II of the Handbook), or a Small-Scale PIA is sufficient (addressed in Part III), or neither is required.

A PIA examines broad questions about privacy impacts and people's perceptions. Organisations also have an obligation to comply with relevant laws. The Screening Process accordingly assists organisations to determine whether a general Privacy Law Compliance Check needs to be performed (Part IV) and/or a specific Data Protection Act Compliance Check (Part V).

Up to the Contents Page Preparation ==>>

Version 1.0, 31 October 2007

Privacy and PIA Backgrounder

Privacy

Privacy has loomed as a much larger factor in business and government in recent decades. Many new information technologies have increased public concerns about intrusiveness.

Privacy has long been recognised as part of the bundle of human rights, although the concept remains somewhat vague or has different specific meanings. It is usefully interpreted as "the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations".

Many people feel a psychological need for such a 'space'. But arguments are also advanced that the arts and literature, and the inventiveness and innovation needed in a health economy, are all dependent upon people having enough space to be a little bit deviant and thereby create something new. Clearly, democratic freedoms also hinge on people's political behaviour not being 'chilled' into conformity with the dictates of a powerful elite.

Beyond the recognition of privacy as a human right, specific laws have been introduced to deal with particular areas of concern. Much of the legislative attention to date has been focused on information about people that is collected, stored, used and disclosed by organisations. The handling of personal data is regulated by the Data Protection Act, which the Information Commissioner's Office oversees.

There are, however, other dimensions of privacy, and these have been attracting an increasing amount of attention. Current high-profile issues include the surveillance of the activities of employees, consumers and citizens, the monitoring and recording of people's electronic communications and their electronic access to information, and the acquisition of biometrics, body fluids and body tissue.

An important implication of the definition of privacy as an interest is that it has to be balanced against many other, often competing, interests. The practical approach to privacy protection is therefore to find appropriate balances between privacy and those multiple competing interests.

The General Resources segment of this Handbook includes further discussion about privacy, privacy protection and the importance of privacy.

Managing Privacy Concerns

Organisations may adopt various approaches to privacy concerns. As a minimum, they must ensure that they are compliant with the various laws that protect privacy, including the Data Protection Act.

Many organisations find that it is appropriate to go further than that. Some establish a comprehensive privacy strategy, and actively encourage a privacy-sensitive culture. Other organisations judge that significant investment in privacy strategy would be unwarranted, but instead put processes in place to ensure that privacy concerns are considered when business process design and re-design are being undertaken. This may be achieved, for example, by adapting the organisation's system development and project management procedures.

Privacy can be approached as a corporate responsibility, much as ethical and environmental issues are handled. Alternatively, it can be viewed as a risk that threatens the fulfilment of the organisation's objectives. This is a particularly relevant approach to adopt if the organisation is dependent on people adopting new technology, or complying with requests for information. It may prove impossible to achieve service improvements and cost reductions unless constructive relationships are sustained between the organisation and its employees or customers. And return on investment is unlikely to be achieved if people actively distrust the organisation.

Privacy Impact Assessment

Privacy Impact Assessment (PIA) is a process whereby organisations can anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions. Risks can be managed, through the gathering and sharing of information with stakeholders. Systems can be designed so as to avoid unnecessary privacy-invasiveness, and features can be built in from the outset that ameliorate negative privacy impacts. A PIA usually results in a PIA Report, which may be published, distributed to participants, or (less usefully) filed for future reference.

PIAs have become mainstream activities in such countries as Canada, the USA and Australia, particularly in the public sector, and in some jurisdictions are legally required. Their use is also increasing for private sector projects that have significant potential for privacy impact and in personal-data-intensive business sectors.

This Handbook provides guidance for performing a PIA. It also incorporates information relating to compliance with privacy laws generally, and the Data Protection Act in particular.

<<== Introduction Up to the Contents Page Preparation ==>>

Version 1.0, 31 October 2007

Preparing for the PIA Screening Process

Sufficient information must be gathered to allow the criteria in the Screening Process to be applied. The following three steps are suggested:

1. Prepare a Project Outline
2. Undertake a Stakeholder Analysis
3. Perform an Environmental Scan

The Screening Process questions are likely be answered (at least provisionally) on the basis of the information arising from those three steps. If that is not the case, several further suggestions are offered.

---

1. Prepare a Project Outline

Risk management is most effective where it is commenced early in the project life-cycle. On the other hand, during the early stages of a project, there is only limited documentation available, and there is uncertainty about the project's scope and the features of the intended system.

Early in the project life-cycle, the most likely sources of information are:

- project initiation documents such as a Project Charter or Terms of Reference
- interviews with relevant staff in the lead organisation, key stakeholders, members of the Project Steering Committee, and perhaps others as appropriate to the circumstances

On the basis of this information, a relatively short description of the project can be prepared, as a basis for the subsequent analysis. When it is being drafted early in the project, the Project Outline is likely to be a 1-to-2 page document.

Where the activity is conducted at a later stage of the project life-cycle, much more information will be available, and the document should provide references to relevant documents, including descriptions of relevant technologies, predecessor systems and/or similar projects elsewhere.

If any previous PIAs have been conducted, in an earlier phase of the project, or in relation

to the development of the system that the project is intended to enhance or replace, then this step is likely to be greatly facilitated by reference to them.

---

2. Undertake a Stakeholder Analysis

The categories of individuals who may see themselves as 'having a stake' in the project should be identified at an early stage. This may include:

- the organisation conducting the project, but perhaps also various sub-organisations within it
- other organisations directly involved in the project
- organisations and individuals that are intended to benefit from it
- organisations and individuals that may be affected by it
- possibly also organisations that provide technology and services to enable it

It is advisable to document the results of the Stakeholder Analysis in an appropriate form, most likely a 1-page summary.

---

3. Perform an Environmental Scan

It may be valuable to seek out information about prior projects of a similar nature. Where new technology is being used, or the project applies existing technology in new ways, it is likely to assist the evaluation if descriptions of the technology and its applications are gathered.

Such sources as the following may be considered:

- prior PIAs on similar projects, whether conducted:
    - within the organisation
    - by other organisations; or
    - in other countries
- fact sheets, white papers, reports and refereed articles published by industry associations, technology providers, and research centres
- consultations with professional associations. Possibilities include CIO Connect, and the Chief Information Officer Council, but the orientation and expertise of organisations like these vary over time
- consultations with privacy regulators, in particular the Information Commissioner's Office
- consultations with other regulators, e.g., in the consumer rights arena

- consultations with non-government organisations that represent affected segments of the population or perform advocacy on their behalf

These investigations may lead to designs and design features that have been devised by other project teams in order to address much the same categories of problem confronted by the project under consideration.

As with the other parts of this preparatory step, it is advisable to document the outcomes of the Environmental Scan in an appropriate form, most likely a 1-to-2 page summary, with reference to working documents generated during the process. Original documents should be assembled.

Apply the Criteria

With the available information compiled, and documented in a convenient form, it should be possible to undertake the Screening Process. This involves applying Criteria described in the following segment of the Handbook.

It is stressed that the purpose of the Screening Process is to ensure that the investment the organisation makes is proportionate to the risks involved. Only some elements of this Handbook will be relevant in any given case.

If Insufficient Information Is Available ...

It is possible that the available information about the project may not be sufficient to enable a clear conclusion to be reached in respect of any particular Criterion. In that case, the following options are available:

- further discuss the matter with relevant staff of the key organisation, stakeholders, Steering Committee members, and/or other relevant people
- commence a Full-Scale PIA, keeping in mind the possibility that it may need to be curtailed in the event that the project proves to have only limited privacy impact
- suspend the PIA Screening Process, pending clarification
- look further afield for information sources, such as PIAs performed on projects that may at first appear dissimilar but share characteristics with the current project.

<<== Introduction Up to the Contents Page Screening Process ==>>

Version 1.0, 31 October 2007

The PIA Screening Process

It can be very expensive for an organisation to discover too late that a project has substantial privacy impacts. On the other hand, conducting an assessment of privacy impacts can be expensive too. It is desirable to conduct a limited preliminary evaluation, in order to establish the extent to which the organisation needs to invest in privacy impact assessment.

This segment of the document presents a four-step PIA Screening Tool. The answers to the four sets of questions about the project should indicate whether a PIA is needed, and if so, whether the project requires the intensity of effort of a Full-Scale PIA or a Small-Scale PIA. In addition, the Screening Tool clarifies whether Compliance Checking is necessary against privacy laws generally, and the Data Protection Act specifically.

Click on the link for guidance relating to the question under each Step.

Step 1

Is a Full-Scale PIA Necessary?

Do the Key Characteristics of the Project indicate that a Full-Scale PIA is needed?

If YES	THEN	Conduct a Full-Scale PIA
	AND	Go to Step 3

Step 2

Is a Small-Scale PIA Necessary?

If the answer to Step 1 is NO, then:
Do the Project Characteristics indicate that a Small-Scale PIA is needed?

If YES	THEN	Conduct a Small-Scale PIA
	AND	Go to Step 3

Step 3

Is Privacy Law Compliance Checking Necessary?	Are any of the activities subject to any form of privacy law?		
	If YES	THEN	Conduct a Privacy Law Compliance Check
		AND	Go to Step 4

Step 4 Is Data Protection Act Compliance Checking Necessary?	Do the activities involve the handling of 'personal data'?		
	If YES	THEN	Conduct a Data Protection Act Compliance Check

<< Preparation Up to the Contents Page

Version 1.0, 31 October 2007

Step 1 - Criteria for Full-Scale PIA

This segment provides guidance for evaluating whether a Full-Scale PIA should be conducted. The evaluation depends on sufficient information about the project having been collected during the previous step.

The evaluation process involves answering the following set of 11 questions about Key Characteristics of the project and the system that the project will deliver. These factors tend to give rise to considerable concern among at least some parts of the general public, and accordingly may be judged to represent significant project risk factors.

The answers to the questions need to be considered as a whole, in order to determine whether the overall impact, and the consequential risk, warrant investment in a Full-Scale PIA. *The questions are shown below in italics*. Guidance in relation to the interpretation of each question is provided in plain text.

Following the series of screening questions, further guidance is given on undertaking this analysis.

The 11 Questions About Key Project Characteristics

Technology

(1) Does the project apply new or additional information technologies that entail substantial potential for privacy invasiveness?

Examples of such technologies include, but are not limited to, smart cards, RFID tags, biometrics, locator technologies (including mobile phone location, applications of GPS and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic. Technologies that are inherently intrusive, and technologies that are new and sound threatening, excite considerable public concern.

Identity

*(2) Does the project involve new **identifiers**, re-use of existing identifiers, or intrusive identification, identity **authentication** or identity management processes?*

Examples of project features that are likely to trigger this criterion include a digital signature initiative, a multi-purpose identifier, interviews and the presentation of identity documents as part of a registration scheme, and an intrusive identifier such as biometrics. All schemes of this nature have considerable potential for privacy impact, and inevitably give rise to substantial public concern and hence project risk.

*(3) Might the project have the effect of denying **anonymity and pseudonymity**, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?*

Many agency functions cannot be effectively performed without access to the client's identity. On the other hand, many others do not inherently require identity, and an important aspect of privacy protection is sustaining the right to interact with organisations without declaring one's identity.

Multiple Organisations

(4) Does the project involve multiple organisations, whether they are government agencies (e.g. in 'joined-up government' initiatives) or private sector organisations (e.g. as outsourced service providers or as 'business partners')?

Schemes of this nature inevitably facilitate the breakdown of personal data silos and identity silos, and undermine the protections afforded by generic data protection legislation.

This breakdown may be desirable from the viewpoint of fraud detection and prevention, and in some cases of business process efficiency. On the other hand, data silos and identity silos are of long standing, and have in many cases been effective privacy protections. Particular care is therefore needed in relation in preparation of a business case that justifies the privacy invasions of projects involving multiple organisations. Compensatory protections should be considered.

Data

*(5) Does the project involve new or significantly changed handling of **personal data that is of particular concern to people**?*

The Data Protection Act at s.2 identifies a number of categories of 'sensitive personal data' that require special care. These include racial and ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life, offences and court proceedings.

There are many other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, particular data about people in stigmatised population-segments, and data sufficiently rich to enable identity theft.

Further important examples apply in particular circumstances. The addresses and phone-numbers of a small proportion of the population need to be suppressed, at least at particular times in their lives, because such 'persons at risk' may suffer physical harm if they are found.

*(6) Does the project involve new or significantly changed handling of a considerable **amount of personal data** about each individual in the database?*

Examples include intensive data collections such as those used in welfare administration, health care, consumer credit, and consumer marketing based on intensive profiles.

*(7) Does the project involve new or significantly changed handling of a even a modest amount of personal data about a large **number of individuals**?*

Any data collection of this nature represents a magnet for organisations and individuals seeking to locate people, or to build or enhance profiles of them.

*(8) Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of **personal data from multiple sources**?*

This is an especially important factor. Issues arise in relation to data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term.

Exemptions and Exceptions

*(9) Does the project relate to data-handling which is in any way **exempt from legislative privacy protections**?*

This may arise, for example, with law enforcement and national security information systems, and criminal intelligence systems, but also with other schemes where some or all of the generic privacy protections have been negated by legislative exemptions or exceptions.

Such schemes are especially likely to give rise to serious public concern about privacy impacts and implications, and hence to significant project risk. As a result, particular care is called for.

*(10) Does the project's justification include significant contributions to **public security***

measures?

Measures to address concerns about physical safety of the population and of critical infrastructure commonly have substantial impacts on privacy. Yet there have been tendencies in recent years to abbreviate or even avoid conventional risk assessment procedures, and instead depend on assertions of necessity as the means of justifying privacy-invasive proposals. The lack of proper justification results in tensions with privacy interests, and creates the risk of public opposition and non-adoption of the programme or scheme.

(11) Does the project involve systematic disclosure of personal data to, or access by, ***third parties that are not subject to comparable privacy regulation****?*

Disclosure may arise through various mechanisms such as sale, exchange, unprotected publication in hard-copy or electronically-accessible form, or outsourcing of aspects of the data-handling to sub-contractors.

Third parties may not be subject to comparable privacy regulation because they are not subject to, or are somehow wholly or partially exempted from, the provisions of the Data Protection Act or other relevant statutory provisions, or because they are in a foreign jurisdiction. Concern may also arise in the case of organisations within the U.K. which are subsidiaries of organisations headquartered outside the UK.

Facing Facts Early

In considering these questions, there will be a natural temptation to downplay the seriousness of the issues, in an endeavour to avoid delays and costs, or simply because familiarity makes the issues seem less threatening. It is advisable that this temptation be resisted. The Key Characteristics addressed here represent significant risk factors for the project, and the later the problems are addressed, the higher the costs will be to overcome them.

Perspectives to Consider

It is important to appreciate that the various stakeholder groups may have distinctly different perspectives on these factors. If the analysis is undertaken solely from the viewpoint of the organisation itself, it is likely that risks will be overlooked. It is therefore highly advisable that stakeholder perspectives also be borne in mind as each question is considered.

In relation to the individuals affected by the project, the focus needs to be more precise

than simply citizens or residents generally, or the population as a whole. In order to ensure a full understanding of the various segments of the population that have an interest in, or are affected by, the project, the Stakeholder Analysis that was undertaken as part of the Preparation Step may need to be refined. For example, there are often differential impacts and implications for people living in remote locations, for the educationally disadvantaged, for itinerants, for people whose first language is not English, and for ethnic and religious minorities.

Applying the Criteria

Once each of the 11 questions has been answered individually, the set of answers needs to be considered as a whole, in order to reach a conclusion as to whether a Full-Scale PIA is warranted. If so, a conclusion is also needed as to whether the scope of the PIA should be wide-ranging, or focused on particular aspects of the project.

The Full-Scale PIA is described in detail in Part II. Before proceeding to that Part, however, it is necessary to continue with Steps 3 and 4 of the Screening Process, to determine whether Compliance Checking should also be included in the project schedule.

<<== Screening Process Up to the Contents Page Screening Process ==>>

Version 1.0, 31 October 2007

Step 2 - Criteria for Small-Scale PIA

This segment provides guidance for evaluating whether a Small-Scale PIA should be conducted. The evaluation depends on sufficient information about the project having been collected when Preparing for the PIA Screening Process. If a prior PIA has been performed in relation to the existing system, this will also provide useful input to the process.

The evaluation process involves answering a set of questions about characteristics of the project or the system that the project will deliver. These are factors that tend to give rise to concern among at least some parts of the general public, and accordingly may be judged to represent project risk factors.

The questions are shown below in italics. Where guidance is provided in relation to the interpretation of a question, it is provided in plain text.

The 15 Questions About Project Characteristics

Technology

(1) Does the project involve new or inherently privacy-invasive technologies?

Examples of such technologies include, but are not limited to, smart cards, RFID tags, biometrics, locator technologies (including mobile phone location, applications of GPS and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic. Technologies that are inherently intrusive, and technologies that are new and sound threatening, excite considerable public concern, and hence represent project risk.

