Privacy Impact Assessment Handbook

Version 2.0

Promoting public access to official information
and protecting your personal information

ICO

Information Commissioner's Office

Back to ICO homepage

Advice on using this handbook

Because organisations vary greatly in size, the extent to which their activities intrude on privacy, and their experience in dealing with privacy issues makes it difficult to write a 'one size fits all' guide. The purpose of this handbook is to be comprehensive. It is important to note now that not all of the information provided in this handbook will be relevant to every project that will be assessed.

The handbook is split into two distinct parts. Part I (Chapters I and II) are designed to give background information on the privacy impact assessment (PIA) process and privacy. Part II is a practical "how to" guide on the PIA process. The handbook's structure is intended to enable a reader who is knowledgeable about privacy to quickly start working on the PIA. Background information on privacy and PIAs is provided for other readers who would like some general information prior to starting the PIA process.

It is also important to note that some of the recommendations in this handbook may overlap with work which is being done to satisfy other requirements, such as information security and assurance, other forms of impact assessment or requirements to carry out broader consultations during the development of a project. A PIA does not have to be conducted as a completely separate exercise and it can be useful to consider privacy issues in a broader policy context.

The term 'project' is used in this handbook to refer to whatever the activity or function is that the organisation is assessing. However, for the purposes of this handbook it could equally refer to a system, database, program, application, service or a scheme, or an enhancement to any of the above, or an initiative, proposal or a review, or even draft legislation.

Finally, the information in this handbook is provided purely as guidance to organisations, to assist them in making their own judgements for each project that they undertake which has potential privacy impacts. Each organisation is encouraged to use the handbook to devise and implement a PIA process that is appropriate to their circumstances.

« Previous | Top of page | Next »

Back to ICO homepage

PIAs and other processes

Compliance checking and data protection audit

A PIA must be seen as a separate process from compliance checking or data protection audit processes. Often organisations ask whether a PIA can be conducted on a project that is being implemented or has been up and running for some time. The nature of the PIA process means that it is best to complete it at a stage when it can genuinely affect the development of a project. Carrying out a PIA on a project that is up and running runs the risk of raising unrealistic expectations among stakeholders during consultation. For this reason, unless there is a genuine opportunity to alter the design and implementation of a project, the ICO recommends that projects which are already up and running are not submitted to a PIA process, but to either a compliance check or a data protection audit, whichever is more appropriate.

The PIA process is considerably broader than just an audit of compliance with existing privacy related laws. 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 Chapter VI and Chapter VII of 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.

A PIA needs to be distinguished from a privacy or data protection 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.

The ICO Data Protection Audit Manual is available at www.ico.gov.uk.

Information security procedures

Many organisations feel that if they complete an information security or information assurance process that they have completed a similar process to that of a privacy impact assessment. However, while many of the issues addressed by PIAs are addressed as part of information security or assurance procedures, these are limited in scope to the needs of the organisation and do not, as a general rule, seek to garner views from a range of stakeholders who may be affected by a project.

While information security and assurance procedures will enable compliance with the law, they do not look at the broader issues of whether or not a particular project should be implemented from a privacy perspective, how to ensure that external privacy concerns are identified and addressed or whether a particular programme is compliant with the broader rights to privacy and confidentiality provided by UK and European law.

Stakeholder management

Managing the expectations of anyone who has an interest in a project or who may be affected by its outcome is vital in the public and private sectors. The PIA process will cover a lot of the same ground as stakeholder management. Again, if your organisation already has a stakeholder management strategy in place, make sure it will also address and manage the expectations of stakeholders in relation to personal privacy.

Consultation

Consultation is mandatory for many public sector projects. It is advisable to ensure that any consultation process is informed by the PIA process. This embeds the PIA process into current processes and avoids having to repeat work as part of the PIA.

« Previous | Top of page | Next »

Back to ICO homepage

Why 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.

Government and corporate reputations can be fragile and easily undermined. In order to maintain and enhance their reputations these organisations need to act responsibly in relation to key issues like privacy, and to be seen to be acting responsibly. Experience shows that once an organisation's reputation is damaged and trust is lost it is then very hard to regain that trust.

For many organisations, privacy now poses risks which need to be professionally managed in a similar way to other categories of risk. Organisations that handle personal data need to monitor their ongoing operations, whether they are dealing with clients, employees, or the public in general.

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

- Identifying and managing risks.
- Avoiding unnecessary costs.
- Inadequate solutions
- Avoiding loss of trust and reputation.
- Informing the organisation's communications strategy.
- Meeting and exceeding legal requirements.

Identifying and managing risks

At senior levels of organisations, a PIA is part of good governance and good business practice. A PIA is a means of addressing project risk as part of overall project management. 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.

Avoiding unnecessary costs

By performing a PIA early in a project, an organisation avoids problems being discovered at a later stage, when the costs of making significant changes will be much greater. Making clear 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 just as part of a privacy impact assessment.

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

Inadequate solutions

Another problem which arises with privacy risks being discovered at a later stage is that the solutions that are devised at this stage are often not as effective at addressing and managing the privacy risks as solutions that are designed into the project from the start.

Designing in privacy solutions can make a project more resistant to a failure around individual privacy and better able to recover if a failure does occur. Bolt-on solutions devised only after a project is up and running can often be a sticking plaster on an open wound, providing neither the same level of protection for the individual nor the confidence for the organisation that privacy risks have been identified and adequately addressed.

Avoiding loss of trust and reputation

Customers value privacy. A PIA is a means of ensuring that systems are not deployed with privacy flaws which will attract the attention of the media, competitors, public interest advocacy groups or regulators, or give rise to concerns among customers. In this context a PIA will help to maintain or enhance an organisation's reputation.

Addressing privacy issues raised in a PIA can mitigate the risks of low adoption rates (or poor participation in the implemented scheme) due to a poor perception of the scheme as a whole, or particular features of its design or a 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. It also helps mitigate the risk of retrospective imposition of regulatory conditions as a response to public concerns about the project, with inevitable additional and unbudgeted costs or even the entire project being put at risk of being in non-compliance with the new laws.

A PIA provides an organisation with an opportunity to obtain a commitment from stakeholder representatives and advocates to support the project from an early stage, in order to avoid the emergence of opposition at a late and expensive stage in the design process.

Informing the organisation's communications strategy

Linked to the importance of a loss of trust and reputation is the importance of a PIA to an organisation's media and communications strategy. As stated above there is a risk of the collapse of a project as a result of adverse publicity and/ or withdrawal of support by the organisation or one or more key stakeholders.

Carrying out a PIA should enable the organisation to ensure that the representative and advocacy organisations achieve an understanding of the project and assess it from their own perspectives. It enables an organisation to understand the perspectives of other stakeholders and make the aims of the project better understood. It also provides stakeholders the opportunity to have their perspectives reflected in the project design.

By actively seeking out and engaging the concerns of stakeholders, even those who are expected to oppose a particular project, you can discover the reasoning behind their position and identify where further information needs to be provided and pre-empt any possible misinformation campaigns by opponents of the project.

Meeting and exceeding legal requirements

The Data Protection Act already stipulates eight data protection principles, but these only address certain aspects of privacy. There are a range of other pieces of legislation which have an impact on privacy and either empower or prohibit certain acts which may intrude upon the privacy of the individual. These are explored in more depth in the privacy law compliance check in Chapter VI.

The Government has accepted their value and they will be used in all Departments. Future Gateway reviews of ICT projects will check that they have been carried out as an integral part of the risk management assessment.

« Previous | Top of page | Next »

Back to ICO homepage

What are the end results of an effective PIA process?

Ideally the end results of an effective PIA 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 lessen negative impacts on privacy;
- where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them; and
- documentation and publication of the outcomes.

« Previous | Top of page | Next »

Back to ICO homepage

When to do a PIA?

Making any change to specifications, and fixing any error, requires re-work which incurs delays and costs, and because it is error-prone it risks even more 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 bolted-on 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.
- 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 today, so that any major issues are identified with the minimum possible delay.

While a PIA should be conducted at an early stage of a project, compliance checks, on the other hand, are usually performed later, after business processes and rules have been specified sufficiently so that they can be assessed for their compliance with the law. 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 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; and
- re-visited in each new project phase.

Each version 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 versions can correspond with the later phases of the project (eg requirements analysis, logical design, physical design, construction, integration and deployment of the new system, or their equivalents in whichever project method the organisation uses).

« Previous | Top of page | Next »

Back to ICO homepage

Managing a PIA

This section provides some further guidance on managing the PIA process, who should take responsibility, who carries out the PIA and the role of the organisation's data protection/ privacy officer.

Who should take responsibility for a PIA?