In order to answer this question, considerations include:

- whether all of the information technologies that are to be applied in the project are already well-understood by the public
- whether their privacy impacts are all well-understood by the organisation, and by the public
- whether there are established measures that avoid negative privacy impacts, or at least ameliorate them to the satisfaction of the people whose privacy is affected
- whether all of those measures are being applied in the design of the project

Justification

(2) Is the justification for the new data-handling unclear or unpublished?

People are generally much more accepting of measures, even measures that are somewhat privacy-intrusive, if they can see that the loss of privacy is balanced by some other benefits to themselves or society as a whole. On the other hand, vague assertions that the measures are needed 'for security reasons', or 'to prevent fraud', are much less likely to calm public disquiet.

Identity

*(3) Does the project involve **additional use of an existing identifier**?*

*(4) Does the project involve use of **a new identifier for multiple purposes**?*

*(5) Does the project involve new or substantially changed **identity authentication requirements that may be intrusive or onerous**?*

The public understands that an identifier is a means whereby an organisation collates data about an individual, and that identifiers that are used for multiple purposes enable data consolidation. They are also aware of the increasing onerous registration processes and document production requirements imposed by organisations in recent years. From the perspective of the project manager, these are warning signs of potential privacy risks.

Data

*(6) Will the project result in the handling of a significant **amount of new data** about each person, or significant change in existing data-holdings?*

*(7) Will the project result in the handling of new data about **a significant number of people**, or a significant change in the population coverage?*

*(8) Does the project involve new **linkage of personal data with data in other collections**, or significant change in data linkages?*

The degree of concern about a project is higher where data is transferred out of its original context. The term 'linkage' encompasses many kinds of activities, such as the transfer of data, the consolidation of data-holdings, the storage of identifiers used in other systems in order to facilitate the future searches of the current content of records, the act of fetching data from another location (e.g., to support so-called 'front-end verification'),

and the matching of personal data from multiple sources.

Data-Handling

*(9) Does the project involve new or changed **data collection policies or practices that may be unclear or intrusive**?*

*(10) Does the project involve new or changed **data quality assurance processes and standards** that may be unclear or unsatisfactory?*

*(11) Does the project involve new or changed **data security arrangements** that may be unclear or unsatisfactory?*

*(12) Does the project involve new or changed **data access or disclosure arrangements** that may be unclear or permissive?*

*(13) Does the project involve new or changed **data retention arrangements** that may be unclear or extensive?*

*(14) Does the project involve changing **the medium of disclosure for publicly available information** in such a way that the data becomes more readily accessible than before?*

Exemptions

*(15) Will the project give rise to new or changed **data-handling that is in any way exempt from legislative privacy protections**?*

Perspectives to Consider

As with the Criteria for Full-Scale PIA, risks may be overlooked unless these factors are considered from the various perspectives of each of the stakeholder groups, rather than just from the viewpoint of the organisation that is conducting the project.

Similarly, in relation to the individuals affected by the project, it may not be adequate to think in terms of citizens or residents generally, or the population as a whole. In order to ensure a full understanding of the various segments of the population that have an interest in, or are affected by, the project, the Stakeholder Analysis that was undertaken as part of the Preparation Step may need to be refined. For example, there are often differential impacts and implications for people living in remote locations, for the educationally disadvantaged, for itinerants, for people whose first language is not English, and for

ethnic and religious minorities.

Applying the Criteria

Where questions are answered in the affirmative, consideration should be given to the extent of the privacy impact and the resulting project risk. The greater the significance, the more likely that a Small-Scale PIA is warranted.

If only one or two aspects give rise to privacy concerns, the PIA process should be designed to focus on them. If, on the other hand, multiple questions are answered in the affirmative, a more comprehensive assessment is appropriate.

The Small-Scale PIA is described in Part III. Before proceeding to that Part, however, it is necessary to continue with Steps 3 and 4 of the Screening Process, to determine whether Compliance Checking should also be included in the project schedule.

<<== Screening Process Up to the Contents Page Screening Process ==>>

Version 1.0, 31 October 2007

Step 3 - Criteria for Privacy Law Compliance Checks

Senior executives of government agencies and company directors must ensure that the operations for which they are responsible comply with all relevant laws. The purpose of this segment of the Handbook is to assist organisations comply with privacy-related laws. The services of a legal professional with relevant expertise may be needed for this exercise.

If any of the following questions are answered "Yes", then a Privacy Law Compliance Check should be conducted:

1. Does the project involve any activities (including any data handling), that are subject to **privacy or related provisions of any statute or secondary legislation, other than the Data Protection Act**?

In particular, the following laws and secondary legislation should be considered, but the list may not be exhaustive:

- the Human Rights Act, in particular Schedule 1, Article 8 (Right to Respect for Private and Family Life) and Article 14 (Prohibition of Discrimination)
- the Regulation of Investigatory Powers Act 2000 and Lawful Business Practice Regulations 2000
- the Privacy and Electronic Communications Regulations 2003
- the Data Retention (EC Directive) Regulations 2007
- in the case of government agencies, the statutes under which the agency or programme operates
- statutes that impose regulatory conditions on the manner in which the organisation operates
- sectoral legislation, e.g. Financial Services and Markets Act 2000
- Statutory Codes, e.g. the Information Commissioner's CCTV Code of Practice (2000)

Where projects are cross-jurisdictional the law of more than one country may be involved. For example, organisations dealing with the US may need to be aware of the provisions of legislation such as Gramm-Leach-Bliley Financial Services Modernization Act of 1999, the Health Insurance Portability and Accountability Act of 1996, the Fair Credit Reporting Act and Fair and Accurate Credit Transactions Act 2003, the Sarbanes-Oxley Act of 2002, as well as State laws such as California's "Personal Information Security" and "Security Breach Notice" laws.

2. Does the project involve any activities (including any data handling) that are subject to **common law constraints relevant to privacy**?

In particular, the following should be considered:

- confidential data relating to a person, as that term would be understood under the common law of confidence
- the tort of privacy, which may be emergent in case law

3. Does the project involve any activities (including any data handling) that are subject to **less formal requirements relevant to privacy**?

In particular, the following should be considered:

- industry standards, e.g. the BS ISO/IEC 17799:2005 Information Security Standard
- industry codes, e.g. the NHS Code of Practice on Confidentiality

Privacy Law Compliance Checking is described in Part IV of this Handbook. Before proceeding to that Part, however, organisations must continue with Step 4 of the Screening Process, to determine whether Data Protection Act Compliance Checking also needs to be included in the project schedule. Note that Compliance Checking activities are usually conducted reasonably late in the overall project schedule, once detailed information about business processes and business rules is available.

<<== Screening Process Up to the Contents Page Screening Process ==>>

Version 1.0, 31 October 2007

Step 4 - Criteria for Data Protection Act Compliance Checks

Senior executives of government agencies and company directors must ensure that the operations for which they are responsible comply with all relevant laws. The purpose of this segment of the Handbook is to assist organisations in that endeavour.

The services of a professional lawyer with relevant expertise may be needed for this exercise.

If either of the following questions is answered, "Yes", then a Data Protection Act Compliance Check should be conducted:

(1) Does the project involve the handling of any data that is **personal data, as that term is used in the Data Protection Act**?

'Personal data' means data which relate to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (Data Protection Act, s.1).

(2) Even if the organisation claims that the project is covered by one of the limited forms of exemption and exception available under the Act, **does the organisation have a policy position of taking the Data Protection Principles into account**?

Data Protection Act Compliance Checking is described in Part V. Before proceeding to that Part, however, it is advisable to return to the Screening Process and review the outcomes of the four steps.

Note that, where a PIA is needed it should be commenced at an early stage of the overall project, whereas Compliance Checking activities are usually conducted only once a fairly mature stage of business process design has been reached.

[<<== Screening Process](#) [Up to the Contents Page](#) [Screening Process ==>>](#)

Version 1.0, 31 October 2007

Full-Scale PIA - Introduction

Many aspects of business and government operations have only modest privacy implications. Yet a privacy disaster can damage a multi-million pound project in a short time. So organisations that interact with people need to be prepared for privacy problems.

This segment provides access to introductory material about ideas underlying Privacy Impact Assessments. It is anticipated that for many readers of this document, the introductory material will be superfluous. However, it is likely that some members of a project or PIA team who are unfamiliar with privacy concepts will benefit from this material.

Access is provided as a matter of completeness, and so that a common reference-point is available for discussions between organisations and the Information Commissioner's Office.

The remainder of this segment briefly highlights questions that may arise when an organisation is preparing to conduct a Full-Scale PIA, and provides access to introductory material on each topic.

To read general background information relating to the following questions, click on the questions below:

- What is 'Privacy'?
- How is Privacy Protected?
- Why is Privacy Important?
- Why have a Privacy Strategy?

Many readers of this Handbook will want to move directly to the following key questions.

---

(1) Benefits of a PIA

Even though the Screening Process may have indicated that a Full-Scale PIA is warranted, there may be some lack of clarity about why a PIA offers benefits to the organisation.

Background information is provided to assist in considering the question, Why do a Privacy Impact Assessment?.

(2) Triggers for a PIA

There are various stimuli that may be the immediate cause of a PIA being conducted.

Background information is provided to assist in considering the question, What triggers a PIA?

(3) Timing Considerations

An organisation may want to know the stage of a project's life-cycle at which it is appropriate to commence a PIA. Generally, 'the earlier the better' is good advice, because that prevents small problems growing into bigger ones.

Background information is provided to assist in considering the question, When to do a PIA?

(4) Distinguishing PIAs from Other Privacy-Related Processes

An organisation may want to understand how a PIA relates to other processes that appear to have similarities.

Background information is provided to assist in clarifying What is and is not a PIA?

<<== Screening Process Up to the Contents Page PIA Framework ==>>

Version 1.0, 31 October 2007

Full-Scale PIA – Background Information

This segment provides answers to some questions that an organisation about to conduct a PIA may pose. The topics addressed are:

Why do a Privacy Impact Assessment?

Public trust in its institutions is generally felt to be in decline, with people tending to feel distanced, alienated and even disengaged. The reputations of corporations and government agencies alike need to be sustained. This implies that these organisations need to act responsibly in relation to key public policy issues like privacy, and to be seen to be acting responsibly.

There are much more concrete and specific reasons to do a PIA. Organisations take considerable care to manage a variety of risks, including competitive manoeuvres by other corporations, natural disasters, environmental contamination, cyber-attacks, and the risk of embarrassment to executives and Ministers. 'Issues management' has emerged as a common activity based on contingency planning.

For many organisations, privacy now represents a cluster of risks that need to be as professionally managed as other categories of risk. Organisations that handle personal data need to monitor their ongoing operations, whether their interactions are with clients, employees, or the public in general. But of even greater significance are new initiatives, especially ones that deploy advanced technologies which are ill-understood, and which harbour both new opportunities and new threats.

In summary, the reasons an organisation undertakes a PIA are as follows:

1. The Avoidance of Loss of Trust and Reputation
2. The Identification and Management of Risks
3. Cost Avoidance
4. Meeting and Exceeding Legal Requirements

1. The Avoidance of Loss of Trust and Reputation

Customers value privacy. A PIA is a means of ensuring that systems are not deployed with privacy flaws that will attract the attention of the media, competitors, public interest advocacy groups or regulators, or give rise to concerns among customers.

2. The Identification and Management of Risks

The kinds of projects that give rise to privacy concerns generally involve a considerable amount of effort and investment. Company Directors and the senior executives of government agencies are responsible for ensuring that risks are identified, assessed and managed. That responsibility extends to checking whether privacy issues exist. If that is the case, then the risks need to be assessed, and a risk management plan needs to be devised and implemented. In short, at senior levels of organisations, a PIA is part of good governance and good business practice.

At project management levels, a PIA is a means of addressing project risk. Risk management has considerably broader scope than privacy alone; so organisations may find it appropriate to plan a PIA within the context of risk management. Apart from business publications and textbooks on the subject, a formal Standard exists: ISO/IEC 27001:2005 (formerly BS 7799-2:2002).

One small but important part of privacy protection is information security, and some aspects of a PIA need to reflect the accumulated body of knowledge in that area. Once again, this is well-supported by text-books, business publications, and formal Standards (e.g. ISO/IEC 27002:2005, formerly ISO/IEC 17799:2005).

3. Cost Avoidance

By performing a PIA early in a project, an organisation avoids problems being discovered at a later stage, when changes and the 'retrofitting' of features are much more expensive. Of course, articulation of a project's objectives, the organisation's requirements and the justifications for particular design features all have important benefits for project management generally, rather than exclusively as part of privacy impact assessment.

A further benefit of building privacy-sensitivity into the design from the outset is that it provides a foundation for a flexible and adaptable system, reducing the cost of future changes and ensuring a longer life for the application.

4. Meeting and Exceeding Legal Requirements

The Data Protection Act already stipulates eight Data Protection Principles, but these only address **the informational aspect of privacy**.

There are other dimensions, and with modern business practices and technologies some or all of these may come into play as well:

- **privacy of the person**. Examples of the kinds of issues that arise are bodily intrusions (e.g., demands for bodily fluids, or for submission to biometric measurement), and threats to personal safety. Physical safety is of particular concern to persons at risk)
- **privacy of behaviour**. Common issues in this area include CCTV, substance-abuse testing, and the surveillance of people's physical and electronic activities
- **privacy of communications**. This relates to such issues as the monitoring of conversations, the interception of messages, traffic analysis and access to recorded and stored messages

Where the project affects these dimensions of privacy, and the public may be concerned about it, it will be to the organisation's advantage to define the scope of the PIA to extend beyond information privacy.

What Triggers a PIA?

The need for a Full-Scale PIA may be triggered in several ways. For example:

- a PIA may be a requirement in **law**. At present, there is no laws requiring a PIA in the U.K.
- a PIA may be a requirement of **Government organisational policy**. For example, it might be stipulated that one be performed prior to approval of the detailed design phase of a particular project or a particular category of projects, or of funding for product acquisition or system development work
- the organisation conducting a project, or some other participating organisation, may appreciate that a proposal has **broad and significant implications** that should be the subject of investigation. The motivation of the organisation may be public policy, business ethics / corporate citizenship, or a desire to achieve public and consumer confidence and hence ensure return on investment
- there may be **existing public concerns** about the particular proposal or about proposals of that kind, perhaps arising from media-fanned rumours or a previous media event

The most common trigger for a PIA, however, is that the lead organisation, or perhaps some other participating organisation, is concerned that a proposal may later give rise to public concerns, which would represent significant **project risk**. To address that risk, a risk management plan is called for.

When to do a PIA?

Making any kind of change to specifications, and fixing any kind of error, requires re-work and retro-fitting of features. That incurs delays and costs, and because it is error-prone it risks even more re-work afterwards. The cost of making changes increases rapidly the later in the project they are made. Therefore, privacy-protective features should be designed into a system, rather than grafted onto it later.

In order to achieve that, the following guidelines are suggested:

- **start early** to ensure that project risks are identified and appreciated before the problems become embedded in the design
- if possible, commence a PIA **as part of the Project Initiation Phase** (or its equivalent in whichever project method the organisation uses)
- if the project is already under way, start 'now', so that any major issues are identified with the minimum possible delay

A PIA can be conceived and conducted as a one-time activity. If so, it takes into account the information available about the project at the time, and feeds ideas forward into the design. But it cannot reflect information, often of a more detailed nature, that becomes available at a later stage.

A PIA can be conceived and conducted as a stand-alone activity, alongside the project and separate from it. This may, however, create distance between the staff conducting the PIA and the project team, and resistance to insights arising from the PIA by designers and other project team members.

Particularly in major projects, the most beneficial and cost-effective approach may be to conceive of the PIA as:

- **a cyclical process**
- **linked to the project's own life-cycle**
- **re-visited in each new project phase**

Each iteration can then take account of both the more detailed specifications that are currently available for the scheme, and the outcomes of previous phases of the PIA. More specifically, later iterations can correspond with the later phases of the project (e.g. Requirements Analysis, Logical Design, Physical Design, Construction, Integration and Deployment of the new system, or their equivalents in whichever project method the organisation uses).

Finally, the organisation may conduct a more general risk assessment as part of the project, or may have generic risk management processes in place. If so, consideration should be given to undertaking the PIA **within the context of a broader risk management framework**.

What is and is not a PIA?

Privacy Impact Assessment is usefully defined as a process whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and a constructive search is undertaken for ways to avoid, minimise or at least ameliorate privacy concerns.

A PIA is a tool for executives and management. The organisation needs to know what the problems are, and how to devise solutions to them. In particular, the organisation needs to ensure that the people affected by the initiative are comfortable with the shape that the new initiative is taking. Measures are needed to ensure that the media doesn't misunderstand or misrepresent the initiative in ways that could harm the undertaking. To achieve those ends, a PIA adopts a risk management approach to privacy issues.

As a management tool, a PIA is most effective if it is undertaken in a systematic manner, is commenced at an early stage in the process, and is oriented towards process rather than outputs.

Although the PIA process takes the Data Protection Act and other relevant laws into account, it does not focus on them. A complementary process is needed to ensure that the project is legally compliant. That process can begin early, but cannot be finalised until late in the project life-cycle, when the design is complete. Separate guidance is provided in this Handbook relating to the conduct of **Compliance Checking**. The cost and delay involved in Compliance Checking need not be great, because the process draws heavily on work undertaken during the course of a PIA.

Finally, a PIA needs to be distinguished from **Privacy Audit**. An audit is undertaken on a project that has already been implemented. An audit is valuable in that it either confirms that privacy undertakings and/or privacy law are being complied with, or highlights problems that need to be addressed. To the extent that it uncovers problems, however, they are likely to be expensive to address and may disturb the conduct of the organisation's business. A PIA aims to prevent problems arising, and hence avoid subsequent expense and disruption.

<<== Introduction Up to the Contents Page Framework ==>>

Version 1.0, 31 October 2007

Full-Scale PIA – Framework

The term 'framework' is used here to refer to the measures that need to be taken at senior executive level prior to the commencement of the PIA, in order to ensure that the process is properly structured.

Relationship to the Project as a Whole

A PIA is likely to be of greatest benefit to the organisation if it is started early, and conducted in conjunction with the life-cycle of the project as a whole. Therefore, the PIA should be initiated at the time of project conception, and either sustained for the period of the project as a whole, or activated at the appropriate stage in each Phase of the overall project life-cycle.

A PIA is part of the overall risk assessment and risk management process. Most organisations are therefore likely to find it beneficial to make clear the relationship between the PIA and such other routine risk assessment and mitigation activities they have in place.

Stakeholder Involvement

A major project risk is that participants may not be fully committed, or may later withdraw from participation in the project. In order to ensure that this risk is managed, it is advisable that a stakeholder analysis be conducted at the outset, and that the governance arrangements and the process adopted ensure appropriate involvement of key stakeholders. Further discussion is provided in relation to these matters.

Governance

At the level of the project as a whole, and particularly if it is a large or complex project, the organisation should formalise the **governance structure and processes** including those for the PIA. It may be advantageous for these to extend beyond the boundaries of the organisation that is conducting the project, to encompass key stakeholders. In cases with substantial privacy implications, it is advisable to encompass all stakeholders.

A common approach is to establish a Project Steering Committee (a group that has directive powers), or a Project Advisory Committee or Project Reference or Consultative Group (a representative group whose function is to discuss, advise and assist, but which has no formal powers to direct the process).

Similar consideration should be given to governance structure and processes in relation to the conduct of the PIA, within the overall project. This might be achieved, for example, by establishing a Privacy Sub-Committee, or a PIA Advisory, Reference or Consultative Group. This Handbook uses the term PIA Consultative Group (PCG). The title of any such body, however, is the choice of the organisation concerned and should be consistent with terms used for similar groups.

Whether or not formal governance arrangements are adopted, it is generally advisable for **Terms of Reference for the PIA** to be prepared and agreed. Important elements of the Terms of Reference include:

- the functions to be performed
- the deliverables
- the desired outcomes
- the scope of the assessment
- roles and responsibilities of various parties involved in the PIA

Further discussion is provided in relation to these matters.

PIA Team Formation

The conduct of the PIA requires strong understanding of the project itself, knowledge of privacy, and expertise in the performance of risk assessments generally and privacy impact assessments in particular.

Some organisations have some or all of the necessary expertise available in-house. Others find it appropriate to use external resources for some of the tasks, particularly if they have limited prior or recent experience in conducting PIAs. Further discussion is provided in relation to these matters.

Resourcing

Appropriate resources need to be located, and assigned to the process. Further discussion is provided in relation to these matters.

Role of the Information Commissioner

The Information Commissioner's Office provides information to support the performance of PIAs – in particular through publication of this Handbook. In addition, the ICO may be available for consultation on particular projects; but it does not participate directly in any PIA process, and is under no circumstances responsible for the conduct of any PIA.

In the first instance, contact should be made with the Deputy Commissioner, Data

Protection, via the telephone, email or postal address on the ICO's 'Contact Us' Web-Page.

<<== Introduction Up to the Contents Page Overview ==>>

Version 1.0, 31 October 2007

Full-Scale PIA – Framework Details

This segment provides further discussion about aspects of the framework that senior executives create in order to ensure that a PIA is conducted effectively. It addresses the following topics:

Stakeholder Involvement

Organisations

The term 'stakeholder' is useful as a collective word for the various groups and individuals who have a significant interest in the project and its outcomes, because they are participating in it, or may be affected by it.

The first consideration is **the organisation itself**. In small organisations, the PIA team may be able to appreciate all aspects of the interests of the organisation. In large organisations, on the other hand, there are likely to be multiple units that have perspectives on the project and that will wish to be involved.

PIAs also need to actively involve representatives from relevant segments of **other participating organisations**. These may be 'partner' organisations, or organisations that will provide or receive data. In some cases, organisations that provide services to support the system (e.g., as outsourced service providers) may have a role that is so significant that they may be best treated as stakeholders rather than merely as sub-contractors. Where new technology is involved, the same may be true for technology providers.

Individuals

Effective risk assessment can only be performed by gaining insight into the reactions of **the individuals affected by the project**. In some cases, this may be gained by means of public meetings, or through focus groups. However, it is often more effective, and more cost-effective, to gain those insights through consultations with **public interest**

associations, sometimes called non-government organisations (NGOs) or civil society organisations. These either represent the relevant public, or conduct advocacy on their behalf.

When devising consultation processes with these categories of stakeholder, it is seldom adequate to think in terms of the 'general public' – that term is imprecise. People are affected in various ways, depending on the system's features, and their own circumstances. When conducting PIAs, organisations will generally find it to be of value to distinguish, and focus on, **relevant customer segments**.

A further category of stakeholder is **organisations that perform some form of regulatory function**. In additional to public bodies such as the Information Commissioner's Office and the Financial Services Authority, this may include industry associations.

Stakeholder analysis should be conducted at an early stage to ensure that the Governance Arrangements are appropriate.

Governance Arrangements

Executives and senior managers should control and be committed to the PIA process.

Disgruntled stakeholders represent a risk to project success and return on project investment. Stakeholders should be provided sufficient information and the opportunity to convey their perspectives and their concerns. The organisation should attempt to reflect stakeholder views in the project design.

There are several alternative ways in which the project governance structure and processes can be extended to encompass all stakeholders.

For large projects, it is conventional to establish an oversight group. A **Project Steering Committee** normally has the power to give directions to the project, whereas an **Advisory, Reference or Consultative Group** does not.

If there are multiple stakeholders with an interest in the privacy aspects of the project, there may be benefits in creating a Privacy Sub-Committee, or PIA Advisory, Reference or Consultative Group. In this Handbook, the term **PIA Consultative Group (PCG)** is used. For some projects, it may be desirable to give the Committee or Group broader considerations, such as a Public Policy or Regulatory Affairs. If such an arrangement is created, effective links should be established between the two levels of committee.

With smaller projects, such arrangements are not practical, but measures are needed that achieve clear communications among the three groups:

- senior management
- the project team
- representatives of, and advocates for, the various stakeholders

Conventionally, a Terms of Reference document would document the governance structure and processes, including the nature of the delegation of responsibility and authority provided to the person(s) or team (s) who are involved in the PIA.

It is generally not recommended that the Terms of Reference be too prescriptive in relation to the process to be used. Because some flexibility is needed, processes are best determined by the responsible staff members. The Terms of Reference should, however, include:

- clear definition of the **functions** to be performed
- specification of the **scope** of the assessment to be undertaken
- a statement of the desired **outcomes**
- a statement of the **deliverables** expected

The scope of the assessment requires particular attention, from several perspectives.

(1) The Breadth of Risks

A PIA is an important element within the organisation's risk management strategy. There may be benefits in defining at the outset the PIA's relationship with other aspects of risk assessment.

(2) The Breadth of Applicability

There are circumstances under which it may be sensible and economic to focus on something other than a single project. Examples include:

- **commercial software packages**. A software development company might commission an independent PIA for a packaged application, taking into account one or more typical deployments or implementations
- **common functions in government**. A group of government agencies might commission a generic PIA in an area such as identity authentication or identity management, in order to provide a platform and template on which individual agencies can build
- **common functions in business**. An industry group might commission a PIA in relation to a common application across an industry sector or segment. Examples

include financial applications such as credit reporting, and electronic health applications

(3) The Breadth of Privacy and Social Impacts

A significant decision in relation to scope is the sense in which 'privacy' is to be understood. In many cases, the primary focus will fall on **information privacy**. The Principles embodied in the Data Protection Act provide guidance in this area. However, it will generally be advisable for the PIA to consider whether any broader aspects are relevant, such as:

- processes relating to identifiers and identity management that may be perceived by people to be intrusive or onerous
- denial of anonymity and pseudonymity, particularly where they were previously available
- negative effects on individuals who exercise their privacy rights
- use of personal information whose unauthorised disclosure could give rise to threats to the person's physical safety
- use of personal information that some people may regard as being of particular concern
- long-term retention of personal information

In some cases, the best interests of the organisation will be served by defining the scope much more broadly than information privacy alone. Modern business processes and technologies are having impacts on other aspects of privacy. Examples include:

- **privacy of the physical person** (e.g. the processes involved in gathering biometrics or body fluid samples from staff or customers)
- **privacy of personal behaviour** (e.g. audio and visual monitoring, even if no records are created)
- **privacy of personal communications** (e.g. monitoring of staff emails and chat-traffic in the workplace, or using employer-provided infrastructure whether during working-time hours or not)

Some major projects give rise to **even broader social and public policy issues**, which the organisation may find convenient to consider within the same risk assessment process as privacy. Examples include:

- the allocation of effort, costs and risks. Further discussion is provided
- the availability, quality, accessibility and equity of services. Further discussion is provided
- the accessibility of information. This is a requirement in government under the Freedom of Information Act, but also in the private sector, although in a much

more limited form, under s.7 of the Data Protection Act
- the human rights of employees, contractors, consumers and citizens. At the most abstract level, there may be relevant constitutional provisions, and there are statutory provisions under the Human Rights Act. There may also be relevant provisions in occupational health and safety law, industrial law, and the common law more generally

---

PIA Team Formation

Because of the diversity of expertise and interests involved, it is unusual for a PIA to be performed by a single person. More commonly, a small PIA Team is formed, who together have expertise in a number of areas. Team members' involvement is likely to extend over a period of time, but need be intensive only for relatively brief periods.

Depending on the context, knowledge and expertise of the following kinds are generally needed:

- understanding of the business area that the project addresses
- knowledge of the overall project
- knowledge of the relevant stakeholders and customer segments
- knowledge about privacy
- expertise in project management
- expertise in records management, information management and data management
- expertise in relevant technologies
- expertise in information security processes and technologies
- knowledge about privacy law
- expertise in framing, planning and conducting a PIA
- knowledge of appropriate representatives of and advocates for the stakeholder groups and consultation techniques

An organisation may have sufficient expertise to perform a PIA entirely in-house. In organisations with a strong internal privacy culture, the staff responsible for the project may have the capabilities already, particularly if they are supported by an experienced corporate Privacy Officer.

In other organisations, project teams may have very strong professional capabilities and confidence, and may tend to resist input, even if concerns are expressed by stakeholders about some of its features. If that risk exists, it may be necessary to assign a privacy specialist to work within the project on a periodic, part-time, or even full-time basis. The authority of this individual should be clearly defined and communicated.

In a number of circumstances, there are benefits in acquiring specialist support from outside the organisation. One reason is to provide access to experience with the performance of PIAs generally or PIAs in the particular context. This may be useful because of the kinds of data involved, the kinds of data subjects, or the technologies.

Another reason for including outsiders in the Team is to provide an external perspective. People from outside the organisation are likely to deliver insights that are difficult for employees to achieve because of their day-to-day responsibilities or organisational loyalties.

Where an external consultant is selected to perform a considerable proportion of the work involved in the PIA, it should be independent (i.e., the consultant should not have an interest in particular solutions such as software applications). In addition, the organisation must always maintain responsibility for the PIA. The organisation will benefit from having direct access to the insights that consultations and analysis lead to, rather than having them filtered, or worse still captured by the consultant.

Resourcing

Appropriate **resources** need to be assigned to enable effective and efficient performance of the PIA.

One aspect of resource allocation relates to the members of the PIA Team itself. The senior executive with overall responsibility for the project may need to temporarily reallocate responsibilities or other support to allow staff to devote sufficient time to conduct the PIA thoroughly.

In addition, the time of staff outside the PIA Team needs to be considered and committed. The categories of employees who need to be involved may come from executive, managerial and operational levels, and include policy, technical, business process design and legal staff.

<<== Framework Up to the Contents Page Overview ==>>

Version 1, 31 October 2007

Full-Scale PIA – Overview

Privacy Impact Assessment (PIA) is usefully defined as a process whereby the potential privacy impacts and implications of a project are identified and examined from the perspectives of all stakeholders, and a constructive search is undertaken for ways to avoid, minimise or at least ameliorate them.

Projects with substantial privacy impacts and implications require a comprehensive PIA process, to ensure that the issues are appreciated and addressed, and risks are managed. A Full-Scale PIA should be a disciplined process. It involves deep analysis of technologies and business processes and consultation with stakeholders. Its outcomes are likely to affect the project conception, process and design features.

The term **'project'** is used in this Handbook to refer to whatever the activity or function is that the organisation is assessing. It may be, for example, a project to develop a 'system', a 'database', a 'program', an 'application', a 'service' or a 'scheme', or an enhancement to any of the above, or an 'initiative', a 'proposal' or a 'review', or even draft legislation.

Throughout this Handbook, the term **'the organisation'** is used. This is intended to refer to the company or government agency that is primarily responsible for the project as a whole, and that may be seen as sponsoring the activity. Other organisations that are involved in some way are referred to as **'participating organisations'**. In the case of very large projects in which several major organisations are heavily involved in partnership or joint venture, it may be appropriate to interpret 'the organisation' to refer to that one of them that performs the function of **'lead organisation'**.

Experience has shown that the most effective approach to **the timing of a PIA** is to:

- commence it early in the life-cycle of the overall project
- run it in conjunction with the life-cycle of the overall project
- perform it progressively and in an iterative fashion

This approach ensures that privacy issues are identified and addressed early, rather than becoming embedded and thereby turning into major risks to the project's objectives and budget.

To be effective, a PIA has a number of **general features**:

- it is primarily about process, and only secondarily about producing a report
- the process is considerably broader than just an audit of compliance with existing

privacy-related laws. The latter is the function of a complementary Privacy Law Compliance Study. Guidance in relation to that process is provided in another segment of this Handbook
- the process is inclusive and participative, or at least consultative

The **outcomes of an effective PIA process** are:

- the identification of the project's privacy impacts
- appreciation of those impacts from the perspectives of all stakeholders
- an understanding of the acceptability of the project and its features by the organisations and people that will be affected by it
- identification and assessment of less privacy-invasive alternatives
- identification of ways in which negative impacts on privacy can be avoided
- identification of ways to ameliorate negative impacts on privacy
- where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them
- documentation and publication of the outcomes

A PIA necessarily identifies and involves **project stakeholders**. An effective PIA does not arbitrarily limit the notion of 'stakeholder' to organisations participating in the project, but is fully inclusive. Stakeholder categories include:

- the organisation itself (generally including various sub-units with somewhat different perspectives and requirements)
- other participating organisations (in some cases possibly also including sub-units with somewhat different perspectives and requirements)
- the organisations and individuals intended to benefit from the project and/or affected by it. These are usually from various 'market segments', which benefit or are affected in different ways. It may require creativity or the use of proxies such as existing public interest groups and privacy advocates to obtain the views of this type of stakeholder.

[<<== Framework](#) [Up to the Contents Page](#) [Planning ==>>](#)

Version 1.0, 31 October 2007

Full-Scale PIA – Planning the Process

Once the framework for the PIA has been established, the conduct of the activity needs to be planned. An experienced manager may be able to do this with a minimum of formality. There are benefits, however, in investing some effort at the outset, in order to ensure the smooth performance of the work.

This segment offers discussion about the following key aspects of a Full-Scale PIA:

The Responsibility for a PIA

The organisation that is the primary driver of the project must take responsibility for the PIA. The organisation will gain the greatest benefit from the PIA, and it will suffer the most if a PIA is not performed, or is poorly performed.

A PIA has strategic significance, and therefore, direct responsibility for the PIA must be assumed by a **senior executive**. PIAs are conducted when the screening process identifies potential privacy threats or negative impact on individuals. These amount to risks to the project's success and return on investment, and to the proper use of corporate or public funds.

In delegating that responsibility to a suitable manager, the executive has two alternatives: an appointment within the overall project-team, or someone who is outside the project.

The delegation can be provided to a senior member of the project team as the **privacy lead or project privacy manager**. The privacy lead should be a person with high standing within the team. The person must have a clear mandate to actively participate in the project design decisions, to ensure that those decisions reflect the outcomes from the PIA process. The privacy lead should also provide ongoing advice and feedback to the responsible senior executive.