Responsibility for conducting a PIA should be placed at senior executive level. A PIA has strategic significance, and therefore, direct responsibility for the PIA must be assumed by a senior executive. It might also be advisable to assign this responsibility to a senior executive with lead responsibility for risk management, audit or compliance.

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

- ensure effective management of the privacy impacts arising from the project;
- ensure effective management of the project risks arising from the project's privacy impacts; and
- 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.

Who should carry out a PIA?

In delegating responsibility for conducting a PIA, senior executives have three alternatives:

- an appointment within the overall project-team;
- someone who is outside the project; or
- an external consultant.

Where responsibility is delegated to a senior member of the project team, this 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.

If the executive delegates responsibility for the PIA to someone outside the project team, it may be difficult for that person to ensure a balanced appreciation of the views of all stakeholders and to assimilate the information generated. There is a possibility that the project team might resist the conclusions and recommendations that result from the PIA process.

Some organisations have decided to employ external consultants to carry out a PIA, either because they feel that they do not have the necessary skills in-house, or they want the PIA to be as independent as possible from potential influences within the organisation. While there are sometimes good reasons for ensuring the independence of the PIA process, this handbook has been designed as a self-assessment tool. The advantages of employing an independent consultant need to be weighed against the disadvantages of resistance to the conclusions reached during the PIA, the potential lack of understanding or appreciation of the organisation's needs and the business case for the project. As stated above, a PIA is distinct from an audit process and so there is not as great a need for independence throughout the process.

Regardless of who is asked to complete the PIA, the organisation must take direct responsibility for the PIA team's work, rather than delegating it. 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.

The PIA project steering committee

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).

A project steering committee normally has the power to give directions to the project, whereas an advisory, reference or consultative group does not. The title of any such body, however, is the choice of the organisation concerned and should be consistent with terms used for similar groups.

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; and
- representatives of, and advocates for, the various stakeholders.

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; and
- the roles and responsibilities of various parties involved in the PIA.

The terms of reference should 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.

Role of the organisation's data protection/ privacy officer or team

Often an organisation will delegate responsibility for conducting a PIA to their data protection or privacy officer. While the ICO recommends that this person is given a role in the steering committee or consultative group, responsibility should only be delegated to the data protection or privacy officer where they have sufficient authority to influence the design and development of a project and participate fully in the project design decisions.

Resourcing a PIA

Sufficient resources must be made available to enable effective and efficient performance of the PIA. There are two aspects to this.

- The members of the PIA team itself need to be provided adequate time to carry out the PIA. The senior executive with overall responsibility for the project may need to temporarily reallocate responsibilities 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.

Role of the Information Commissioner’s Office

The Information Commissioner’s Office provides information and guidance to support the organisations that carry out PIAs, in particular through publication of this handbook. In addition, the ICO may be available for consultation on particular projects.

However, it needs to be emphasised that PIAs have been designed as a self-assessment tool for organisations and the ICO does not have a formal role in conducting them, approving or signing off any final report which is produced.

« Previous | Top of page | Next »

Back to ICO homepage

Conducting the PIA process

It is sensible 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 section provides an outline description of a suggested set of phases. 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 to use terms that are consistent with their own internal standards, policies and practices. The five phases of a PIA are as follows.

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.

2. Preparation 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 recognition of problems, and the search for solutions.

4. Documentation phase

The purpose of this phase is to document the process and the results. The suggested deliverable is a PIA Report.

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 PIA project plan

A full-scale PIA is sufficiently important and complex that it may itself warrant a formal project plan. More detailed guidance in relation to the phases, tasks and outcomes involved in a PIA is provided in the following parts. 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.

PIAs across more than one project

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

- Procuring 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.

« Previous Next »

Back to ICO homepage

What is privacy?

Interpreted most broadly, privacy is about the integrity of the individual. It therefore encompasses many aspects of the individual's social needs.

However, for the purposes of completing a privacy impact assessment (PIA) , it is more useful to examine different aspects of privacy. A PIA could consider:

- the privacy of personal information;
- the privacy of the person;
- the privacy of personal behaviour; and
- the privacy of personal communications.

These four aspects of privacy will obviously overlap and should be seen as working guides to the issues a PIA should explore, rather than strict definitions.

Privacy of personal information 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 impacts on information privacy.

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 separate human rights rather than as aspects of privacy. Issues that are more readily associated with privacy include body searches, compulsory immunisation, 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 as optical surveillance and 'media privacy'. It could relate to matters such as sexual preferences and habits, political or trade union 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.

Privacy of personal communications could include various means of analysing or recording communications such as 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.

« Previous | Top of page | Next »

Back to ICO homepage

How is privacy protected?

Privacy is protected by a patchwork of laws that overlap with or protect specific aspects of privacy. English common law provides protection for information with a quality of confidence and which has been provided in circumstances that create an obligation of confidence from unauthorised use. Telephone conversations have been subject to prohibitions on recording and interception for many decades.

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 European Convention on Human Rights. This gave rise to the Human Rights Act, including Articles 8 and 14 relating to private life and discrimination. The Data Protection Act 1998 regulates the processing of information relating to individuals, including the collection, use and disclosure of such information. 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.

A more extensive list of laws which affect or protect privacy rights in the UK can be found in Chapter VI legal compliance checking.

« Previous | Top of page | Next »

Back to ICO homepage

Why is privacy important?

The general public have shown a growing awareness of privacy issues over the last few years. High-profile losses of personal information and growing concerns about the nature and extent of personal information collected by organisations has led to a growing debate about the impact on privacy.

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 what the media and the public will accept has resulted in negative impacts on business enterprises and government agencies alike. With the growth in data-intensity and increasing use of privacy intrusive technologies, the risks of a project or scheme being rejected by the public are increasing.

« Previous | Top of page | Next »

Back to ICO homepage

Privacy risks

What do we mean by ‘privacy risks’?

The enormous increases in the collection, storage, use and disclosure of personal data, and the imposition of many intrusive technologies, have caused increased concern about individual privacy.

Privacy risks fall into two categories.

i. Risks to the individual as a result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information.

ii. Risks to the organisation as a result of:

- perceived harm to privacy;
- a failure to meet public expectations on the protection of personal information;
- retrospective imposition of regulatory conditions;
- low adoption rates or poor participation in the scheme from both the public and partner organisations;
- the costs of redesigning the system or retro-fitting solutions;
- collapse of a project or completed system;
- withdrawal of support from key supporting organisations due to perceived privacy harms; and/ or
- failure to comply with the law, leading to:
    - enforcement action from the regulator; or
    - compensation claims from individuals.

Recognising privacy risks

It is important to note that any collection, use or disclosure of personal information has the potential to have a risk to personal privacy. Sometimes those risks are not obvious and as a result it can be easy to overlook or not adequately address them.

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. However, because of project complexities and the diversity of interests among stakeholders, the consultation processes may sometimes create the need for parts of the project and its design to be re-considered.

This section provides some guidance on the type of risks, impacts and vulnerabilities you might look for when designing a project or conducting a PIA.

Broad personal information issues, including:

- The nature of the personal information. This could include “sensitive personal data” as defined by the Data Protection Act 1998, but also personal financial information, family structures, home and personal email addresses, information about persons considered “at risk”, travel plans etc.
- The quality of personal information. This includes characteristics of the information itself, such as accuracy, relevance and adequacy. The further personal information moves from its original context,

the greater the likelihood it can be misinterpreted. The quality of information also raises questions about data matching and mining, whether you are matching like with like and the number of false matches which may be produced.

- The meaning behind terms used in personal information. This takes into account that terms used can be context or sector specific. Variations in meaning of apparently similar terms may give rise to misunderstandings or error which in turn could result in harm or disadvantage to the individual. This area would also include examining metadata attached to personal information.
- The retention, deletion and destruction of personal information. How long do your business needs require retention of information? Are there legal obligations to dispose of or retain data? Do you need to keep information to counter legal claims or for audit and inspection purposes? Can your organisation make better use of ‘soft deletion’, where after the original purpose has been met, access to the information is much more tightly controlled until the organisation can permanently delete it?
- The protection of personal information. This includes 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; and
    - resources for investigating breaches and applying sanctions.

Issues around identification of the individual, including:

- the multiple use of different identifiers;
- the denial of anonymity, identifying individuals where it is only necessary to authenticate rights to benefits, access and services;
- identifiers that directly disclose personal data, for example 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; and
- the use of biometric identifiers.

Function creep, beyond the original context of use, in relation to the use of personal information or the use of identifiers.

Registration and authentication processes, including the burden such processes impose, their intrusiveness, and the exercise of power by government over individuals.

Surveillance, whether audio, visual, by means of data, whether electronically supported or not, and whether the observations are recorded or not.