However, **all members of the project-team** need to have an appreciation of privacy and the design's impacts on it. This is most likely to be the case when privacy has senior

executive support, and the organisation has a culture of privacy-sensitivity. Further guidance is provided on how organisations may achieve a privacy-friendly climate.

If the responsible executive delegates responsibility for the PIA to someone outside the project team, that person is likely to participate considerably less in the PIA process. It may also be more difficult for the privacy lead to ensure a balanced appreciation of the perspectives of all stakeholders and to assimilate the information arising from the process. There is a reasonable likelihood that the project team might resist the conclusions and recommendations that arise from the PIA process. The management of privacy-related project risks may therefore be less effective than would be the case if the project-team as a whole participates in developing the privacy solutions.

The Objectives of a PIA

Through the adoption of a positive approach, a PIA becomes an opportunity for the organisation to ensure that its business processes are **aligned with its mission and its overall strategy**. This section considers the range of Objectives that may be relevant.

Organisations in both the public and private sectors should take into account the 'big picture' questions. These are about the relationships between people and the institutions that deliver services to them, and the varying degrees of control that organisations exercise over individuals. The enormous increases in the collection, storage, use and disclosure of personal data, and the imposition of many intrusive technologies, have eroded the public's trust of organisations. All organisations have a responsibility to recognise that problem.

Primarily, however, PIA is a form of **risk management**. It enables avoidance of project risks such as:

- **the need for system re-design or feature retrofit**, late in the development stage, and at considerable expense
- **loss of public credibility** as a result of perceived harm to privacy or a failure to meet expectations with regard to the protection of personal information
- **retrospective imposition of regulatory conditions** as a response to public concerns, with the inevitable cost that entails
- **low adoption** rates (or poor participation in the implemented scheme) due to a perception of the scheme as a whole, or particular features of its design, as being inappropriate
- **collapse of the project, or even of the completed system**, as a result of adverse publicity and/or withdrawal of support by the organisation or one or more key participating organisations

- **compliance failure**, through breach of the letter or the spirit of privacy law (with attendant legal consequences)

When planning a PIA, the responsible executive within the organisation should ensure that all of these possibilities have been considered, and that the organisation seeks an appropriate set of outcomes from the investment.

At an **executive** level, the following are suggested as appropriate **objectives** for a PIA:

1. ensure effective management of the privacy impacts arising from the project
2. ensure effective management of the project risks arising from the project's privacy impacts
3. avoid expensive re-work and retro-fitting of features, by discovering issues early, devising solutions at an early stage in the project life-cycle, and ensuring that they are implemented

In order to achieve those objectives, the following are suggested as **operational aims** for a PIA:

1. clearly define:
    - the organisation's business needs
    - the design, including:
        - the technical elements
        - the relevant data flows
        - the relevant business processes
        - the criteria used in making decisions about people
    - the features of the design that have potential privacy impacts and implications
    - the rationale underlying those features
    - the business case that justifies:
        - the design as a whole
        - the design features with potential privacy impacts and implications
2. identify:
    - the project's first-order privacy impacts (i.e., those that are direct and immediate)
    - the project's second-order privacy implications (i.e., those that are indirect, deferred, contingent or speculative). An example that is easily over-looked is 'function creep', which refers to the application of personal data to additional purposes that were not originally envisaged

- identify the stakeholder groups, including all segments of the population that may be affected by the project and what it delivers

- identify and involve representative and advocacy organisations for the relevant stakeholder groups
- enable the representative and advocacy organisations to:
    - achieve an understanding of the project
    - assess it from their own perspectives
    - have their perspectives understood by other stakeholders
    - understand the perspectives of other stakeholders
    - have their perspectives reflected in the project design
- assure all stakeholder groups that their perspectives have been taken into account
- enable the design to work towards maximisation of the positive impacts and implications of the project
- enable negative impacts and implications of the project to be avoided, or at least ameliorated
- avoid the emergence of new requirements at a late stage in the design process (or, worse still, during construction, deployment, or even operation), when modifications are much more expensive, slower and risk-prone
- be publicly credible, in order to support public confidence in the project, and minimise the risk of the project encountering difficulties with public acceptance
- achieve awareness-raising and education for:
    - executives, managers and operational staff of the organisation and other participating organisations
    - representatives and advocates of stakeholders
    - relevant segments of the public
- pre-empt any possible misinformation campaigns
- commit stakeholder representatives and advocates to support the project, in order to avoid the emergence of opposition at a late and expensive stage in the design process

---

The PIA Project Plan

A Full-Scale PIA is sufficiently important and complex that it may itself warrant a formal project plan.

This segment is intended to assist organisations devise and implement such a plan. More detailed guidance in relation to the **Phases, Tasks and Deliverables** involved in a PIA is provided in the following segments. In addition, the ICO may be available to discuss issues and provide general advice on the project plan, although it retains independence from the PIA project itself.

An organisation may have all relevant expertise in-house, in which case it may have its **own staff** perform the PIA. Many organisations, however, can benefit from the use of **specialist consultant support**, in order to draw in expertise, and provide access to

external perspectives. Where the project team comprises both internal and external resources, the organisation needs to retain responsibility and exercise control. Otherwise, key information will be filtered rather than being assimilated by the organisation, and the project risks will not be adequately addressed.

In either case, however, the organisation must take direct **responsibility** for the PIA team's work, rather than delegating it away.

Other **involved organisations** are likely to wish to participate in, and make contributions to, the development of the project plan. In many cases, the most appropriate approach to project **governance** will involve the formation of a Project Steering Committee.

[<<== Overview](#) [Up to the Contents Page](#) [Process ==>>](#)

Version 1.0, 31 October 2007

Full-Scale PIA – Conducting The Process

It is highly advantageous to apply conventional project management techniques to the process of assessing privacy impact. This includes the definition of Phases, Tasks within Phases, and Deliverables.

This segment provides an outline description of a suggested set of Phases, together with links to more detailed Guidelines concerning the Tasks and Deliverables that may be appropriate.

The terms used here (such as 'Preliminary Phase') are intended to be descriptive and are not in themselves of any great significance. Organisations that apply these Guidelines are encouraged use terms that are consistent with their own internal standards, policies and practices.

The following Phases are suggested:

[IN THE FINAL, PUBLISHED VERSION, IT IS ENVISAGED THAT THE TEXT DESCRIBING THE PHASES AND DELIVERABLES WILL BE ACCOMPANIED BY A DIAGRAMMATIC DEPICTION OF THE FLOW AND OUTPUTS]

1. Preliminary Phase

The purpose of this Phase is to ensure that a firm basis is established for the PIA to be conducted effectively and efficiently. The suggested Deliverables are a Project Plan and a Project Background Paper.

Guidance is available to assist in specifying the Tasks and Deliverables involved in this Phase.

2. Preparatory Phase

The purpose of this Phase is to make the arrangements needed to enable the critical Phase 3 to run smoothly. The suggested Deliverables are a Stakeholder Analysis, a Consultation Strategy and Plan, and establishment of a PIA Consultative Group (PCG).

Guidance is available to assist in specifying the Tasks and Deliverables involved in this Phase.

3. Consultation and Analysis Phase(s)

With the framework in place, this Phase focuses on consultations with stakeholders, risk analysis, the articulation of problems, and the search for constructive solutions.

It is likely that some activities will need to be performed more than once (e.g., by calling more than one meeting of the PCG).

The greatest value to the organisation arises where the PIA is commenced at an early stage in the overall project life-cycle. In that case, it may be advisable to define multiple Consultation and Analysis Phases, to parallel the Conception, Analysis, Design, Construction and Implementation Phases of the overall project.

The suggested deliverables are changes to the relevant project documents, an Issues Register, and a Privacy Design Features Paper.

Guidance is available to assist in specifying the Tasks and Deliverables involved in this Phase.

4. Documentation Phase

The purpose of this Phase is to document the process and the outcomes. The suggested Deliverable is a PIA Report.

Guidance is available to assist in specifying the Tasks and Deliverables involved in this Phase.

5. Review and Audit Phase

The purpose of this Phase is to ensure that the Design Features arising from the PIA are implemented, and are effective. The suggested Deliverable is a Review Report.

Guidance is available to assist in specifying the Tasks and Deliverables involved in this Phase.

<<== Planning Up to the Contents Page Preliminary Phase ==>>

Version 1.0, 31 October 2007

Full-Scale PIA - Preliminary Phase

This is Phase 1 of the suggested 5-Phase PIA Process.

The **purpose** of this Phase is to ensure that a firm basis is established for the PIA to be conducted effectively and efficiently.

The **suggested Deliverables** are a **Project Plan** and a **Project Background Paper**.

The following **Tasks** are suggested:

- **Review (or, if necessary, prepare) the PIA Project Terms of Reference**. Guidance is provided in relation to **the PIA Objectives**
- **Review the outcomes of the PIA Screening Process**
- **Review (or, if necessary, determine) the scope of the PIA**. At its narrowest, the scope could be limited to one or more particular data-items, or a particular process (such as data collection, acquisition of consent, or disclosure), or a particular technology (such as a smartcard). At its most comprehensive, the scope could extend to a social impact assessment. Because it is a form of risk assessment, the scope of a Full-Scale PIA is generally likely to be reasonably broadly expressed
- **Review (or, if necessary, prepare) the Stakeholder Analysis**, to ensure that major players in the project have been identified
- **Review (or, if necessary, prepare) the PIA Project Plan**. Although a set of Phases, Tasks and Deliverables is suggested, the Project Plan should take into account the specific features of the particular project and depart from the norm if necessary
- **Hold preliminary discussions with relevant organisations**. These discussions would generally focus on relevant parts of the organisation itself and any key participating organisations. Early discussions with external organisations, including the Information Commissioner's Office, may also be advisable in some circumstances
- **Hold preliminary discussions with representatives of and advocates for stakeholder groups**. This is likely to be of importance where particular external parties may be significantly affected by the project and what it delivers, or the matter has already drawn media attention
- **Conduct a preliminary analysis of privacy issues**. This is likely to commence with a deeper re-consideration of the outcomes of the Screening Process
- **Review (or, if necessary, prepare) the Environmental Issues Scan**, to ensure an up-to-date appreciation of research, publications and media activity, and how other organisations and other jurisdictions have approached similar projects

- **Review the resourcing** in light of the level of understanding achieved to date
- **Prepare the Project Background Paper**. This document will establish the basis for discussions with stakeholders

---

[<<== Process](#) [Up to the Contents Page](#) [Preparatory Phase ==>>](#)

Version 1, 31 October 2007

Full-Scale PIA - Project Background Paper

The Preliminary Phase of the 5-Phase PIA Process leads to the preparation of a Project Background Paper for the project that is subject to the PIA. The following provides guidance in relation to its content.

The **purpose** of the Project Background Paper is to establish a sound informational base on which preparations, consultation and analysis can proceed.

The Project Background Paper should contain the following, many of which will already exist in some form:

- a description of the **context or setting** in which the proposal is being brought forward (including relevant social, economic and technological considerations)
- a statement of the **motivations, drivers or opportunities** underlying the project
- a statement of the project's **objectives, scope and business rationale**
- **a description of project's design**. reflecting the organisation's current understanding of how the project will take shape. The explanation needs to be at a sufficient level of detail that participants can consider the project's impacts and implications. The detail available will vary depending on the developmental stage of the project. The design description may be conceptual and sketchy if salient design features have not been pre-determined. If the project has already been through the requirements analysis and design phases, the Project Background Paper can describe the flows of personal information at the appropriate level of detail. These may be placed in appendices containing diagrams that depict process descriptions and lists of items of personal data involved
- an initial assessment of **potential privacy issues and risks**, including both obvious or direct impacts and longer-term or secondary impacts on privacy, as perceived by the primary sponsor at the time the document is prepared
- brief descriptions of **options and sub-options** that the primary sponsor has identified, including both those already dismissed, and those that remain under consideration
- the **business case** which explains the justification for the features that give rise to the potential impacts on privacy, expressed both as:
    - a systemic explanation of how the key features of the scheme will achieve the objectives; and
    - a cost/benefit analysis
- descriptions of **the project plan** as a whole, the PIA process within it, and the consultation processes within the PIA
- lists of **involved organisations, stakeholder groups and representatives and advocates** who have been or will be invited to contribute to the PIA

- **attachments**, as appropriate that will contribute to understanding the project and its potential privacy implications.

The Project Background Paper should contain a clear and well-argued case for the project as a whole, and particularly for those features that have greatest potential for negative privacy impacts. This will facilitate the identification and collaborative examination of privacy risks and, ultimately, an effective PIA.

This process of rigorous challenge and justification for privacy-invasive aspects of schemes should be continued through logical design, to physical design, construction and integration, and on to implementation. This process facilitates the discovery of alternatives to achieve project goals while minimising negative impacts, and the creation of compensating measures to address project features with negative impacts that are judged to be necessary despite their downsides.

Where some of the information is subject to **commercial or security sensitivity**, that information can be separated into an Appendix, which can be distributed less widely and/ or subject to clear confidentiality constraints. This enables the issue to be managed without compromising the openness of the bulk of the information.

There may be resistance within the organisation to providing some of this information to stakeholders. For example, designers may consider that they do not need to give any explanations of the reasons for aspects of the concept or the design that some stakeholders may see as privacy-threatening. The project manager may hesitate to make available the business case underlying particular features or even the project as a whole. This may be in part for understandable commercial or security reasons. On the other hand, stakeholder trust needs to be achieved. It is therefore important to ensure that the real reason is not to avoid exposing loose reasoning or other motivations.

Where elements of the document cannot be delivered at the outset, it may be appropriate to distribute the information in two or more instalments.

Additional information may be needed in the case of projects that involve technologies that are new, or are otherwise unlikely to be understood by the participants in the consultation process. To achieve an effective consultation process, the primary sponsor may need to make available **technical documentation and briefings, and perhaps demonstrations**. Examples of technologies for which this is currently likely to be needed include:

- contact-based smartcards
- contactless smartcards and RFID tags
- identity management
- portals for services and authentication
- data warehousing and data mining

- locator technologies
- biometrics

<<== Preliminary Phase Up to the Contents Page Preparatory Phase ==>>

Version 1.0, 31 October 2007

Full-Scale PIA - PreparatoryPhase

This is Phase 2 of the 5-Phase PIA Process.

The **purpose** of this Phase is to make the arrangements needed to enable the critical Phase 3 to run smoothly.

The **suggested Deliverables** are a Stakeholder Analysis, a Consultation Strategy and Plan, and the establishment of a PIA Consultative Group (PCG).

The following **Tasks** are suggested:

- **Further articulate the Stakeholder Analysis**. This builds on the work previously undertaken in order to ensure that all relevant groups have been identified
- **Determine a Consultation Strategy**. This ensures that discussions with stakeholders are effective
- **Form a PIA Consultative Group (PCG)**. This comprises representatives of stakeholder groups
- **Distribute the Project Background Paper to the PCG**. This ensures that the PCG members can understand the nature of the proposal

---

<<== Preliminary Phase Up to the Contents Page Consultation & Analysis Phase ==>>

Version 1.0, 31 October 2007

Full-Scale PIA - Stakeholder Analysis

The Preparatory Phase of the 5-Phase PIA Process includes analysis of stakeholders in the project. This segment provides guidance in relation to this Task. Guidance at a preliminary level was provided during the discussions concerning the Framework for the PIA.

The objectives of a PIA cannot be achieved, and the aims of the project as a whole may be seriously harmed, if a PIA process is undertaken behind closed doors. The nature of contemporary information systems is such that many organisations are involved, variously as partners, participants, outsourced service providers, and technology providers. In government projects and public-private partnerships, the relevant Minister (s) is/are concerned about how the project develops.

Moreover, in a complex project applying powerful technologies, many segments of the population may be affected. To avoid the risk of alienating stakeholders, each needs to have the opportunity to provide input to the assessment, and to satisfy themselves that the outcomes reflect or have taken into account their concerns.

The **purpose** of Stakeholder Analysis is to lay the foundation for an effective consultation process, by ensuring that all parties are identified who may have an interest in the project.

The following is a checklist of potential stakeholders whose interests may need to be considered:

- **the organisation itself**
- **segments of the organisation** that have a significant interest in the matter
- **participating organisations**
- **regulatory agencies**, such as the Information Commissioner's Office, but possibly others as well
- **the intended subjects of the project**, which may include:
    - incorporated business enterprises, of various sizes, in various roles
    - incorporated associations, of various sizes, in various roles
    - individuals generally, in various roles, including:
        - as consumers or clients
        - as citizens
        - as employees and contractors
        - as small businesspeople
        - as people subject to regulation by government
- possibly, **the general public**
- possibly, **providers of relevant technologies and services**

It is not conventional to regard **the media** as a 'stakeholder'. Journalists and commentators may, however, see the situation differently. There are therefore advantages in considering the media within the context of the Stakeholder Analysis. Some information about any contentious project will inevitably become public, and may give rise to flurries of media attention which may significantly influence the course of the project, and may even undermine it. The provision of an appropriate amount of information to the media at appropriate stages in the process may be instrumental in avoiding misrepresentations of the project's aims and scope and the interruptions to project flow that they can cause.

[<<== Preparatory Phase](#) [Up to the Contents Page](#) [Consultation and Analysis Phase ==>>](#)

Version 1.0, 31 October 2007

Full-Scale PIA - Consultation Strategy

Background

Any project that is sufficiently complex and potentially privacy-threatening that it requires a Full-Scale PIA affects many parties. The Preparatory Phase of the 5-Phase PIA Process therefore includes the development of a Consultation Strategy. This document provides guidance in relation to that Task.

For large-scale projects that embody significant privacy risks, all of the elements described below are likely to be relevant.

For small-scale projects, on the other hand, some may well be superfluous. In this case, it is suggested that the document be used as:

- a checklist of possible elements of an appropriate consultation strategy
- an indication of the risks that need to be managed where elements are omitted

The **purpose** of a Consultation Strategy is to assist in the management of the privacy risks involved in the project.

The **benefits** to the organisation of conducting consultation are:

- gathering of information about the privacy impacts of a project from all relevant perspectives
- facilitation of the exchange of information among the participants
- emergence of mutual appreciation by the various groups of one another's perspectives
- identification and articulation of issues
- creative construction of possible solutions
- gaining of feedback about the acceptability of the possible solutions to the affected parties
- avoidance of problems being discovered at a late stage of the project, when all possible solutions are expensive
- avoidance of credible complaints being made at a late stage by affected parties that they were unaware of the project, or particular features, or of its impacts
- assurance that all relevant parties have the opportunity to contribute to the PIA, are seen to have that opportunity, and perceive themselves to have had that opportunity

Developing a Strategy

A 'consultation strategy' is distinctly different from a 'communications strategy'.

Effective consultation depends on all stakeholders being sufficiently well-informed about the project, having the opportunity to convey their perspective and their concerns, and developing confidence that their perspectives are being reflected in the design.

It is common for consultation processes to result in changes to the project and to its design. In order to make the maximum contribution to risk management in return for the smallest cost, consultation therefore needs to commence early and continue throughout the project life-cycle.

Key **characteristics** of effective consultation processes are:

- priming of discussions by means of an initial transfer of information about the project
- ongoing information exchange among all parties
- participation of representatives of and advocates for stakeholder groups, who have appropriate background in the technologies, systems and privacy impacts involved
- facilitated interactions among the participants
- outcomes that demonstrate accommodation by the parties of the perspectives of other stakeholders

Key **considerations** in the preparation of the Consultation Strategy are as follows:

- a sufficient diversity of participants to ensure that all relevant perspectives are represented, and all relevant information is gathered
- multiple rounds of:
    - information provision by the organisation
    - events that enable interactions among the various stakeholders
- assimilation of the information provided by all parties into the subsequent rounds of design and implementation activities

An outline of the **process** of forming a Consultancy Strategy is as follows:

- identify the preliminary set of issues that may arise from the project
- identify the stakeholders that are likely to be affected by, or concerned about, the project
- seek out representatives of those stakeholders
- seek out advocates who have specialist knowledge about the relevant interests
- form a **PIA Consultative Group (PCG)** by inviting a cluster of representatives and advocates that is not unduly large, but has sufficient diversity to ensure that the objectives are achieved
- devise **communication processes that will enable the effective interchange of**

ideas. This will commonly involve workshops and meetings, perhaps supplemented by formal submissions. It is generally advisable to conduct at least one face-to-face meeting at the outset, in order to provide the opportunity for the members of the PCG to meet one another and establish rapport. However, it may be possible to undertake much of the activity through teleconferences and/or video-conferences together with email discussions and submissions. Consideration should be given to the technical capabilities of the stakeholders and their access to such technologies.

The Population Segments Affected by the Project

Perhaps the most challenging aspect of a Consultation Strategy is to ensure effective access to the perspectives of relevant segments of the affected public. Three broad approaches can be adopted:

1. conduct **no consultations**, and rely on the perspectives of the people affected by the project to be identified, appreciated and adequately represented by the organisation, its staff, any consultants it uses, and/or other stakeholders
2. conduct **direct consultations** with members of the relevant segments of the public
3. **include within the PCG representatives of and/or advocates for** the relevant segments of the public

Avoidance of consultation with the affected public or proxies for them is fraught with risk. It may be appropriate, however, where the organisation is already well-versed in the issues or is using a consultant that has well-established and current knowledge of the issues, or the project is building on a prior PIA, conducted by some other organisation, which has involved direct consultation.

It is possible to approach **direct consultations** with affected segments of the population in two main ways:

- open meetings advertised and held in a variety of locations
- focus groups

Direct consultations are generally only effective, however, where the key aspects of the initiative are readily understandable by the participants. They are generally not effective where the initiative involves new technologies that are little-understood by the public, or the assessment needs to consider options, alternatives and contingencies that are highly complex or conceptual.

Whether or not open public processes are used, benefits can be gained by including in the consultations representatives of and advocates for the affected segments of the population. These two categories are usefully distinguished as follows:

- **representatives** have plausible claims to represent the interests of some relevant constituency. Their credibility arises primarily from their closeness to that constituency, and their ability to sense and explain their constituency's concerns
- **advocates** have plausible claims to understand the interests of some relevant group of people, particularly in newly-emerging and even hypothetical circumstances. Their credibility is based not on their ability to 'represent' any particular population segment, but rather on their capacity to appreciate and consider the complexities and the options, and to present evidence and coherent arguments

Where the organisation has an established public consultation strategy, or linkages with relevant public interest organisations, the PIA Consultation Strategy should be devised in a manner consistent with the broader strategy, and should take advantage of existing linkages.

If difficulties are encountered in identifying relevant stakeholder groups, or appropriate representatives of and advocates for those segments, regulatory agencies are likely to be able to assist. The experiences of other corporations, industry associations and government agencies, or of similar organisations in other jurisdictions, may also be relevant. Specialist consultancies are also likely to be able to assist.

Effective consultative processes are dependent upon all parties having **mutual understandings in relation to confidentiality**. Generally, trust is enhanced when organisations resist placing unnecessary restrictions on the documents used as the basis for discussions.

Where some of the material is subject to commercial or security sensitivities, it can be placed in separate appendices which can be subjected to confidentiality constraints without adversely affecting trust. Some caution is warranted in relation to words spoken during discussions. Mutual confidence can be achieved by providing all parties with protection for parts of the discussions where participants brainstorm and 'test the water'.

Where **security considerations** militate against full openness of the consultative processes, it is suggested that:

- the PIA be undertaken in as open a manner as is practicable
- such aspects as give rise to sensitivities be separated into closed or confidential appendices and separate, relatively closed discussion sessions
- where security considerations result in the suppression of relevant information, proxy measures be devised that are as effective and credible as possible. (For example, the security-sensitive information could be provided to the Information Commissioner's Office, with the ICO then delivering to PCG members evaluative comments that avoid exposing the information)

An important consideration for effective consultation is access to **financial resources** to facilitate the participation of members of the public, and representatives and advocates. Individuals, and many public interest groups, lack the necessary funding base to enable suitable people to participate in PIA processes, particularly since many are volunteers acting on a *pro bono* basis. A budget needs to be set aside for travel support and possibly sitting fees or honoraria.

[<<== Preparatory Phase](#) [Up to the Contents Page](#) [Consultation & Analysis Phase ==>>](#)

Version 1.0, 31 October 2007

Full-Scale PIA - Consultation and Analysis Phase

This is Phase 3 of the 5-Phase PIA Process. It involves consultations with stakeholders, risk analysis, and articulation of problems and the search for constructive solutions.

The **purpose** of this Phase is to ensure that problems are identified early, that effective solutions are found early, and that the design is adapted to embody those solutions.

The **suggested Deliverables** are changes to the relevant project documents, an Issues Register, and a Privacy Design Features Paper.

The following **Tasks** are suggested:

1. **Implement the Consultation Strategy** that was established during the previous Phase. This will generally include a PCG process, with workshops and face-to-face meetings, supplemented by electronic discussions and teleconferences and perhaps formal submissions
2. **Assimilate the comments provided**
3. **Identify the Design Issues and Privacy Problems**
4. **Re-consider the Design Options**. This focuses on the various approaches that are available to resolve issues and solve problems. Key concepts at this stage are:
    - Privacy Impact Avoidance Measures
    - Privacy Impact Amelioration Measures
    - Privacy Enhancing Technologies (PETs)
5. **Progressively document the problems and solutions in an 'Issues Register'**. Particularly with large projects, there is a serious risk that 'corporate memory' will not be sustained between iterations. This problem can be overcome by carrying the Issues Register forward as an Appendix to each revision of the Project Background Paper that is made available to the PCG, and to other relevant documents. The Issues Register also serves as means to note issues that cannot be addressed immediately and avoid the possibility of their being overlooked
6. **Reflect the conclusions reached, in the Issues Register and/or in an evolving 'Privacy Design Features Paper'**. This documents:
    - issues identified
    - avoidance and amelioration measures considered, rejected and adopted
    - design changes to be undertaken as a result
    - outstanding issues
7. **Provide the Privacy Design Features Paper to**
    - **the PCG**
    - **the project team**

8. **Relay the project team's feedback to the PCG**
9. **Conduct further consultations with the PCG**
10. **Incorporate the decisions on privacy design features into the design**
11. **While unresolved issues remain, continue consultation and analysis**

This Phase generally involves **multiple iterations**. The most effective approach is to conduct the first iteration at the stage of Project Initiation, and arrange subsequent iterations to correspond with the later phases of the project (e.g., Requirements Analysis, Logical Design, Physical Design, Construction, Integration and Deployment of the new system).

The Project Background Paper is likely to require progressive upgrading, or supplementation by further documents, to reflect developments during the project.

As will be apparent from the descriptions provided, it is normal for a PIA to result in changes to the design in order to avoid or ameliorate negative privacy impacts. Late changes can of course be expensive. This is an important reason why early commencement of a PIA is highly advisable.

<<== Preparatory Phase Up to the Contents Page Documentation Phase ==>>

Version 1.0, 31 October 2007

Design Issues and Privacy Problems

If the project design has reflected a strong understanding of privacy issues, it is possible that the participants in the consultation processes may agree to the design.

More commonly, however, because of project complexities and the diversity of interests among stakeholders, the consultation processes will create the need for aspects of the project and the project's design to be re-considered. Complex projects that apply advanced technologies give rise to public concerns in addition to those addressed by the Data Protection Principles.

Efforts to identify and describe privacy issues will pay dividends in the following stage, because the better a problem is understood, the easier it becomes to devise and negotiate ways to address it.

Particular clusters of privacy concerns that arise in PIAs include the following:

1. broad personal information issues, including:
    - **data sensitivity**. (This term is used here in the general sense, rather than the very specific sense used in s.2 of the Data Protection Act). This relates to:
        - particular data about all people in the data collection (e.g., medical conditions and impairments, financial data, family structure)
        - all data about a particular person (e.g., persons at risk)
        - particular data about a particular person, possibly of a long-term nature (e.g., home address), but also possibly with a short period of validity (e.g., temporary address, travel plans)
    - **data quality**. This encompasses many specific characteristics, particularly accuracy, timeliness, completeness, precision, and relevance to purpose. The further data strays from its original context, the greater the likelihood that it will be misinterpreted, and the greater the impact of even small limitations in quality
    - **data meaning**. This varies considerably, but often subtly, from one context of use to another. For example, 'spouse' and 'child' are highly ambiguous terms. Variations in the meaning of apparently similar data-items readily give rise to misunderstandings and administrative error, which can result in harm to individuals
    - **data destruction**. The public seeks a positive approach, including a legal framework and specific policies and programmes that ensure retention of data only as long as its original purposes have not been fulfilled. Data

protection is achieved by phrasing specific and narrow purposes rather than broadly-written purposes that justify indefinite retention. Data destruction applies to both primary data collections of identified data, and to personal data transferred away from its origins for particular purposes (e.g. for evaluation of programmes, audit, and longitudinal analysis). The life-cycle for special-purpose data is a particular area of privacy concern

2. **identity**, including:
    - the multiple use of identifiers
    - the denial of anonymity
    - identifiers that directly disclose personal data (e.g. embedded date-of-birth)
    - identifiers linked with authenticators (such as credit-card number plus additional details), because that creates the risk of identity fraud and in extreme cases even identity theft
    - biometrics, which give rise to very serious privacy concerns
3. **function creep**, beyond the original context of use, in relation to:
    - the use of personal information
    - the use of identifiers
4. **registration and authentication processes**, including their onerousness, their intrusiveness, and the exercise of power by government over individuals
5. **surveillance**, whether audio, visual, by means of data, whether electronically supported or not, and whether the observations are recorded or not
6. **location and tracking** whether within geographical space or on networks, even where it is performed incidentally, and especially where it gives rise to records
7. **intrusions into the privacy of the person**, especially compulsory or pseudo-voluntary (such as in employment relationships) yielding of tissue and body-fluid samples, and biometric measurement

It is highly advisable to record the issues that arise in documentary form. This Handbook uses the term **'Issues Register'** to refer to such documentation. In large projects it is likely to be formalised, but in other cases it may take the form of an attachment to meeting minutes, or a web-page maintained by project staff.

[<<== Consultation & Analysis Phase] [Up to the Contents Page] [Design Options ==>>]

Version 1.0, 31 October 2007

Design Options

Development of Design Options is the constructive part of the PIA process. The process entails considering each item in the Issues Register arising from the preceding Design Issues and Privacy Problems activity, and searches for ways in which those problems can be overcome.

There are two broad categories of solution.

An '**avoidance measure**' is a means of dissipating a risk. It refers to the exclusion of technologies, processes, data or decision criteria, in order to avoid particular privacy issues arising. Examples include:

- minimisation of personal data collection
- non-collection of contentious data-items
- active measures to preclude the use of particular data-items in the making of particular decisions
- active measures to preclude the disclosure of particular data-items
- non-adoption of biometrics in order to avoid issues about invasiveness of people's physical selves

An '**amelioration measure**' is a design feature that compensates for other, privacy-invasive aspects of a design. An amelioration measure may compensate wholly for a negative impact, or only partially. Examples include:

- minimisation of personal data retention by not recording it
- minimisation of personal data retention by destroying it as soon as the transaction for which it is needed is completed
- destruction schedules for personal information
- limitation of the use of a data-item to a very specific purpose, with strong legal, organisational and technical safeguards preventing its application to any other purpose
- design, implementation and resourcing of a responsive complaints-handling mechanism, backed by serious sanctions and enforcement powers, priorities and resources

Problems must be analysed, to devise acceptable avoidance and amelioration measures. The following suggestions are made about the process of problem analysis:

- • the differing **perspectives** of the multiple stakeholder groups should be reflected

- the **locus** of each impact and implication should be identified. For instance, what kinds of people or organisations will experience the various impacts, and under what circumstances?
- the **justification** for the feature that gives rise to the problem should be examined. For example, is the privacy infringement proportional to, or appropriately balanced with, any benefits gained from the infringement? And is it clear that the claimed benefits will actually arise?
- the **circumstances** in which the feature needs to be applied should be questioned. Is it appropriate for the data to be collected, used or disclosed in every instance, or can the data-handling in question be limited to particular situations in which it is demonstrably relevant?
- consideration may need to be given to **alternative future economic and social environments**. It may be possible to do this using a structured approach. Alternatively, scenario analysis may need to be applied in order to identify potential second-order effects. Inevitable first-order impacts and second-order implications should be taken into account, as well as contingent effects that will only arise under particular circumstances
- relevant **legal considerations** need to be taken into account, including responsibilities in relation to both direct impacts and indirect implications, and contingent liabilities that may arise. Examples include the responsibility to deliver services and to do so on an equitable basis, the law of confidence and the duty of care arising under negligence law
- one major issue is **the effectiveness of privacy protections**. An effective privacy protection regime requires all of the following to be in place:
    - clear specifications of privacy protections
    - clear prohibitions against breaches of protections
    - clear sanctions or penalties for breaches of protections
    - mechanisms in place to detect and report breaches
    - processes whereby such breaches an be sanctioned
    - resources to pursue sanctions
    - process for investigations and application of sanctions
    - imposition and enforcement of the specified sanctions

One particular issue that may need careful consideration is the location at which data is stored. From the perspective of privacy protection, there are considerable privacy benefits in **de-centralisation** rather than centralisation, in intentionally **dis-aggregation of data collections** rather than consolidated data collections, and in **dis-integration** rather than integration. The benefits include:

- to greatly reduce the risk of function creep
- to facilitate the application of access controls
- to ensure availability at the point of use
- to encourage relevance to purpose
- to retain flexibility and extensibility to cater for local conditions

- to minimise misinterpretation of data as a result of loss of context
- to avoid diseconomies of scale
- to increase the likelihood of data being destroyed when its purposes have been fulfilled

Where a project involves any shifting of data towards the centre, it is all the more important that clear justification be demonstrated. Further, proponents of speculative uses of data (such as 'statistical analysis', 'management reporting' and 'data mining') need to be challenged for greater detail, and for demonstration that benefits will actually be achievable. Once a case for centralisation has been established, it is necessary to identify, assess and balance the disadvantages.