Location and tracking, whether within geographical space or on networks, even where it is performed incidentally, and especially where it gives rise to a record. From the perspective of privacy protection, there are considerable privacy benefits in decentralisation rather than centralisation. The benefits include:

- reducing the risk of function creep;

- enabling the application of access controls;
- encouraging a focus on relevancy;
- reducing the misinterpretation of data due to a loss of context; and
- increasing the likelihood of prompt data destruction when it is no longer required.

Where a project involves centralising information, it is important that there is clear justification. Further, those who want to use information in a more speculative manner (such as ‘statistical analysis’, ‘management reporting’ and ‘data mining’) need to be challenged for greater detail, and to show that benefits will be achievable. Once a case for centralisation has been established, it is necessary to identify, assess and balance the disadvantages.

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 document the issues which are identified.

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 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 might include younger children or adults who lack capacity to provide consent. Your organisation might also want to consider the difficulties faced by individuals who are homeless, those who are or have been recently been in prison or refugees. Certain health conditions might also put individuals at risk if inappropriately disclosed.

Issues around the exercise of rights by individuals, such as whether personal information can be quickly and expediently identified, accessed, corrected or deleted. You should also consider whether an individual is disadvantaged in any way if they choose to assert their rights.

Future economic and social developments can also be considered.

Relevant legal considerations need to be taken into account, including liabilities that may arise and changes to regulatory impositions which may be necessitated by the project or by the public reaction to your project.

The conclusions regarding design features should be documented in the ‘issues register’, and provided to the project team as a whole. This is described in the later activities of the consultation and analysis phase.

« Previous | Top of page | Next »

Back to ICO homepage

Identifying privacy solutions

Once you have identified and assessed the privacy risks your project presents, you need to consider what action you intend to take in relation to each risk. At this stage you have three options:

- accept the risks, impacts or liabilities;
- identify a way to avoid the risks (a privacy impact avoidance measure); or
- identify a way to mitigate the risks (a privacy impact mitigation measure).

Accepting the risks

In some instances, because of the nature of the risks, impacts or liabilities, the chances of the risks being realised or the minimal impact they may have, it might be entirely appropriate to simply recognise and accept the privacy risks or certain aspects of the privacy risks. However, this must not be done simply as an alternative to taking action to address risk and must be considered carefully as an option. If considering this option, ensure that a record of the identified risk is made, along with the reasons for accepting the risk.

Privacy impact avoidance measures

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:

- minimising the collection of personal information to what is strictly necessary;
- non-collection of contentious data-items;
- active measures to stop or block the use of particular information in decision making (a good example of this is ethnic monitoring forms being filled out anonymously when companies are recruiting);
- active measures to preclude the disclosure of particular data-items, for example screening or hiding of certain services which are being provided to the individual which might disclose other personal information;
- non-adoption of biometrics in order to avoid issues about invasiveness of people’s physical selves.

Privacy impact mitigation measures

A mitigation measure is a feature that compensates for other, privacy intrusive aspects of a design. A mitigation measure may compensate partially or wholly for a negative impact. Examples include:

- minimisation of personal data retention by not recording it;
- destruction of personal information as soon as the transaction for which it is needed is completed;
- destruction schedules for personal information which are audited and enforced;
- limits on the use of information which has been collected for 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 system, backed by serious sanctions and enforcement powers. Problems must be analysed, to devise acceptable avoidance and mitigation measures. The following suggestions are made about the process of problem analysis:

- The differing perspectives of the multiple stakeholder groups should be reflected.
- The focus 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?

Privacy by design

Further information about the technologies, processes and methodologies which can be used to address privacy risks is available in the ICO “Privacy by Design” report.

« Previous | Top of page | Next »

Back to ICO homepage

PIA process – an overview

Initial assessment

Examines the project at an early stage, identifies stakeholders, makes an initial assessment of privacy risk and decides which level of assessment is necessary.

Full-scale PIA

Conducts a more in-depth internal assessment of privacy risks and liabilities. Analyses privacy risks, consults widely with stakeholders on privacy concerns and brings forward solutions to accept, mitigate or avoid them.

Small-scale PIA

Similar to a full-scale PIA, but is less formalised. Requires less exhaustive information gathering and analysis. More likely to be used when focusing on specific aspects of a project

Privacy law compliance check

Focuses on compliance with various "privacy" laws such as HRA, RIPA and PECR as well as DPA. Examines compliance with statutory powers, duties and prohibitions in relation to use and disclosure of personal information.

Data protection compliance check

Checklist for compliance with DPA. Usually completed when the project is more fully formed.

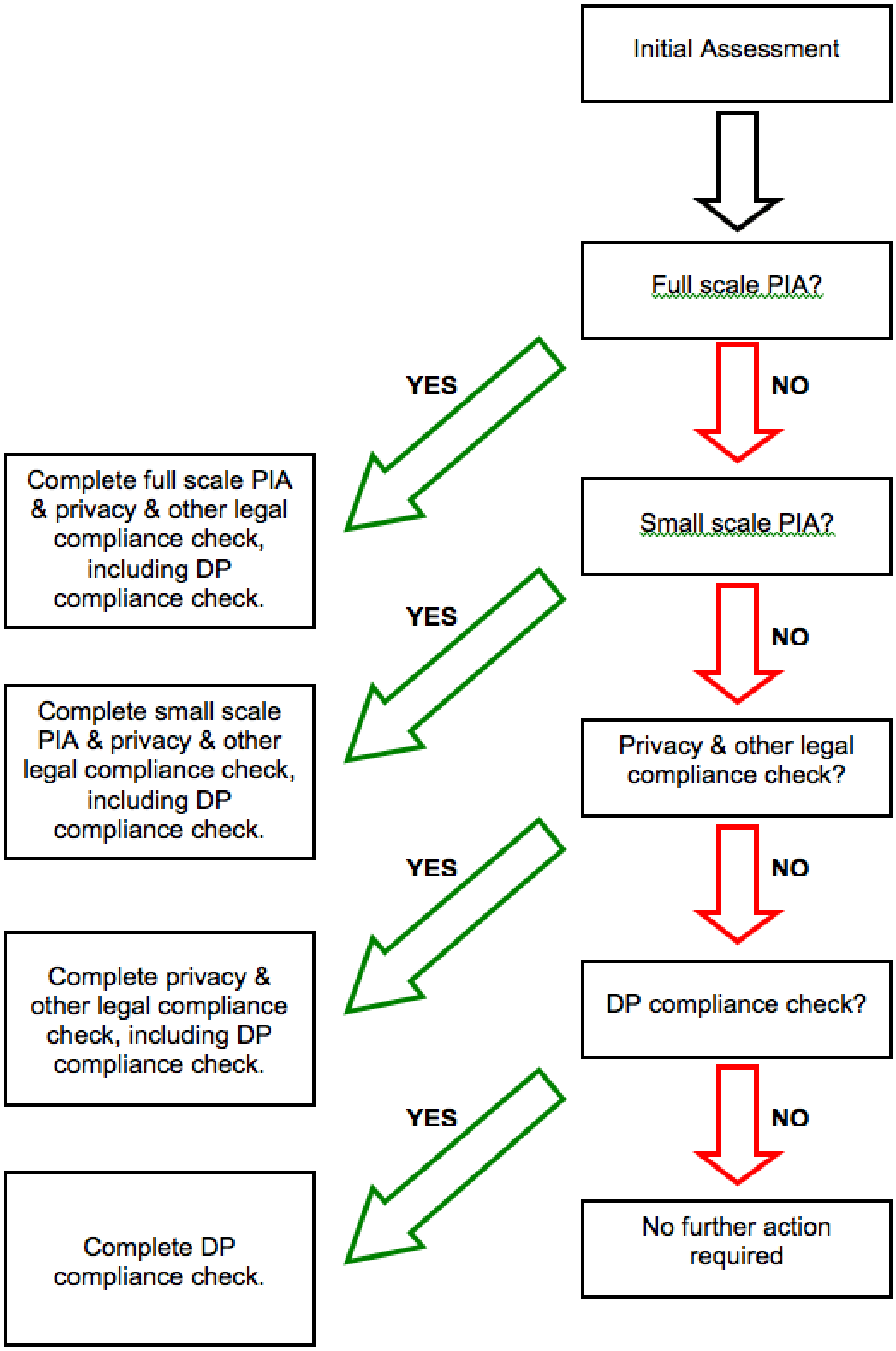
Review and redo!

Sets out a timetable for reviewing actions taken as a result of a PIA and examines their effectiveness. Looks at new aspects of the project and assesses whether they should be subject to a PIA.

« Previous | Top of page | Next »

Back to ICO homepage

PIA Decision Tree



Initial Assessment

Full scale PIA?

YES

Complete full scale PIA & privacy & other legal compliance check, including DP compliance check.

NO

Small scale PIA?

YES

Complete small scale PIA & privacy & other legal compliance check, including DP compliance check.