Many technologies are privacy-invasive. Some technologies, however, have been developed for the specific purpose of protecting privacy or enhancing it. A commonly-used term to describe such tools is Privacy-Enhancing Technologies (PETs). It is strongly advisable that PETs be considered as design options.

Interactions within the PIA Consultative Group may result in consensus on some measures that avoid privacy impacts, and some measures that ameliorate privacy impacts that cannot be avoided. In some circumstances, at least in respect of some issues, consensus may not be feasible. In those cases, the organisation responsible for the project must exercise judgment as to an appropriate balance between the competing interests. Where the issue is major, consultation with the Information Commissioner's Office may be appropriate.

The conclusions regarding design features should be documented in an 'Issues Register', and provided to the project team as a whole. This is described in the later activities of the Consultation and Analysis Phase.

<<== Design Issues and Privacy Problems

Up to the Contents Page

Consultation & Analysis Phase ==>>

Version 1.0, 31 October 2007

Privacy-Enhancing Technologies

Since the mid-1990s, a range of technologies have been developed to assist privacy rather than threaten it. The term commonly used for these is privacy-enhancing technologies (PETs). PETs help mitigate the effects of privacy-invasive technologies (PITs). This segment provides background information on PETs.

It is useful to distinguish three categories of PETs:

1. means of countering against privacy-invasive technologies
2. means of providing genuine, untraceable anonymity
3. means of providing strongly protected pseudonymity

1. Counter-Privacy-Intrusive Technologies

Many technology applications gather data, collate data, apply data, or otherwise assist in the surveillance of people and their behaviour. A useful collective term is 'privacy-intrusive technologies' ('the PITs'). Among the host of examples are surveillance technologies (such as CCTV), data-trail generation (such as keystroke monitoring) and intensification through the denial of anonymity (e.g., telephone caller ID, stored-value or loyaly cards, and intelligent transportation systems), data warehousing and data mining, stored biometrics, and imposed biometrics. In Internet contexts, there are considerable concerns about the various categories of malware, including viruses, worms, trojans, keystroke-loggers, 'spyware' and 'phishing'.

Some PETs are designed to counter the effects of PITs. Examples include spam-filters, cookie-managers, password managers, personal firewalls, virus protection software, SSL/TLS for channel encryption and spyware-sweepers. Other advanced PET services display to the browser-user information about the owner of an IP-address before connecting to it, and monitor inbound traffic for patterns consistent with malware and hacking and monitor outbound traffic for spyware-related transmissions.

In some projects, it may be appropriate for organisations to provide advice to their users to assist them to protect themselves against malware, and to protect their authenticators (such as passwords). There may be benefits in going further, and offering assistance to users in relation to such matters as the installation and configuration of software such as web-browsers, firewalls, and anti-virus and anti-spyware packages.

The effective incorporation of PETs into a scheme may alleviate pressures on privacy that result from program goals or efficiency requirements, with little increase in cost.

2. Anonymity PETS

The first category of PETs described above addresses particular problems, but does little to prevent the accumulation of personal data into dossiers and profiles. A much more aggressive approach is available. This sets out to deny personal identity by providing untraceable anonymity. Examples include genuinely anonymous ('Mixmaster') remailers and web-surfing schemes, and genuinely anonymous e-payment mechanisms. (The inclusion of 'genuinely' is necessary, because some remailers and payment mechanisms have been incorrectly described as 'anonymous', even though it is possible to trace transactions to the people who conducted them).

There are many circumstances in which organisations can and should permit anonymous communications. Examples include general enquiries, and the provision of generalised (as distinct from person-specific) information. A further important application is to support 'whistle-blowing'.

On the other hand, many of an organisation's mainstream business processes cannot be conducted with anonymous users. The reasons include the inability to prevent fraud, the likelihood of inappropriate access to personal data, and the need for some kinds of transactions to be recorded against the appropriate person's records.

3. Pseudonymity PETs

With anonymity, an organisation is precluded outright from being able to detect the identity of the person with whom is is communicating. Pseudonymity refers to circumstances in which the person's identity is not apparent, but could, under some circumstances, be discovered.

Genuine anonymity has the disadvantage that it can be used for nefarious purposes, to avoid detection of criminal activity and hence to prevent retribution and deny accountability. Most people would be prepared to use pseudonymity instead, as a more balanced form of privacy protection. However, they may need assurance that the veil will not be broken through casually or without due cause.

A pseudonymous record or transaction is one that cannot, in the normal course of events, be associated with a particular individual. Hence a transaction is pseudonymous in relation to a particular party if the transaction data contains no direct identifier for that party, and can only be related to them in the event that specific additional data is associated with it.

To be effective, pseudonymous mechanisms must involve legal, organisational and technical protections, to ensure the link between a transaction and an identifiable

individual can be achieved only under appropriate circumstances. Examples of relevant techniques are:

- use 'pseudonyms', and ensure that the linkage between a personal identifier and the person who uses it is recorded only by a 'trusted intermediary'
- avoid collecting identifiers, and instead use one of these techniques to manage risks:
    - ensure that payment has been received before providing the goods or services (hence authenticating value rather than identity)
    - check a person's eligibility, or a relevant characteristic of the person such as age, disability, or educational qualifications (which is referred to as attribute authentication, rather than identity authentication)

Pseudonymous techniques can provide innovative ways of addressing fundamental issues in system design while protecting personal information. Used to their full potential, such technologies can provide secure identification to reduce fraud; secure networking to reduce losses from theft; and secure payment systems that dispense with the administrative costs of cash while permitting high levels of user anonymity and privacy protection. Cost savings and privacy protection need not be opposing values.

<<== Consultation & Analysis Phase | Up to the Contents Page | Design Options ==>>

Version 1.0, 31 October 2007

Full-Scale PIA - Documentation Phase

This is Phase 4 of the 5-Phase PIA Process.

Privacy Impact Assessment is a process. The benefits to the organisation that conducts it arise primarily from that process, in the form of learning and adaptation, partly by the stakeholders, and partly by the organisation and the team responsible for the project.

There are, however, advantages in generating a final document towards the end of the PIA process.

The **purpose** of this Phase is to document the PIA process and the outcomes.

The suggested **Deliverable** is a PIA Report.

The following **Tasks** are suggested:

- **Consolidate the decisions on avoidance and amelioration measures into a final version of the Issues Register and/or Privacy Design Features Paper**
- **Produce a PIA Report**
- **Make the PIA Report available to the PCG**
- **Publish the PIA Report** (withholding any security-sensitive information in confidential, or closed, appendices)

<<== Consultation & Analysis Phase

Up to the Contents Page

Review & Audit Phase ==>>

Version 1.0, 31 October 2007

The PIA Report

The benefits to an organisation of conducting a PIA arise more from the process than the product, and therefore, the focus should not be on document-production.

Nonetheless, it can be beneficial to document the outcomes in a PIA Report at the conclusion of the project. The **reasons for preparation of a PIA Report** are:

- as an element of **accountability**, in order to demonstrate that the PIA process was performed, and was performed appropriately
- to provide a **basis for post-implementation review** (within the context of the project)
- to provide a **basis for audit** (from outside the project)
- to **provide corporate memory**, ensuring that the experience gained during the project is available to those conducting further iterations of the PIA if original staff have left
- to **facilitate sharing experience gained** during the project with future PIA teams and others outside the organisation

The following are **key elements** of a PIA Report:

- a description of the project
- an analysis of the privacy issues arising from it
- the business case justifying the negative privacy impacts and implications
- discussion of alternatives considered and the rationale for the decisions made
- a description of the privacy design features adopted to avoid and ameliorate negative privacy impacts and implications
- an analysis of the public acceptability of the scheme and its applications

It may be appropriate to include the following as **appendices**:

- a summary of the consultative processes undertaken
- contact-details of organisations and individuals with whom consultations were undertaken
- the Project Background Paper(s) provided to those consulted
- the PIA Project Plan
- the Issues Register and/or Privacy Design Features Paper(s)
- references to relevant laws, codes and guidelines

At a late stage, once the design has been checked for legal compliance, it may be

appropriate to add the following as further Appendices to the PIA Report:

- the Privacy Law Compliance Study
- the Data Protection Act Compliance Study

A PIA Report should be **written with the expectation that it will be published**, or at least be widely distributed. If so, the report can fulfil the functions listed above: accountability, post-implementation review, audit, input into future iterations of the PIA, and background information for people conducting PIAs in the future.

Some of the information gathered during a PIA process may be subject to security or commercial sensitivities. In such cases, it may be appropriate for the detailed information to be in **confidential, or closed, appendices**. Such information suppression, however, needs to be limited to only that which is justified. Sufficient information needs to be included within the PIA Report to ensure that the arguments and assessments are complete, informative and comprehensible.

[<<== Documentation Phase](#) [Up to the Contents Page](#) [Documentation Phase ==>>](#)

Version 1, 31 October 2007

Full-Scale PIA – Review and Audit Phase

This is Phase 5 of the 5-Phase PIA Process.

The **purpose** of this Phase is to ensure that the undertakings arising from the Consultation and Analysis Phase are carried through into the running system or implemented project.

The suggested **Deliverables** are delivery of the undertakings in the Privacy Design Features Paper.

The following **Tasks** are suggested:

- **Undertake a Review** of the implementation of the avoidance and amelioration measures that were documented in the Issues Register and/or the Privacy Design Features Paper
- **Prepare a Review Report**
- **Present the Privacy Review Report to the PCG**
- **Make the Privacy Review Report publicly available**

As with the preceding Phases, it is beneficial to perform this Phase at an appropriate stage in the life-cycle of the overall project. This could be, for example, **at a milestone such as the Detailed Design Review**, or its equivalent in the organisation's preferred project method.

Another approach that organisations may consider appropriate or cost-effective is to build the review of performance into the organisation's standard, periodic or occasional **internal audit or external audit processes**.

<<== PIA Process Up to the Contents Page

Version 1.0, 31 October 2007

Small-Scale PIA – Overview

Where a project has privacy impacts and implications, the conduct of a PIA is a means of ensuring that the issues are appreciated and addressed.

Projects with substantial impacts warrant a Full-Scale PIA process. Other projects require attention, but do not warrant as great an investment of time and resources. A Small-Scale PIA involves analysis of the privacy issues arising from the aspect or aspects that the Screening Process has highlighted through the application of the Criteria for Small-Scale PIA.

A Small-Scale PIA process differs considerably from a Full-Scale PIA. In particular:

- it is less formalised
- it involves less investment
- it calls for less exhaustive analysis and information-gathering
- it is more likely to be focused on specific aspects of the project rather than the project as a whole

Because projects vary greatly, a process should be devised that fits the need, is as comprehensive as it needs to be, but is only as resource-intensive as is appropriate in the circumstances.

This segment draws on the Full-Scale Privacy Impact Assessment process described in Part II of this Handbook, but is much briefer. The guidance is in two Parts:

- Background Information intended to assist organisations to gain an appreciation of the kinds of projects for which Small-Scale PIA is appropriate, and its key characteristics
- The PIA process:
    - Preliminary Phase
    - Preparatory Phase
    - Consultation and Analysis Phase(s)
    - Documentation Phase
    - Review and Audit Phase

<<== Screening Process Up to the Contents Page Background Information ==>>

Version 1.0, 31 October 2007

Small-Scale PIA – Background Information

This segment provides information that lays the foundation for the Small-Scale PIA process.

The scope of the PIA should reflect the nature of the project as a whole. The following are examples of a range of significantly different kinds of projects for which a Small-Scale PIA is likely to be appropriate. However, any of these projects could have attributes which could make a Full-Scale PIA more appropriate (for instance, if the personal data were highly sensitive or the technology untested).

A Small-Scale PIA is likely to be appropriate for:

- replacement of an existing personal data system by new packaged software, with consequential changes to business processes and perhaps data storage
- design and development of a new personal data system that will only contain data about people who have given their consent
- enhancements to an existing system in order to collect, store and use several additional items of personal data
- a proposal to collect items of personal data from a new source, e.g., to reduce the costs incurred by the organisation or the inconvenience to the individuals concerned, or to enable cross-checking against data provided by the data subject
- revisions to staff instructions relating to the disclosure of personal data
- adaptations to an existing system to reflect new legislation, codes or industry standards
- the drafting of legislative amendments authorising the collection, use or disclosure of personal data (particularly where a specific project authorised by the amended legislation will be subject to a PIA)
- the application of a new technology to an existing purpose (e.g., replacement of bar-code or magnetic-stripe technology with a contact-based chip containing the same data)
- drafting of new procedures for customer authentication, e.g., in order to reflect new knowledge about 'identity theft', or respond to media coverage of it
- the re-design of web-forms for capture of personal data from customers, including the explanations provided, and the circumstances in which particular data-items are declared to be mandatory or optional
- plans to outsource business processes involving personal data, or the storage and processing of personal data
- the application of existing personal data to a new purpose
- changes to retention policies relating to personal data
- policy statements concerning staff usage of employer-provided facilities such as

telephones, mobile phones, desktops, portables, and broadband and wireless ISP subscriptions
- review of the means whereby patients express their requests, consents and denials regarding the disclosure of their medical data from the records of a health care professional or clinic
- the design of a pseudonymous scheme for customer survey data
- amendments to the organisation's privacy policy statement

Some key characteristics of an effective Small-Scale PIA are as follows:

- a PIA is a form of risk management
- a PIA serves the needs of the organisation itself, by identifying privacy issues early, and enabling them to be addressed quickly and inexpensively, rather than becoming major problems later
- in order to serve the needs of the organisation, a PIA needs to reflect the perspectives of all stakeholders in the project, including and especially the individuals who are affected by it
- a PIA is primarily about process, and only secondarily about producing a report
- a PIA is more than just a check of legal compliance
- the effective conduct of a PIA depends on having appropriate expertise available. If it is not available within the organisation, it should be possible to acquire relatively inexpensive consultancy support

The following segment provides guidance in relation to the planning and performance of a Small-Scale PIA.

[<<== Overview](#) [Up to the Contents Page](#) [PIA Process ==>>](#)

Version 1.0, 31 October 2007

Small-Scale PIA - The Process

It is neither feasible nor even desirable to specify a fixed process for a Small-Scale PIA, due to the diversity of circumstances,. The process for any particular project needs to reflect:

- the nature of the project (e.g., new system, replacement system, enhancements to an existing system, new technology, outsourcing, changed business processes or staff instructions, replacement user interface, revised privacy policy statement, drafting of legislative changes)
- the specific aspects of the project that the Screening Process has highlighted
- any relevant PIAs that have been previously conducted
- the organisation's level of experience in conducting PIAs

Hence the following guidance is of necessity general in nature, and intended to assist organisations in developing their own project plan.

Conventional project management techniques may be applied to the process of assessing privacy impact. This segment provides an outline description of a suggested set of Phases for a Small-Scale PIA.

In each case, the detailed guidance for the relevant Phase of a Full-Scale PIA is referred to. That is because those segments provide deeper discussion of aspects that may be relevant to the circumstances. However, the scale of a Small-Scale PIA is such that it may be appropriate to compress Phases together, consolidate Tasks, or reduce the number of Deliverables by merging several documents into one.

The terms used here (such as 'Preliminary Phase') are intended to be descriptive and are not in themselves of any great significance. Organisations may use other terms that are consistent with their own internal standards, policies and practices.

The following suggested Phases are described below:

1. Preliminary Phase
2. Preparatory Phase
3. Consultation and Analysis Phase(s)
4. Documentation Phase
5. Review and Audit Phase

1. Preliminary Phase

The purpose of the Preliminary Phase is to ensure that a firm basis is established for the PIA to be conducted effectively and efficiently. Depending on the scale of the project and the experience of the project manager in relation to PIAs, it may be appropriate to produce and maintain a **Project Plan**. It will generally be advisable to produce a **Project Background Paper**, although this is likely to be succinct.

Because the circumstances of Small-Scale PIAs vary so much, this Handbook does not contain any specific guidance in relation to this phase. However, a useful checklist is available, which describes the Tasks involved in the corresponding phase of Full-Scale PIAs. All the tasks recommended in the checklist would be excessive for a small project. However, the ideas are likely to be of assistance, and may be applied in some less onerous manner such as combination or selectiveness according to the circumstances.

2. Preparatory Phase

The Purpose of the Preparatory Phase is to make the arrangements needed to enable the critical Phase 3 to run smoothly. In this Phase, organisations may undertake a Stakeholder Analysis, development of a Consultation Strategy and Plan, and establishment of a PIA Consultative Group (PCG). It will be useful to consult the checklist which describes the Tasks involved in the corresponding phase of Full-Scale PIAs. It is likely that ideas extracted from that document will need to be scaled, however, in order to be applicable to the particular project.

3. Consultation and Analysis Phase(s)

The Consultation and Analysis Phase builds on the foundations established by the first two Phases. It includes consultations with stakeholders, risk analysis, the articulation of problems, and the search for constructive solutions.

Some activities may need to be performed more than once (e.g., by having several successive conversations with a key stakeholder). On the other hand, if a comprehensive and clear Project Background Paper is produced, and the participants are experienced or issues relatively simple, it may be feasible to conduct the process quite briskly.