NO

Privacy & other legal compliance check?

YES

Complete privacy & other legal compliance check, including DP compliance check.

NO

DP compliance check?

YES

Complete DP compliance check.

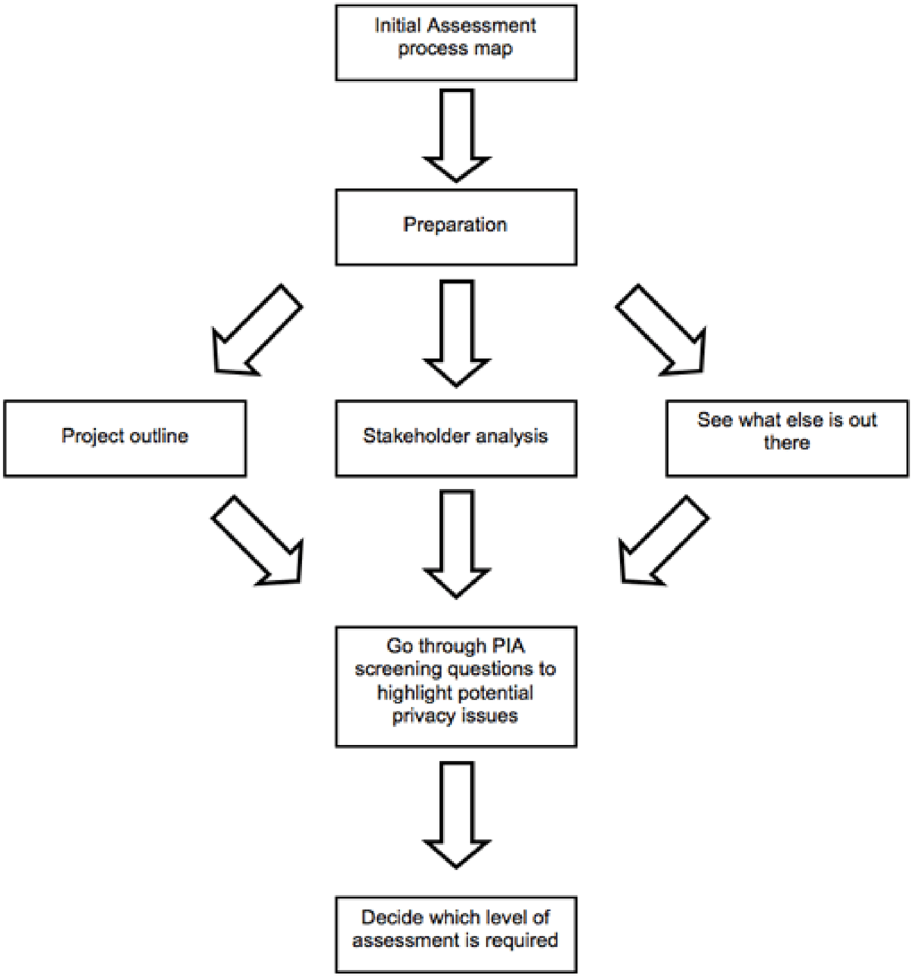
NO

No further action required

« Previous | Top of page | Next »

[Back to ICO homepage]

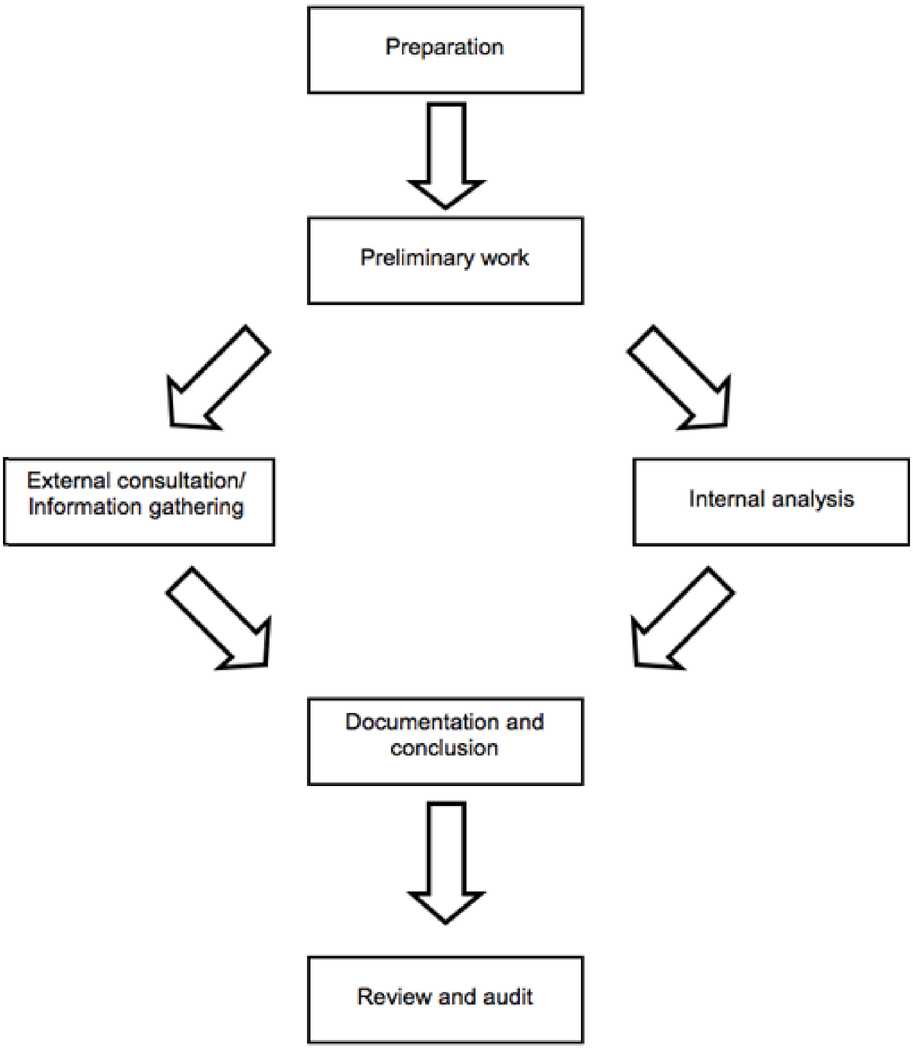
Initial Assessment Process Map


Initial Assessment process map
Preparation
Project outline
Stakeholder analysis
See what else is out there
Go through PIA screening questions to highlight potential privacy issues
Decide which level of assessment is required

« Previous | Top of page | Next »

Back to ICO homepage

Full Scale and Small Scale PIA Process Map


Preparation
Preliminary work
External consultation/ Information gathering
Internal analysis
Documentation and conclusion
Review and audit

« Previous | Top of page | Next »

Back to ICO homepage

How to determine if a PIA is needed

This section provides some guidance on how you determine whether a privacy impact assessment (PIA) would be recommended for your project and, if so, what level of PIA is required.

This is a fairly short process but provides a basis for the work you will do when it comes to actually completing a PIA or checking legal compliance. It can be very expensive for an organisation to discover too late that a project has substantial privacy impacts. On the other hand, it would be a waste of resources to unnecessarily carry out a PIA, or complete a full-scale PIA where only a small-scale PIA is needed. It is therefore worth doing some preliminary evaluation to determine whether a PIA is necessary and what level of PIA is required.

There are two stages – preparation and a series of screening questions.

« Previous | Top of page | Next »

Back to ICO homepage

Preparing for the PIA screening process

Sufficient information must be gathered to allow the questions in the screening process to be applied. It is possible that there will not be enough available information about the project to enable a clear conclusion to be reached in respect of any particular aspect. To help ensure that enough information is available to decide which level of PIA, if any, is required, the following three pieces of information are needed:

- a project outline;
- a stakeholder analysis; and
- an environmental scan.

The screening process questions are likely be answered (at least provisionally) on the basis of this information.

Obtain or develop a project outline

During the early stages of a project, there is only limited documentation available, and there may be uncertainty about the project's scope and the features of the intended system.

To ensure that you know what the project's aims are and to start thinking about what the potential impact of the project might be, make sure you get a copy of the project initiation documents, such as a project charter or terms of reference.

If such documents are not available, consult with relevant staff in the lead organisation, key stakeholders, members of the project steering committee, and perhaps others as appropriate to the circumstances. From this information, a relatively short description of the project can be prepared if necessary, as a basis for subsequent analysis.

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

Any previous PIAs 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, will be useful when preparing a project outline.

Undertake a stakeholder analysis

This involves making a list of any groups or organisations who may have an interest in, a role to play in delivering, or be affected by your project. This could include:

- the organisation conducting the project, and 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; and
- organisations that provide technology and services to enable it.

At this stage you want to have as broad a list of groups as possible with a very brief description of the stake each group might have in the project. This list can be edited down later for more focused consultation. At this stage any analysis of stakeholders should be brief, ideally a one page summary.

See what else is out there

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.

The following sources 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, eg in the consumer rights arena.
- Consultations with non-government organisations that represent or provide advice to those potentially affected by the project.

These investigations may reveal 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 rest of the preparation work, this does not have to be exhaustively catalogued, a one to two page summary, with reference to working documents generated during the process should be enough.

« Previous | Top of page | Next »

Back to ICO homepage

The PIA screening questions

Once you have completed the preparation and gathered the information together, you can carry out the screening process. This involves applying criteria described in the following section of the handbook.

The purpose of the screening process is to ensure that the investment the organisation makes is proportionate to the risks involved. Depending on the scope and size of the project, only some elements of this handbook will be relevant in any given case.

This part of the handbook contains a PIA screening tool. Answering these four sets of questions about the project should provide an indication of whether a PIA is needed, and if so, whether the project requires a full-scale PIA, a small-scale PIA or just a check against compliance with the law.

The following section shows the decision making process for conducting a PIA.

Is a full-scale PIA recommended?

Do the key characteristics of the project indicate that a full-scale PIA is needed?
See the screening questions in Appendix 1 Step 1.
If yes then conduct a full-scale PIA (Chapter IV), a privacy law compliance check (Chapter VI) including data protection compliance check (Chapter VII).
If a full-scale PIA is not recommended then:

Is a small-scale PIA recommended?

Do the project characteristics indicate that a small-scale PIA is needed?
See the screening questions in Appendix 1 Step 2.
If yes then conduct a small-scale PIA and a privacy law compliance check (Chapter VI) including data protection compliance check (Chapter VII).
If a small-scale PIA is not recommended then:

Is privacy law compliance checking recommended?

Are any of the activities subject to any form of privacy law?
If yes then conduct a privacy law compliance check (Chapter VI) including data protection compliance check (Chapter VII).
If a privacy law compliance check is not recommended then:

Is Data Protection Act compliance checking recommended?

Do the activities involve the handling of ‘personal data’?
If yes then conduct a data protection compliance check (Chapter VII).

« Previous | Top of page | Next »

Back to ICO homepage

Make an initial assessment of the privacy risks

Once you have gone through all of the other steps outlined above, you will be in a position to list some of the initial privacy impacts, risks and vulnerabilities that the project might present. This is an initial view which you can use to inform how you complete your PIA, what questions you ask stakeholders and what problems might arise during implementation of the project.

However, you must be clear that this is merely a first attempt at identifying privacy risks and has been very much considered from the perspective of your organisation. During the PIA stakeholders might raise concerns that you have not considered or might put much greater weight on concerns you identified but dismissed.

« Previous | Top of page | Next »

Back to ICO homepage

The five stages of a full-scale PIA

This section of the handbook provides more in depth advice and guidance on the five phases of a full-scale privacy impact assessment (PIA).

- Preliminary phase.
- Preparation phase.
- Consultation and analysis phase.
- Documentation phase.
- Review and audit phase.

1. Preliminary phase

This is phase one of the five-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 the outcomes and documents from the initial assessment. If necessary, prepare any documents that were not produced during the initial assessment and which might be helpful in completing the PIA.
- Develop the project outline produced in the initial phase.
- Ensure at this stage that the terms of reference, the scope and the resources dedicated to the PIA are appropriate.
- 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.
- Conduct a preliminary analysis of privacy issues. This is likely to commence with a deeper re-consideration of the outcomes of the screening process.
- Prepare the project background paper. This document will establish the basis for discussions with stakeholders.

Developing the project outline

You will have produced or got hold of an outline or background paper for the project that is subject to the PIA. The preliminary phase of the five-phase PIA process leads to the development of this project background paper. The following provides guidance in relation to its content.

The purpose of the project background paper is to establish a sound base for the subsequent preparation, consultation and analysis. 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 the 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 lead organisation at the time the document is prepared.
- Brief descriptions of options and sub-options that the lead organisation 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:
    - an 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 help the identification and collaborative examination of privacy risks and, ultimately, in having an effective PIA.

This process of rigorous challenge and justification for privacy-intrusive 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 important that information is not withheld because it exposes poor thinking.

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; and
- biometrics.

« Previous | Top of page | Next »

Back to ICO homepage

2. Preparation phase

This is phase two of the five-phase PIA process.

The purpose of this phase is to make the arrangements needed to enable the critical phase three 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:

- Develop a consultation plan to ensure 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.

Developing a consultation plan

Any project that is sufficiently complex and potentially privacy-threatening that it requires a full-scale PIA is likely to affect many parties. To ensure you make the most of the consultation and analysis phase, it is useful to put a consultation plan in place.

Remember that any consultation should be appropriate to the scale, scope and nature of the project for which a PIA is being completed. Large-scale projects that embody significant privacy risks, might use most or all of the methods described below. In small-scale projects it may not be necessary to use all of these. Some organisations might already have a well-developed consultation strategy in place and there is no reason why any PIA consultation cannot be completed within this strategy. For those organisations who do not have a consultation strategy in place, further advice is provided below.

Effective consultation depends on all stakeholders being sufficiently well-informed about the project, having the opportunity to convey their perspectives 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. Some useful ways of ensuring effective consultation include:

- priming of discussions by providing some initial information about the project;
- making sure there is ongoing dialogue with consultees throughout the PIA process;
- 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;
- making sure that there is sufficient diversity among those groups or individuals being consulted, to ensure that all relevant perspectives are represented, and all relevant information is

gathered;

- making sure that each group has the opportunity to provide information and comment, even including multiple rounds of consultation where necessary;
- making sure that the method of consultation suits the consultation group, for example using workshops or focus groups as an alternative to, or even as well as, formal written consultation;
- making sure that the information provided by all parties to the consultation is fed into the subsequent rounds of design and implementation activities; and
- ensuring that the perspectives, concerns and issues raised during the consultation process are seen to be reflected in the outcomes of the PIA process.

Devise communication processes that will enable the effective interchange of ideas. This may involve workshops and meetings, perhaps supplemented by formal submissions.

Where security considerations or indeed other privacy concerns prevent the consultation processes from being fully open, it is suggested that:

- the PIA be undertaken in as open a manner as is possible;
- parts which have security concerns be separated into closed or confidential appendices and separate, relatively closed discussion sessions; and
- where security considerations result in the suppression of information, proxy measures be devised that are as effective and credible as possible. (For example, the security-sensitive information could be provided to a trusted third party who could then deliver to PCG members evaluative comments that avoid exposing the information).

« Previous | Top of page | Next »

Back to ICO homepage

3. Consultation and analysis phase(s)

This is phase three of the five-phase PIA process.

It involves consultations with stakeholders, risk analysis, and identification of problems and the search for solutions. The purpose of this phase is to ensure that problems are identified early, that effective solutions are found and that the design is adapted to include those solutions. The suggested deliverables are changes to the project documents, an issues register, and a privacy design features paper. The following tasks are suggested:

- Implement the consultation plan that was established during the previous phase.
- Identify the design issues and privacy problems with the project.
- Re-consider the design options. This focuses on the various approaches that are available to solve problems.
- Document the problems and solutions in an 'issues register'. There is a risk with large projects that corporate memory will be lost if the PIA is carried out in stages. 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. The issues register also serves as a means to note issues that cannot be addressed immediately and avoid the possibility of them being overlooked.
- Reflect the conclusions reached, in the issues register and/ or in an evolving 'privacy design features paper'. This documents:
    - issues identified;
    - avoidance and reduction measures considered and either rejected or adopted;
    - design changes to be undertaken as a result; and
    - outstanding issues.
- Provide the privacy design features paper to:
    - the PCG; and
    - the project team.
- Pass the project team's feedback to the PCG.
- Conduct further consultations with the PCG.
- Incorporate the decisions on privacy design features into the design.
- Where there are unresolved issues, continue consultation and analysis.

This phase generally involves repeating the exercise a number of times. The most effective approach is to conduct the exercise first at the stage of project initiation, and arrange subsequent run-throughs to correspond with the later phases of the project (eg requirements analysis, logical design, physical design, construction, integration and deployment of the new system).

The project background paper is likely to require progressive changes 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 reduce or avoid privacy intrusion. Late changes can of course be expensive. This is an important reason why early commencement of a PIA is recommended.

« Previous | Top of page | Next »

Back to ICO homepage

4. Documentation phase

This is phase four of the five-phase PIA process.

A privacy impact assessment is a process. The benefits to the organisation that conducts it arise mainly 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 mitigation 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).