The key Deliverable is some kind of document (such as a Privacy Design Features Paper or a Meeting Outcomes Report) that enables the results to be communicated to the various parties involved. The project team, and in particular the designers, are important recipients of this document, because they will need to make decisions based on the outcome of consultations, make changes to the relevant project documents and implement the decisions made.

However, a useful checklist is available, which describes the Tasks involved in the corresponding phase of Full-Scale PIAs. It is likely that ideas extracted from that document will need to be scaled, in order to be applicable to the particular project.

4. Documentation Phase

The purpose of the Documentation Phase is to document the process and the outcomes. The Deliverable is a PIA Report. Depending on the context, this might be a relatively brief 'note to file', with copies to relevant parties; but circumstances may warrant a more substantial or more carefully-prepared document.

However, a useful checklist is available, which describes the Tasks involved in the corresponding phase of Full-Scale PIAs. It is likely that ideas extracted from that document will need to be scaled, in order to be applicable to the particular project.

5. Review and Audit Phase

The purpose of this Phase is to ensure that the Design Features arising from the PIA are implemented, and are effective. The Deliverable is a Review Report. Once again, in some contexts a 'note to file', with copies distributed to relevant parties, might be sufficient to achieve this requirement. In other cases, considerably greater investment may be warranted.

However, a useful checklist is available, which describes the Tasks involved in the corresponding phase of Full-Scale PIAs. It is likely that ideas extracted from that document will need to be scaled, in order to be applicable to the particular project.

<<== Background Information

Up to the Contents Page

Privacy Law Compliance Check ==>>

Version 1.0, 31 October 2007

Privacy Law Compliance Check

The organisation must ensure that the project, and the personal data it that handles, and the business processes that it uses are compliant with all relevant laws. Unlike a PIA, which is best commenced early in the project life-cycle, Compliance Checking is normally conducted later, once the design has reached a detailed stage.

A separate segment of the PIA Handbook provides guidance in relation to compliance with the Data Protection Act. This segment relates to other elements of the law.

Responsibilities

The organisation should undertake a survey of the law relevant to the project, and to the data-holdings and business processes it gives rise to.

Further, all participating organisations should do the same, regarding their involvement in the project.

Ordinarily, the organisation would utilise the services of professional lawyers with relevant expertise for this exercise.

Sources of the Law and Other Rules

The law comprises statutes, secondary legislation, statutory instruments created and maintained under delegation from the Parliament (including Regulations and formal Codes), and the common law.

Further documents may be relevant, such as codes of conduct and privacy policy statements, particularly where the organisation has provided some form of undertaking to comply with them. This might arise from some formal act of adoption (such as membership of the association that issues the code), or the terms of a document that the organisation itself has uttered.

There are also matters of public policy that may not be formally law, but that are generally respected.

Potentially Relevant Sources of the Law

A number of examples of relevant laws were identified in the segment of this Handbook

that described the Criteria for Privacy Law Compliance Checks.

The following is an indicative, but not exhaustive, list of laws that may be relevant:

- provisions within statutes regulating such activities as public health, education, family law, children's safety, occupational health and safety, archives, telecommunications, and surveillance devices
- for government agencies, provisions within the statutes that govern their activities and programmes
- for public-private partnerships, provisions within the statutes that govern their activities and programmes, and terms within the contracts that the parties have entered into
- for sub-contractors, terms within the contracts that the parties have entered into
- the law of confidence
- the tort of negligence
- the tort of passing off
- the possibly emergent tort of privacy

A specific example of delegated privacy legislation is the Privacy and Electronic Communications Regulations 2003, which applies to organisations conducting marketing projects to interact with potential customers via electronic communications.

Compliance Checking

The organisation must evaluate the project process and the project outcomes (including the design, data collections and business processes), to ensure that all aspects are compliant with all relevant provisions of all relevant laws.

Each participating organisation must evaluate the activities it will undertake as part of the project, and as part of the resulting system or scheme, in order to ensure that it is compliant with all relevant provisions of all relevant laws.

In some cases, guidance may be available to assist in the performance of Compliance Checking. An example arises in respect of the Privacy and Electronic Communications Regulations 2003, for which the Information Commissioner's Office provides a Privacy and Electronic Communications Regulations Template (in Word format).

Deferral of Implementation, and Design Adaptation

To the extent that the design is not compliant, it would be illegal to deploy the new or adapted system or scheme. It will be necessary to change the design prior to deployment, in order to achieve compliance.

<<== Screening Process | Up to the Contents Page | Data Protection Act Compliance Check ==>>

Version 1.0, 31 October 2007

Data Protection Act Compliance Check

The organisation must ensure that the project, and the personal data that it handles, and the business processes that it uses, are compliant with:

- the Data Protection Act in general
- the Data Protection Principles
- the Interpretations of the Principles

This is not a recommendation of this Handbook, but a requirement of law.

Compliance Checking

The organisation must evaluate the project process and the resulting design, in order to ensure that it is compliant with all relevant provisions of the Data Protection Act. Unlike a PIA, which is best commenced early in the project life-cycle, Compliance Checking is normally conducted later, once the design has reached a detailed stage.

Each participating organisation must evaluate the activities it will undertake as part of the resulting system or scheme, in order to ensure that it is compliant with all relevant provisions of the Data Protection Act.

A Detailed Template (in Word format) is provided to assist in checking the compliance of a design against the provisions of the Data Protection Principles.

Deferral of Implementation, and Design Adaptation

To the extent that the design is not compliant, it would be illegal to deploy the new or adapted system or scheme. It will be necessary to change the design prior to deployment, in order to achieve compliance.

<<== Screening Process Up to the Contents Page

Version 1.0, 31 October 2007

General Resources

This segment provides answers to some background questions that an organisation that is about to conduct a PIA may pose. Many of the terms and concepts in the answers are used in other segments of this Handbook and will be important to understand when conducting a PIA. The topics addressed are:

---

1. What is 'Privacy'?

Privacy is recognised as a human right in all major documents applicable in the UK, including the Universal Declaration of Human Rights (UDHR 1948, Article 12), the International Covenant on Civil and Political Rights (ICCPR 1966, Article 17), the European Convention on Human Rights (ECHR 1950, Article 8), and the Charter of Fundamental Rights of the European Union (CFREU 2000, Articles 7 and 8). Specifically, it is mentioned in the UK Human Rights Act 1998, at Article 8.1, as "respect for ... private and family life, ... home and ... correspondence".

These instruments evidence a degree of inconsistencydocuments are not entirely consistent. Moreover, they generally do not define the term 'privacy', and its scope interleaves overlaps with a range of other freedoms and rights. A useful working definition of privacy is **"the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations"**.

Interpreted most broadly, privacy is about the integrity of the individual. It therefore encompasses many aspects of the individual's social needs. The following dimensions can be usefully distinguished.

Privacy of the Person, sometimes referred to as 'bodily privacy', is concerned with the integrity of the individual's body. At its broadest, it could be interpreted as extending to freedom from torture and right to medical treatment, but these are more commonly seen as human rights rather than as aspects of privacy. Issues that are more readily associated with privacy include compulsory immunisation, imposed treatments such as lobotomy

and sterilisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and requirements for submission to biometric measurement.

Privacy of Personal Behaviour relates to the observation of what individuals do, and includes such issues and optical surveillance and 'media privacy'. Many issues that come to attention relate to sensitive matters, such as sexual preferences and habits, political activities and religious practices. But the notion of 'private space' is vital to all aspects of behaviour, is relevant in 'private places' such as the home and toilet cubicle, and is also relevant in 'public places', where casual observation by the few people in the vicinity is very different from systematic observation, the recording or transmission of images and sounds.

Threats to **Privacy of Personal Communications** include mail 'covers', the use of directional microphones and 'bugs' with or without recording apparatus and telephonic interception and recording. In recent years, concerns have arisen about third-party access to email-messages. Individuals generally desire the freedom to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations.

Privacy of Personal Data is referred to variously as 'data privacy' and 'information privacy'. Individuals generally do not want data about themselves to be automatically available to other individuals and organisations. Even where data is possessed by another party, the individual should be able to exercise a substantial degree of control over that data and its use. The last six decades have seen the application of information technologies in many ways that have had substantial negative impacts on data privacy.

---

2. How is Privacy Protected?

Privacy only emerged as a distinct concern in the second half of the twentieth century. Incidental protections already existed for various aspects of privacy, however. For example, the privacy of the physical person is protected by the criminal law relating to assault. The law of confidence applies to personal data collected in any context in which 'confidentiality' exists, including (but not limited to) the particular cases of doctor and patient, lawyer and client, and priest and confessant. An overview of the law of confidence in provided in ICO (2006). Telephone conversations have been subject to prohibitions on recording and interception for many decades. There are also specific laws relating to 'Peeping Tom' / voyeurism offences.

A much broader body of law has emerged since the late 1990s, as a result of the UK's membership of the European Union, and its obligation to be consistent with such documents as the EU Charter of Fundamental Rights. This gave rise to the Human Rights

Act, including Articles 8 and 14 relating to private life and discrimination. In addition, it appears that the courts may be developing a tort of privacy, although to date its primary application appears to be in relation to the media's treatment of celebrities.

An area in which a considerable body of law has developed is privacy of personal data. A 1984 UK statute was replaced by the present EU-conformant Data Protection Act in 1998. For an assessment of the legal framework underlying data protection law, see ICO (2004).

---

3. Why is Privacy Important?

Privacy is important from a number of different perspectives.

Philosophically, particularly on the European Continent, there is a strong emphasis on people being important for their own sake. The concepts of 'human dignity' and integrity play a significant role in some countries, as do the notions of individual autonomy and self-determination. In some (though perhaps not all) traditions and jurisdictions, these are the ideas that underpin the notion and significance of human rights.

Psychologically, people need private space. This applies in public as well as behind closed doors and drawn curtains. We need to be able to glance around, judge whether the people in the vicinity are a threat, before performing actions that could be embarrassing or have other negative consequences in other contexts.

Sociologically, people need to be free to behave, and to associate with others, subject to broad social mores, but without the continual threat of being observed. Otherwise, people are reduced to the inhuman, constrained environments that have been imposed on people in other times and countries.

Economically, people need to be free to innovate. International competition is fierce, and countries with high labour-costs need to innovate if they want to sustain their standard-of-living. Cleverness has to be continually reinvented; but the chilling effect that surveillance brings with it stifles innovation. All innovators are, by definition, 'deviant' from the norms of the time, and they are both at risk, and perceive themselves to be at risk, if they lack private space in which to experiment.

Politically, people need to be free to think, and argue, and act. Surveillance can chill behaviour and speech, and undermine democracy.

Privacy grew in significance in 'advanced western nations' through the twentieth century. Key factors in its emergence as a major factor in the minds of consumer/citizens have included the following:

- There has been **sustained growth in the scale, tempo and professionalism of business and government** since the 1920s
- There has been **an increase in the 'social distance' between individuals and the institutions that serve them**. This is epitomised by the replacement of local store-owners and bank managers with data-intensive operations run from Head Office, whose 'customer interface' is now an impersonal call centre
- There has been **exponential growth in privacy-invasive information technologies** since the 1950s. This has served and reinforced the social distance between people and organisations. In addition, in recent years computing and communications have 'converged', resulting in a compounding of the threat. Relevant technologies include RFID tags, biometrics, locator technologies including mobile phone location and applications of GPS, inexpensive visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic. Such technologies have increased both the level of the threat to privacy and the public perception of that threat-level
- **Privacy-invasive technologies have become pervasive**. Many such technologies are now very widely deployed, including Internet-connected desktops and laptops, mobile phones, networked PDAs of many different kinds and CCTV. These devices are generating greatly increased data-trails and consequent enhanced capacity for inappropriate data access and data disclosures, and for location and tracking. These implications are often of less concern to the generation of people who have grown up with the technology
- There is a tendency in business and government to act as though there is a '**technology imperative**' ('because it can be done, it should be done'), because of the combined pressures of technology marketers and the need for efficiency improvements. This has not always been tempered by skepticism about the real capabilities of technologies, and understanding of the implications of applying them
- There has been an **increasing incidence of multi-organisational arrangements**, in such forms as strategic partnerships among groups of corporations, 'joined-up government', 'single-portal electronic services', and 'public-private partnerships'. In addition to creating the possibility of enhanced services, this exacerbates the privacy threat, because it tempts organisations to apply personal data to multiple purposes, and hence to break down the 'personal data silos' and 'identity silos' that were the most important form of privacy protection through the second half of the twentieth century
- Increasing **emphasis on public safety**, particularly since 2001, has resulted in the implementation of measures to protect the physical safety of the population and critical infrastructure, with little evidence of attention to their privacy impacts

People are aware that organisations acquire personal data, and that those organisations use the information to exercise power over them. Some give up with the attitude that, “they already know everything about me”. Others react strongly against the intrusiveness (the 'privacy absolutists'). Most are apathetic and seldom think about it. But many flip

between the two extremes, with privacy not mattering most of the time, but occasionally exploding into prominence (“'privacy doesn't matter until it does”).

The media have the capacity to turn a minor issue into a public furore within hours. As a result, privacy is a risk factor for many organisations. Misjudging whether the media and the public will accept has resulted in negative impacts on business enterprises and government agencies alike. For example, the public has demanded action on lack of security at a financial institution (resulting in a fine of almost £1 million for one institution), and on breaches of the Data Protection Act by several major corporations. With the growth in data-intensity and increasing use of privacy-invasive technologies, the risks of rejection and non-compliance by the public are increasing.

---

4. Why have a Privacy Strategy?

The performance of a PIA is much simpler for organisations that have a privacy strategy in place. This is because staff will be better attuned to the kinds of issues, and more aware of public concerns and of the risks that those concerns represent to the organisation's reputation.

Organisations whose operations have considerable impacts on the privacy of their customers, their staff, or indeed any other categories of people, may find themselves embroiled in media controversies from time to time, and may need to respond to enquiries from individuals, their representatives, elected officials. Moreover, they may find that realising potential value from projects is subject to risks arising from public reaction to the project's privacy profile.

Organisations that are in that position may need to undertake PIAs fairly frequently. They may also find that their staff are resistant to changes in business processes and system design that arise as a result of those PIA processes. In order to ensure that the organisation is adaptive, and that PIAs can be conducted quickly and inexpensively, strategic measures may be appropriate.

Further discussion is provided in relation to 'What is a Privacy Strategy?'.

Up to the Contents Page Publications ==>>

Version 1.0, 31 October 2007

What is a Privacy Strategy?

For many organisations that depend upon personal data, privacy has become a strategic factor. This segment of the PIA Handbook discusses how the conduct of a PIA is much easier, quicker, less expensive and more effective, if the organisation's overall strategy encompasses privacy.

To deliver value to an organisation, a PIA is best approached not as a standalone activity, but rather integrated into the organisation through two levels:

- a PIA needs to be situated within an overall organisational privacy strategy
- the organisation's privacy strategy needs to be positioned squarely within the organisation's overall strategic framework

A comprehensive approach is often referred to as an Enterprise Privacy Strategy. As with any strategy, an Enterprise Privacy Strategy needs to be proactive, and to be expressly stated rather than merely implied. Therefore, it should be articulated into a plan. Execution of the plan should be resourced, and performance should be monitored against the plan.

The scope of an Enterprise Privacy Strategy (the Strategy) should reflect the organisation's nature and mission. The remainder of this section provides guidance for determining the appropriate scope of the Strategy, and identifies four alternative approaches, ranging from the very narrow to the very broad:

1. A Minimalist Information Privacy Strategy
2. A Comprehensive Information Privacy Strategy
3. A Broad Privacy Strategy
4. A Social Impacts or Public Policy Strategy

---

1. A Minimalist Information Privacy Strategy

The most basic approach to Enterprise Privacy Strategy is to reflect the requirements of privacy law, including (but not limited to) the Data Protection Principles established by the Data Protection Act.

The minimum that an organisation that handles personal data can reasonably be expected

to do is as follows:

- develop an organisational understanding of privacy, and of the key privacy issues that arise in the organisation's relationships with individuals (generally its staff and customers)
- conduct a review of the organisation's holdings of personal data and the business processes relating to that data
- build recognition of privacy matters into its project processes (e.g. as a component of project scoping documents, or budget approvals). This should include:
    - a requirement that PIAs be considered where appropriate
    - a requirement that a Privacy Law Compliance Check be performed
    - a requirement that a Data Protection Act Compliance Check be performed

---

2. A Comprehensive Information Privacy Strategy

The Data Protection Act focusses on data privacy concepts that originated in the 1970s. Public expectations have moved well beyond those ideas, and a range of claims have emerged for more extensive forms of privacy protection. Organisations that recognise privacy as being a strategic factor in trust relationships with their staff or customers, or that recognise privacy as a matter of corporate responsibility, often implement a much more comprehensive strategy.