The reasons for preparation of a PIA report are:

- as an element of accountability, in order to demonstrate that the PIA process was performed appropriately;
- to provide a basis for post-implementation review;
- to provide a basis for audit;
- to provide corporate memory, ensuring that the experience gained during the project is available to those completeing new PIAs if original staff have left; and
- to enable the experience gained during the project to be shared 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 privacy intrusion and its implications.
- Discussion of alternatives considered and the rationale for the decisions made.
- A description of the privacy design features adopted to reduce and avoid privacy intrusion and their implications of these design features.
- An analysis of the public acceptability of the scheme and its applications.

Possible sources for the content of the PIA report include:

- 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 appendices to the PIA report:

- the Privacy law compliance study; and
- 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.

« Previous | Top of page | Next »

Back to ICO homepage

5. Review and audit phase

This is phase five of the five-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 following tasks are suggested:

- Undertake a review of the implementation of the mitigation and avoidance 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 the 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 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.

« Previous | Top of page | Next »

Back to ICO homepage

Overview

Projects with potentially substantial privacy impacts warrant a full-scale privacy impact assessment (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 in Chapter III has highlighted through the application of the criteria for small-scale PIA in Appendix 1, Step 2.

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, and
- it is more likely to be focused on specific aspects of a large-scale 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 part draws on the full-scale privacy impact assessment process described in Chapter IV 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 a small-scale PIA is appropriate, and its key characteristics.
- The PIA process:
    - preliminary phase;
    - preparation phase;
    - consultation and analysis phase(s);
    - documentation phase;
    - review and audit phase.

« Previous | Top of page | Next »

Back to ICO homepage

Why do a small-scale PIA?

The scope of the PIA should reflect the nature of the project as a whole. By conducting a full-scale privacy impact assessment on every project, regardless of its nature, scale or scope, an organisation may be committing too much resource for a project of limited scale or scope. This may lead to the PIA process being perceived as not delivering value for the organisation.

There is also a danger that too much full-scale public consultation may lead to fatigue among stakeholder groups, who themselves do not have the resources to devote to providing so many consultation responses. As a result, stakeholders may begin to channel resources into higher profile projects. This can lead to the PIA process not achieving one of its core aims of representing the privacy concerns from all perspectives, particularly in more limited projects.

A small scale PIA can be more readily scaled to fit the scale, scope and nature of a smaller project and will require less investment by the organisation.

« Previous | Top of page | Next »

Back to ICO homepage

Examples of projects for which a small-scale PIA may be appropriate

The following are examples of a range of different kinds of projects for which a small-scale PIA is more likely to be appropriate.

- 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, eg 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 (eg, replacement of bar-code or magnetic-stripe technology with a contact-based chip containing the same data).
- Drafting of new procedures for customer authentication, eg, 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.

« Previous | Top of page | Next »

Back to ICO homepage

The small-scale PIA process

The process for completing a small scale PIA for any particular project needs to reflect:

- the nature of the project (eg 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; and
- the organisation's level of experience in conducting PIAs.

Hence the following guidance is intended to assist organisations in developing their own small-scale PIA. 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.

These phases mirror the detailed guidance for the relevant phase of a full-scale PIA. In a small-scale PIA it may be appropriate to compress phases together, consolidate tasks, or reduce the number of deliverables by merging several documents into one.

The following suggested phases are described below:

1. preliminary phase;
2. preparation phase;
3. consultation and analysis phase(s);
4. documentation phase; and
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 or get hold of a project background paper, although this is likely to be quite short.

Because the circumstances in which a small-scale PIA should be conducted 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 in Chapter IV. Carrying out all the tasks recommended in the checklist would be excessive for a small project but the ideas can be of assistance, and may be applied in a less onerous manner such as in combination or selectively according to the circumstances.

At the very least, the preliminary phase should have as deliverables a project outline, a preliminary assessment of privacy concerns and some preliminary talks with key stakeholders. A clear and informative project outline will make the consultation and analysis phase much easier and more effective.

2. Preparation phase

The purpose of the preparation phase is to make the arrangements needed to enable the critical phase three 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). Due to the nature of a small-scale PIA, these tasks do not need to be formalised.

It will be useful to consult the checklist which describes the tasks involved in the corresponding phase of full-scale PIAs in Chapter IV. It is likely that not every task will be appropriate to a small-scale PIA or that some of the tasks completed as part of a full-scale PIA will need to be scaled back in order to be appropriate to a small-scale PIA.

3. Consultation and analysis phase(s)

The consultation and analysis phase builds on the foundations established by the first two sections. It includes consultations with stakeholders, risk analysis, the articulation of problems, and the search for constructive solutions.

Consultation does not have to be a formal process and can be limited to the stakeholders who have a key interest in the project or those who may have the biggest concerns about the project. It may, depending on the size of the project, be limited to a meeting or workshop with the key stakeholders, a series of short telephone interviews or even involve simply writing to the key stakeholders.

Sometimes, projects and systems may develop during the PIA process, in particular where concerns have been raised by stakeholders. As such, it can sometimes be useful to carry out several consultations over time to update stakeholders on developments and ask for further feedback as to whether this has addressed their concerns. 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 sufficient to carry out one consultation exercise.

The key deliverable is a document (such as a privacy design features paper or a meeting outcomes report) that details the privacy impacts identified and the solutions or actions which will be taken to deal with them. This document must be in a form which can be published and provided to the various parties involved in the consultation. The project team, and in particular the designers, should receive copies 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.

Again, the corresponding guidance for the consultation and analysis phase as part of a full-scale PIA described in Chapter IV provides a list of tasks which can be scaled back as appropriate for a small-scale PIA.

4. Documentation phase

The documentation of a full-scale PIA will justify more extensive documentation than a small-scale PIA. The purpose of the documentation phase is to document the process and the outcomes. The deliverable is a PIA Report, which may draw heavily on the document produced during the consultation and analysis phase. Depending on the context, this might be a relatively brief ‘note to file’, with copies to relevant parties; but circumstances may justify a more carefully prepared document.

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 or update 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, a more detailed document may be required.

Back to ICO homepage

The importance of compliance checking

The organisation must ensure that the project, the personal data that it handles, and the business processes it uses are compliant with all relevant laws. Compliance checking should be started at an early stage of the project to address issues such as the legality of any proposed course of action, but this work will normally only be completed later, once the design of the project has reached a more detailed stage.

While compliance checking as part of a privacy impact assessment (PIA) will focus on laws which affect privacy, organisations will have to consider broader legal compliance as well. Public sector organisations will have to consider the extent of their powers, any obligations they have in relation to the personal information they collect and any prohibitions on the use of that information. Private sector organisations will have to consider industry standards and 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 membership of an association that issues the code, or the terms of a document that the organisation itself has produced. There are also matters of public policy that may not be formally law, but that are generally respected.

Chapter VII of the handbook provides guidance in relation to compliance with the Data Protection Act and the Privacy and Electronic Communications Regulations. This section relates to broader elements of the law but any legal compliance checking should include these areas.

Responsibilities

The organisation proposing the project is responsible for undertaking a survey of the law relevant to the project and to the data processing and business processes it gives rise to. All participating organisations should do the same in connection with their involvement in the project.

Professionals with relevant expertise should be consulted as part of checking compliance with privacy law and other legal obligations. If your organisation has an in-house compliance unit or established compliance process, it might be useful to ensure that the compliance checking process takes full account of privacy law obligations and adds to the compliance checking process if necessary.

Potentially relevant sources of the law

You can refer to the examples of relevant laws 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 other laws that may be relevant.

- 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, which has also developed into the tort of misuse of private information.
- The tort of negligence.
- The tort of passing off.
- The Privacy and Electronic Communications Regulations 2003.
- The Human Rights Act 1998.

Postponing or redesigning a project

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

« Previous | Top of page | Next »

Back to ICO homepage

Responsibilities

The organisation proposing the project is responsible for undertaking a survey of the law relevant to the project and to the data processing and business processes it gives rise to. All participating organisations should do the same in connection with their involvement in the project.

Professionals with relevant expertise should be consulted as part of checking compliance with privacy law and other legal obligations. If your organisation has an in-house compliance unit or established compliance process, it might be useful to ensure that the compliance checking process takes full account of privacy law obligations and adds to the compliance checking process if necessary.

« Previous | Top of page | Next »

Back to ICO homepage

Potentially relevant areas of the law

You can refer to the examples of relevant laws 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 other laws that may be relevant.

- 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, which has also developed into the tort of misuse of private information.
- The tort of negligence.
- The tort of passing off.
- The Privacy and Electronic Communications Regulations 2003.
- The Human Rights Act 1998.

Postponing or redesigning a project

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

« Previous | Top of page | Next »

Back to ICO homepage

The role of compliance checking

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

- the Data Protection Act (DPA) in general;
- the data protection principles;
- the interpretations of the principles; and
- any delegated legislation, such as the Privacy and Electronic Communications Regulations (PECR).

« Previous | Top of page | Next »

Back to ICO homepage

Compliance checking

The organisation must evaluate the project process and the resulting design, in order to ensure that it is compliant with the Data Protection Act. Unlike a privacy impact assessment (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 the Data Protection Act.

A detailed template is provided in Appendix 2 to assist in checking the compliance of a design against the data protection principles. There is a further template in Appendix 3 to assess compliance with PECR. These templates are not comprehensive compliance tools in themselves, but do point to the issues you need to address as part of your own organisation's compliance checking procedures. They can be a useful starting point for developing in-house compliance checking procedures or quality assuring existing compliance tools your organisation already has in place.

Postponing or redesigning a project

To the extent that the design is not compliant with data protection law, it may be necessary to change the design prior to deployment, in order to achieve compliance.

« Previous | Top of page | Next »

Back to ICO homepage

ICO publications

Further information is available on the ICO website on topics including:

- Privacy by Design
- Empowering individuals to control their personal information
- Information Sharing
- CCTV
- Data security tip
- Marketing

In addition, the ICO have produced a range of guidance on data protection and the Privacy and Electronic Communications Regulations

Other sources of help and advice

Further guidance on data protection is available from the Ministry of Justice.

In addition the Cabinet Office Central Sponsor for Information Assurance completed their Data Handling Review in 2008 and have published core mandatory minimum measures to protect personal data, including the use of privacy impact assessments.

« Previous | Top of page | Next »

Back to ICO homepage

Appendix 1

PIA screening process

Step 1 – Criteria for full-scale PIA

This section 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.

The answers to the questions need to be considered as a whole, in order to decide whether the overall impact, and the related risk, warrant investment in a full-scale PIA. **The questions are shown below in bold**. 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 have substantial potential for privacy intrusion?

Examples include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, and logging of electronic traffic.

Identity

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

Examples of relevant project features 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 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 require identity. 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 (eg in 'joined-up government' initiatives) or private sector organisations (eg as outsourced service providers or as 'business partners')?

Schemes of this nature often involve the breakdown of personal data silos and identity silos, and may raise questions about how to comply with data protection legislation. This breakdown may be desirable for fraud detection and prevention, and in some cases for business process efficiency. However, data silos and identity silos are of long standing, and have in many cases provided effective privacy protection. Particular care is therefore needed in relation to preparation of a business case that justifies the privacy invasions of projects involving multiple organisations. Compensatory protection measures should be considered.

Data

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

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 other categories of personal data that may give rise to concerns, including financial data, particular data about vulnerable individuals, and data which can 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 processing such as welfare administration, healthcare, consumer credit, and consumer marketing based on intensive profiles.

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

Any data processing of this nature is attractive to 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 processing which is in any way exempt from legislative privacy protections?

Examples include law enforcement and national security information systems and also other schemes where some or all of the privacy protections have been negated by legislative exemptions or exceptions.

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

Measures to address concerns about critical infrastructure and the physical safety of the population usually have a substantial impact on privacy. Yet there have been tendencies in recent years not to give privacy its due weight. This has resulted 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 the provisions of the Data Protection Act or other relevant statutory provisions, such as where they are in a foreign jurisdiction. Concern may also arise in the case of organisations within the UK which are subsidiaries of organisations headquartered outside the UK.

Facing facts early

The key characteristics addressed here represent significant risk factors for the project and their seriousness should not be downplayed. It should also be remembered that 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 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 recommended that stakeholder perspectives are also considered as each question is answered.

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 it is, 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 chapter IV. Before proceeding to that part, however, it is necessary to continue with steps three and four of the screening process, to determine whether compliance checking should also be included in the project schedule.

Step 2 – Criteria for small-scale PIA

This section 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 bold. 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, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (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 reduce them to the satisfaction of those whose privacy is affected; and
- 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?

Individuals 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 an 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 enables an organisation to collate data about an individual, and that identifiers that are used for multiple purposes enable data consolidation. They are also aware of the increasingly 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 (eg 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 questions 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. There are often different impacts and implications for different sections of the population, especially disadvantaged groups.

Applying the criteria

Where the answers to questions are “Yes”, 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, a small-scale PIA may still be justified. In these circumstances the PIA process should be designed to focus on the areas of concern. If, on the other hand, multiple questions are answered “Yes”, a more comprehensive assessment is appropriate.

The small-scale PIA is described in chapter V. Before proceeding to that part, however, it is necessary to continue with steps three and four of the screening process, to determine whether compliance checking should also be included in the project schedule.

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 section of the handbook is to assist organisations in complying with privacy-related laws. The services of a legal professional with relevant expertise may be needed. 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 other forms of regulation, other than the Data Protection Act?

In particular, the following laws and other forms of regulation 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 (RIPA) and Lawful Business Practice Regulations 2000.
- The Privacy and Electronic Communications Regulations 2003 (PECR).
- 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, eg Financial Services and Markets Act 2000.
- Statutory codes, eg the Information Commissioner's CCTV code of practice.

Where projects are cross-jurisdictional the law of more than one country may be involved and other legal provisions may also need to be considered.

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 as it develops through case law.

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

In particular, the following should be considered:

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

Privacy law compliance checking is described in chapter VI of this handbook. Before proceeding to that part, however, organisations must continue with step four 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.

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 section of the handbook is to assist organisations in that endeavour.

The services of a professional with relevant legal expertise may be needed.

If the following question is answered ”Yes”, then a Data Protection Act compliance check should be conducted:
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).

Data Protection Act compliance checking is described in chapter VII. 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.

« Previous | Top of page | Next »

Back to ICO homepage

Appendix 2

Data Protection Act Compliance Check Template

This checklist aims to assist organisations proposing change to investigate whether the personal information aspects of their project comply with the Principles in Schedule 1 of the Data Protection Act (DPA).

It has been designed as a template to be deployed on desktops, portable computers (provided they are secure) or internal websites for use by any employee proposing change. Where so adopted by agencies, the template may need to be modified to add organisation-specific details.

It should be noted that many terms used in the Schedule 1 Principles have meanings specific to the Data Protection Act, and it would be prudent to refer to the Act for definition for those terms. Another useful reference in this regard is the Information Commissioner's Legal Guidance. Users are also encouraged to seek guidance from sources such as the organisation's Data Protection Officer, legal unit or external lawyers/ consultants.

I BASIC INFORMATION – New or existing Project, System, Technology or Legislation

1. Organisation and Project

Organisation	
Branch / Division	
Project	

2. Contact Position and/or Name, Telephone Number and Email Address.

(This should be the name of the individual most qualified to respond to questions regarding the PIA)

Name, Title	
Branch / Division	
Phone Number	
E-Mail	

3. Description of the Program / System / Technology / Legislation (Initiative) being assessed.

(Please note here if the initiative does **not** collect, use or disclose personal data*). If this is a change to an existing project, system, technology or legislation, describe the current system or program and the proposed changes.

4. Purpose / Objectives of the initiative (if statutory, provide citation).

5. What are the potential privacy impacts of this proposal?

6. Provide details of any previous PIA or other form of personal data* assessment done on this initiative (in whole or in part).

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO III DPA COMPLIANCE – CONCLUSIONS

***IMPORTANT NOTE:**
'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, section 1)

II DATA PROTECTION PRINCIPLES (DPPs)

1 Principle 1: Fair and Lawful Processing

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 19-35

1.1 Preliminary

1.1.1 What type of personal data are you processing?

Please give examples of any sensitive personal data that you are processing.

1.1.2 Are sensitive personal data being differentiated from other forms of personal data?

Yes No

If yes, please specify procedures. If no, please indicate why not.

1.2 Schedule 2 - Grounds for Legitimate Processing of Any Personal Data

1.2.1 Have you identified all the categories of personal data that you will be processing and how?

Yes No

If yes, please list them. If no, please indicate why not.

1.2.2 Have you identified the purposes for which you will be processing personal data and how?

Yes No

If yes, please list them. If no, please indicate why not.

1.2.3 Have you identified which of the grounds in Schedule 2 you will be relying on as providing a legitimate basis for processing personal data?

Yes No

If yes, please list them. If no, please indicate why not.

1.2.4 Are you relying on different grounds for different categories of personal data?

Yes No

If yes, how will this assessment be made?

1.3 Schedule 3 - Grounds for Legitimate Processing of Sensitive Personal Data

If this project does not involve the processing of sensitive personal data, please go to section 1.4

1.3.1 Have you identified the categories of sensitive personal data that you will be processing?

Yes No

If yes, can you list them. If no, please indicate why not.

1.3.2 Have you identified the purposes for which you will be processing sensitive personal data?

Yes No

If yes, can you list them. If no, please indicate why not.