A Comprehensive Information Privacy Strategy involves the following measures being driven from a senior executive level, separately from and prior to the conduct of specific PIAs:

- establish and maintain a focal point that ensures **executive attention** to the matter, including commitment by senior executives to a privacy programme, appointment of a Chief Privacy Officer at a senior level within the organisation, and periodic inclusions of privacy matters in executive committee agendas
- conduct a **strategy formation process** that anticipates problems, and is based on an appreciation of the organisation's data-holdings, data practices, technologies and laws, and deals with public sensitivities in relation to the data, the practices and the technologies
- ensure that **business process engineering and re-engineering activities** have privacy-sensitivity embedded into them. This involves provisions within supplier contracts, and in the organisation's project management framework and methodology, especially during the project initiation stages, through the phases of conception, analysis, design and implementation, and on to post-implementation review and audit
- structure an **acculturation programme** that builds privacy respect into the organisation's philosophy, mind-set and business processes. This requires both

formal and informal measures. Crucial among the formal measures is the integration of elements of the PIA process within the organisation's procedural norms. A key location for acculturation is in staff training programmes. Another is internal audit of personal data practices, including both periodic audit, and on-demand audits occasioned by specific incidents and/or general concerns

- establish and maintain an **internal communications programme**, utilising such vehicles as training courses and newsletters, that keeps privacy in the minds of operational staff, managers and executives alike
- establish and maintain an **external communications programme**, comprising at least the following elements:
    - integration of privacy-related messages into communications with affected individuals (including staff as well as clients)
    - identification of relevant representative and advocacy organisations, and collection of information about them
    - creation and maintenance of channels to and from relevant representative and advocacy organisations
    - capacity to receive and handle incoming communications, through procedures for handling incidents, enquiries, submissions and complaints

A comprehensive Information Privacy Strategy is likely to encompass additional aspects beyond the basic provisions addressed in legislation, such as the following:

- protections for **all categories of people**, without restrictions such as 'citizen', 'resident' or 'customer', and with provisions related to the interests of deceased persons and their relatives
- recognition of the benefits as well as the inefficiencies involved in **'data silos'**. Such patterns as the consolidation of data from multiple sources into a single virtual databank, the use of personal data for additional purposes, 'function creep' from one business function to another, data warehousing and data mining, all encroach on privacy. The scattering of personal data has been one of the most effective forms of protection, and consolidation directly threatens privacy
- recognition of the benefits as well as the inefficiencies involved in **'identity silos'**, by avoiding the use of the same identifier in multiple organisations, systems and programmes
- approval for and facilitation of **anonymous and pseudonymous transaction services** in all circumstances where that is realistic, e.g., by means of authenticating a person's attributes rather than their identity
- **avoidance of prejudice** to the person's access to services, or their ability to exercise other rights, because of the exercise of privacy rights
- **card-holder control over identification and authentication tokens**, such as chip-cards and digital signature keys

Some of these expectations run directly counter to the organisation's orientation towards administrative efficiency, the management of waste and fraud, and an integrated view of

customers across business divisions and even across corporate boundaries to strategic partners. These tensions are at the heart of the need for PIAs.

---

3. A Broad Privacy Strategy

The Data Protection Act is to a substantial extent limited to information privacy. People are concerned about other dimensions of privacy as well, and organisations may judge it to be advantageous to define the scope of their Enterprise Privacy Strategy to reflect broader concerns.

A broad Enterprise Privacy Strategy would also encompass impacts on:

- **privacy of the person**, which relates to personal safety, and interference with the human body. This intersects with information privacy in several ways, for example in relation to locator information for persons-at-risk (e.g. of violent attacks from former partners), the identity underlying authorised aliases, sample extraction for substance-abuse testing, and biometric measures
- **privacy of personal behaviour**, which relates to surveillance of both physical and electronic activities. This also intersects with information privacy, particularly where data is recorded that may, or may become, associable with an individual
- **privacy of personal communications**, which relates to conversation and message interception, traffic analysis and access to recorded and stored messages. Similarly, this has intersections with information privacy

---

4. A Social Impacts or Public Policy Strategy

Some organisations may judge it to be advantageous to adopt a scope definition that is broader than privacy alone, but encompasses it. An Enterprise Social Impacts or Public Policy Strategy would also encompass impacts (both positive and negative) on such matters as:

- the **availability** and **quality** of services
- the **accessibility** and **equity** of services
- the **allocation of effort, costs and risks**, particularly where they are shifted in the direction of citizens
- **choice** in relation to the use of the project as a whole, including benefits foregone if it is not used, and penalties for non-use
- **consent** in relation to participation in the project as a whole, and in particular features of it, rather than legal mandation, effective compulsion, or coercion

- **job-market and industry structure impacts**
- **geographical equity impacts**, e.g. differential service depending on location or access to facilities
- **social equity impacts**, e.g. differential service depending on ethnic background, lingual skills, education or physical limitations
- the **human rights** of clients, employees and contractors
- the **accessibility of information**

[<<== Why Have a Privacy Strategy?](#) [Up to the Contents Page](#)

Version 1.0, 31 October 2007

Publications

This segment provides access to relevant documents published by:

- the Information Commissioner's Office
- Offices of Privacy Commissioners, and similar organisations, elsewhere in the world
- other individuals and organisations

If a deeper appreciation of PIAs and their history is sought, these may be found in a companion Study commissioned by this Office. **[INSERT HOTLINK]**

ICO Publications

ICO (2001) 'Data Protection Act 1998: Legal Guidance' Information Commissioner's Office, 2001

ICO (2001) 'The Complete Data Protection Audit Manual' Information Commissioner's Office, 2001

ICO (2004) 'The Legal Framework: An Analysis of the 'Constitutional' European Approach to Issues of Data Protection and Law Enforcement' UK Information Commissioner Study Project: Privacy & Law Enforcement' Paper No. 4, Information Commissioner's Office, February 2004

ICO (2006) 'Freedom of Information Act Awareness Guidance No 2 – Information Provided in Confidence' Information Commissioner's Office, January 2006

Other Official Publications

Australia (2006) 'Privacy Impact Assessment Guide' Office of the Privacy Commissioner, Sydney Australia, August 2006

New Zealand (2002) 'Privacy Impact Assessment Handbook', Office of the Privacy

Commissioner, March 2002

Ontario (2001) 'Privacy Impact Assessment: a user's guide' Information and Privacy Office, Ontario Management Board Secretariat, June 2001

Other Publications

Bennett C.J. (2001) 'What Government Should Know about Privacy: A Foundation Paper' Proc. Information Technology Executive Leadership Council's Privacy Conf., June 19, 2001

Clarke R. (2006) 'Make Privacy a Strategic Factor - The Why and the How' Cutter IT Journal 19, 11 (October 2006)

Flaherty D.H. (2000) 'Privacy Impact Assessments: an essential tool for data protection' Privacy Law & Policy ReporterReporter 7, 5 (November 2000) 85-90

Marcella A. J. & Stucki C. (2003) 'Privacy Handbook: Guidelines, Exposures, Policy Implementation, and International Issues', Wiley, 2003

Stewart, B. (1996) 'Privacy impact assessments' Privacy Law & Policy Reporter 3, 4 (July 1996) 61-64

Stewart, B. (2002) 'Privacy impact assessment roundup' Privacy Law & Policy Reporter, 9, 5 (October 2002) 90-91

Waters, N. (2001) 'Privacy impact assessment - traps for the unwary' Privacy Law & Policy Reporter 7, 9 (February 2001) 176

<<== General Resources Up to the Contents Page Glossary ==>>

Version 1.0, 31 October 2007

PIA Handbook - Glossary

This segment of the Handbook contains an alphabetical listing of terms that are used in the document in ways that are or may be seen to be in some way specialised.

Advocate

An organisation, or possibly an individual, that has plausible claims to understand the interests of some relevant group of people, including Participating Organisations and the Affected Public, particularly in newly-emerging and even hypothetical circumstances. Their credibility is based not on their ability to 'represent' any particular population segment, but rather on their capacity to appreciate and consider the complexities and the options, and to present evidence and coherent arguments

Amelioration Measure

A design feature that is intended to compensate for other, privacy-invasive aspects of a design. An amelioration measure may compensate wholly for a negative impact, or only partially

Affected Public

The people whose personal data is the subject of the project. People are affected in various ways, depending on the system's features, and people's circumstances, and hence it is often important to distinguish, and focus on, relevant customer segments

Avoidance Measure

A means of dissipating a risk. It refers to the exclusion of technologies, processes, data or decision criteria, in order to avoid particular privacy issues arising

Compliance Checking

An evaluation of a project process and project outcomes (including the design, data collections and business processes), in order to ensure that all aspects are compliant with all relevant provisions of all relevant laws

Data Silo

A database or set of files that is used by a particular application and is not integrated with other databases or sets of files

First-Order Impact

A direct result arising from some measure. Distinguished from an indirect or Second-Order Implication that is mediated by a range of other factors

Identity

A representation or role of some underlying entity, in particular of a person

Identity Silo

An identity that is used to represent an individual in that person's dealings with a particular application and is not integrated with other identities that the person has

Issues Register

A record of the privacy issues that have been identified, and the approaches adopted to avoiding or ameliorating them. In large projects it is likely to be formalised, but in other cases it may take the form of an attachment to meeting minutes, or a web-page maintained by project staff

Lead Organisation

In the case of very large projects in which several major organisations are heavily involved in partnership or joint venture, the organisation that adopts a leadership role

Mail 'Cover'

The process by which a nonconsensual record is made of any data appearing on the outside cover of sealed or unsealed mail

Organisation

The corporation or government agency that is primarily responsible for the project in relation to which a PIA is to be undertaken

Participating Organisation

Other organisations involved in the project, including 'partner' organisations,

organisations that will provide data, or receive data from the resulting system, and perhaps also organisations that provide services to support the system (e.g. as outsourced service providers) and technology providers

PIA Consultative Group (PCG)

A cluster of Representatives and Advocates with whom consultation is undertaken, which is not unduly large, but has sufficient diversity to ensure that the objectives are achieved

Privacy

The interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations

Privacy Enhancing Technology (PET)

A technology that has been specifically developed to assist privacy rather than threaten it.

Privacy Impact Assessment (PIA)

A process whereby a project's potential privacy issues and risks are identified and examined from the perspectives of all stakeholders, and a constructive search is undertaken for ways to avoid, minimise or at least ameliorate privacy concerns

Privacy Intrusive Technology (PIT)

A technology that assists in the surveillance of people and their behaviour

Privacy Law

All sources of law that create rights and obligations relevant to Privacy. They include the constitution, statutes, statutory instruments created and maintained under delegation from the Parliament (including Regulations and formal Codes), and the common law. Further documents may be relevant, such as codes of conduct and privacy policy statements, particularly where the organisation has provided some form of undertaking to comply with them. This might arise from some formal act of adoption (such as membership of the association that issues the code), or the terms of a document that the organisation itself has uttered. There are also matters of public policy that may not be formally law, but that are generally respected

Privacy Strategy

An approach driven by an organisation's senior executives, whereby privacy is recognised as a factor of significance to the achievement of the organisation's objectives. It involves the reflection of privacy concerns within corporate strategy, detailed planning and implementation of measures to address privacy issues, and the embedment of privacy-sensitivity in organisational culture and in computer-based systems

Project

The activity or function is that the organisation is assessing. It may be, for example, a project to develop a 'system', a 'database', a 'program', an 'application', a 'service' or a 'scheme', or an enhancement to any of the above, or an 'initiative', a 'proposal' or a 'review', or even draft legislation

Representative

An organisation, or possibly an individual, that has plausible claims to represent the interests of some relevant constituency, including Participating Organisations and the Affected Public. Their credibility arises primarily from their closeness to that constituency, and their ability to sense and explain their constituency's concerns

Second-Order Implication

An indirect result arising from some measure, which is mediated by a range of other factors. Distinguished from a direct or First-Order Impact

Screening Process

A short, preliminary study to work out whether a PIA is required, and, if so, how substantial it needs to be

Stakeholder

Individuals or groups that perceive themselves to have a significant interest or 'stake' in the project, and that accordingly expect to have involvement in the project process. They include the Organisation itself, other Participating Organisations and the Affected Public

---

<<== Publications Up to the Contents Page

Version 1.0, 31 October 2007

Persons at Risk, and Vulnerable Populations

Some people, in some circumstances, face particularly serious risks if their personal data is disclosed. This applies especially to their physical location or data that may result in disclosure of their physical location. It may also apply to, for example, health care or financial data. Useful generic terms for people to whom this applies are 'persons at risk' and 'vulnerable populations'.

Categories of persons whose **physical safety** is at risk include:

- **people who are under the direct threat of violence**, including:
  - people concealing themselves from previous criminal associates
  - victims of domestic violence
  - protected witnesses
  - people who have been the subject of public or private threats to their safety
- **celebrities, notorieties and VIPs**, including:
  - politicians
  - entertainers and sportspeople
  - people 'in the public eye', such as lottery winners or those who publicly promote controversial views
- **people in security-sensitive roles**, such as:
  - national security operatives
  - undercover police
  - prison warders
  - staff in psychiatric institutions

Even where physical safety is not under threat, care may still be needed in respect of **'vulnerable populations'**, some of whom may find it difficult to exercise control over their personal data. Examples include:

- children
- people with mental disabilities
- people with severe physical disabilities
- the comatose
- people in institutions, particularly for mental health and senile dementia care
- recently-released prisoners and parolees
- the homeless
- refugees
- those with certain health status

[<<== Why Do a PIA? <<== Design Issues & Privacy Problems](#) [Up to the Contents Page](#) [What Triggers a PIA? ==>> Design Issues & Privacy Problems ==>>](#)

Version 1.0, 31 October 2007

The Allocation of Effort, Costs and Risks

Effort and Costs

Any project will require investment by participating organisations. It may also impose new responsibilities on people affected by the project. Where a project does, or may, give rise to personal effort and costs to individuals, the scope of the PIA needs to be sufficiently broad to encompass them.

For example, a project in the area of 'identity authentication' and 'identity management' may impose responsibilities on people to acquire new documents or re-locate existing copies of documents, to carry the documents, and to securely store them so that they can be presented in the future. The obligations may extend to making appointments, taking time out of other activities including work, traveling to a designated location, and queuing. The person may then be subjected to one or more stressful interviews, and to bureaucratic rules that take little account of that person's particular circumstances. If they are unable to comply, people may be forced to repeat the whole process, or to depend on an impersonal bureaucracy making an exception.

People may have to bear financial costs such as registration fees or travel, may have to forego income, and may have to undertake tasks. Some of the costs and some of the efforts may have been transferred from the organisations they are dealing with, as occurs where individuals are required to capture data directly into the organisation's data processing system.

In some cases, people may be precluded from some forms of rights or entitlements, or denied some kinds of services, during the period it takes them to succeed in complying with the requirements. The preclusion or denial may even be permanent.

There may be a public perception that effort and costs are being imposed on people, whether or not it is actually the case.

Risks

People are also likely to be concerned about who bears what risks, both of a financial nature, and of a service-denial nature. Where a project embodies risks of these kinds, the scope of the PIA needs to be sufficiently broad to encompass them.

Both individuals who are subject to a scheme and organisations participating in it are likely to be concerned that risks and contingent liabilities are equitably distributed rather

than imposed on the people or organisations with the least power.

There may be a public perception that risks are being borne by individuals, whether or not it is actually the case.

[<<== Governance Arrangements](#) [Up to the Contents Page](#) [Governance Arrangements ==>>](#)

Version 1.0, 31 October 2007

Service-Provision, Quality, Access and Equity

Where a project entails certain types of risks in addition to privacy (such as quality, access and equity), an organisation may consider addressing multiple social impacts within a single process, rather than conducting an impact assessment focused solely on privacy. This is only one example of how the PIA can be integrated with other existing or necessary processes to achieve efficiency.

Commitment to **customer-service** is fundamental to the activities of business and government alike. In the public sector, the statutes under which the agency or programme operates may include provisions that require the delivery of particular services, or that achieve the same effect because they require the agency to perform particular functions.

Expectations of **quality** exist in relation to services, as they do for physical goods.

There may also be expectations about the **accessibility** of the service. This applies geographically (across urban, regional, rural and remote areas), and over time (business-hours, after-hours, weekends or around-the-clock). There may also be expectations that services be available through a range of communications channels (physical locations, telephone, over the Internet).

An aspect of accessibility that attracts particular attention is **equity**. Some forms of equity are statutorily enforced, in that discrimination on certain grounds is illegal, whereas other aspects are matters of public policy. Bases on which discrimination and equity issues might arise include:

- physical disabilities (e.g. of sight, mobility, or capacity to use a keyboard or mouse)
- mental disabilities (e.g. the inability to remember a username/password pair, or to remember to carry a token)
- educational disabilities (e.g. lack of understanding of username/password prompts, or what to do with a token)
- lingual disabilities (e.g. insufficient English to understand instructions, perhaps even the instructions on how to contact an interpreter)
- location (e.g. in an institution, in a remote area, in a rural or regional area with outdated infrastructure or inadequate bandwidth, or in a foreign country)
- lifestyle (e.g. itinerants, 'street-kids')

[<<== Governance Arrangements](#) [Up to the Contents Page](#) [Governance Arrangements ==>>](#)

Version 1.0, 31 October 2007