1.3.3 Have you identified which of the grounds in Schedule 3 you will be relying on as providing a legitimate basis for processing sensitive personal data?

Yes No

If yes, can you list them. If no, please indicate why not.

1.3.4 Are you relying on different grounds for different categories of sensitive personal data?

Yes No

If so, how will this assessment be made?

1.4 Obtaining consent

1.4.1 Are you relying on the individual to provide consent to the processing as grounds for satisfying Schedule 2?

Yes No

If yes, when and how will that consent obtained?

1.4.2 For the processing of sensitive personal data, are you relying on explicit consent as specified in Schedule 3, s1 of the Data Protection Act?

Yes No

If so, when and how will that consent obtained?

1.5 Lawful Processing

a. If you are a public sector organisation:

1.5.1 Does your processing of personal data fall within your statutory powers?

Yes No

If yes, please state what they will be. If no, please indicate why not.

1.5.2 How is compliance with the Human Rights Act being assessed?

b. All organisations:

1.5.3 Are you assessing whether any of the personal data being processed is held under a duty of confidentiality?

Yes No

If yes, how will that assessment made? If no, please indicate why not.

1.5.4 How is that confidentiality maintained? (eg instructions on disclosure or shredding)

1.5.5 Are you assessing whether your processing is subject to any other legal or regulatory duties?

Yes No

If yes, how is that assessment being made? If no, please indicate why not.

1.5.6 How are you ensuring that those legal duties are being complied with?

1.6 Fair Processing

1.6.1 Are individuals being made aware of the identity of your organisation as the data controller?

Yes No

If yes, state how they are being made aware. If no, please indicate why not.

1.6.2 How are individuals being made aware of how their personal data is being used?

1.6.3 How are individuals offered the opportunity to restrict processing for other purposes?

When is that opportunity offered?

1.6.4 Do you receive information about individuals from third parties?

Yes No

If yes, please give examples. If no, please go to section 1.7

1.6.5 How are individuals informed that the data controller is holding personal data about them?

When are individuals informed?

1.7 Exemptions from the First Data Protection Principle

The Act requires that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:-

1. the identity of the data controller

2. the identify of any nominated data protection representative, where one has been appointed

3. the purpose(s) for which the data are intended to be processed

4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair

Data Protection Act, Schedule 1, Part II, para. 2 (3)

1.7.1 Do you provide individuals with all of the information in the box above?

If no, which exemption to these provisions is being relied upon?

2 Principle 2: Purpose Limitation

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

For the Information Commissioner’s guidance in relation to this DPP, see Legal Guidance pp 35-6

2.1 Uses of Personal Data within the Organisation

2.1.1 Are procedures in place for maintaining a comprehensive and up-to-date record of use of personal data?

Yes No

2.1.2 How often is this record checked?

2.1.3 Does the record cover processing carried out on your behalf (eg by a subcontractor)?

Yes No

2.1.4 What is the procedure for notifying (where necessary) the data subject of the purpose for processing their personal data?

(Cross reference with section 1.6, Fair Processing)

2.2 Use of Existing Personal Data for New Purposes

2.2.1 Does the project involve the use of existing personal data for new purposes?

Yes No

If no, go to section 2.3

2.2.2 How is the use of existing personal data for new purposes being communicated to:-

(a) the data subject;

(b) the person responsible for Notification within the organisation

(c) the Information Commissioner?

2.2.3 What checks are being made to ensure that further processing is not incompatible with its original purpose?

2.3 Disclosures of Data

2.3.1 Do you have a policy on disclosures of personal data within your organisation / to third parties?

Yes No

Is it documented?

Yes No

2.3.2 How are staff made aware of this policy / instructed to make disclosures?

2.3.3 How are individuals / data subjects made aware of disclosures of their personal data?

2.3.4 Do you assess the compatibility of a 3rd party's use of the personal data to be disclosed?

Yes No

If no, go to section 3.1

If yes, how do you make the assessment?

3 Principle 3: Adequate, Relevant and Not Excessive

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 36-37

3.1 Adequacy and relevance of Personal Data

3.1.1 How is the adequacy of personal data for each purpose determined? (Please give examples.)

3.1.2 How is an assessment made as to the relevance (ie no more than the minimum required) of personal data for the purpose for which it is collected?

3.1.3 What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed?

How often will these procedures reviewed?

3.1.4 Are there procedures for assessing the amount and type of personal data collected for a particular purpose?

Yes No

If yes, please describe. If no, please indicate why not.

3.1.5 Are items of personal data held in every case which are only relevant to a subset of those cases?

Yes No

4 Principle 4: Accurate and up to date

Personal data shall be accurate and, where necessary, kept up to date.

For the Information Commissioner’s guidance in relation to this DPP, see Legal Guidance pp 37-8

4.1 Accuracy of Personal Data

4.1.1 Are personal data evaluated to establish the degree of damage to both the data subject / data controller that could be caused through inaccuracy?

Yes No

4.1.2 How, and how often, are personal data be checked for accuracy?

Please give examples:

4.1.3 In what circumstances is the accuracy of the personal data being checked with the Data Subject?

Please give examples:

4.1.4 Are the sources of personal data (i.e. Data Subject, Data User, or third party) identified in the record?

Yes No

If so, how? Please give examples:

4.1.5 Is there any facility to record notifications received from the data subject if they believe their data to be inaccurate?

Yes No

If no, please indicate why not.

4.2 Keeping Personal Data Up to Date

4.2.1 Are there procedures to determine when and how often personal data requires updating?

4.2.2 Are personal data evaluated to establish the degree of damage to:

(a) the data subject

or

(b) the data controller

that could be caused through being out of date?

Yes No

Please specify whether to data subject or data controller:

4.2.3 Are there procedures to monitor the factual relevance, accuracy and timeliness of free text options or other comments about individuals?

Yes No

5 Principle 5: No Longer than Necessary

> Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
>
> For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance p 39

5.1 Retention Policy

5.1.1 What are the criteria for determining retention periods of personal data?

How often are these criteria reviewed?

5.1.2 Does the project(s) include the facility to set retention periods?

Yes No

5.1.3 Is the project subject to any statutory / sectoral requirements on retention?

Yes No

If yes, please state relevant requirements:

5.2 Review and Deletion of Personal Data

5.2.1 Is there a review policy?

Yes No

Is it documented?

Yes No

5.2.2 When data is no longer necessary for the purposes for which it was collected:

(a) How is a review made to determine whether the data should be deleted?

(b) How often is the review be conducted?

(c) Who is responsible for determining the review?

(d) If the data is held on a computer, does the application include a facility to flag records for review / deletion?

Yes No

5.2.3 Are there be any exceptional circumstances for retaining certain data for longer than the normal period?

Yes No

If yes, please give justification:

5.2.4 Is there any guidance on deletion / destruction of personal data?

Yes No

If no, please indicate why not.

6 Principle 6: Data subject access

Personal data shall be processed in accordance with the rights of data subjects under this Act.

For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 39-40

6.1 Subject Access

6.1.1 Are procedures in place to provide access to records under this Principle?

Yes No

If yes, please specify proposed procedures. If no, please indicate why not.

6.1.2 How do you locate all personal data relevant to a request (including any appropriate 'accessible' records)?

6.1.3 Do you provide an explanation of any codes or other information likely to be unintelligible to a data subject?

Yes No

If yes, how? If no, please indicate why not.

6.1.4 Are procedures in place to manage personal data relating to third parties?

Yes No

If yes, please specify proposed procedures. If no, please indicate why not.

6.1.5 How is data relating to third parties managed?

6.2 Withholding of personal data in response to a subject access request

6.2.1 Are there any circumstances where you would withhold personal data from a subject access request?

Yes No

If no, go to section 6.3. If yes, on what grounds?

6.2.2 How are the grounds for doing so identified?

6.3 Processing that may cause Damage or Distress

6.3.1 Do you assess how to avoid causing unwarranted or substantial damage or unwarranted and substantial distress to an individual?

Yes No

If yes, please specify proposed procedures. If no, please indicate why not.

6.3.2 Do you take into account the possibility that such damage or distress to the individual could leave your organisation vulnerable to a compensation claim in a civil court?

Yes No

6.4 Right to Object

6.4.1 Is there a procedure for complying with an individual's request to prevent processing for the purposes of direct marketing?

Yes No

6.5 Automated Decision-Taking

6.5.1 Are any decisions affecting individuals made solely on processing by automatic means?

Yes No

If yes, what will be the procedure(s) for notifying an individual that an automated decision making process has been used?

6.6 Rectification, Blocking, Erasure and Destruction

6.6.1 What is the procedure for responding data subject's notice (in respect of accessible records) or a court order requiring:

(a) rectification;

(b) blocking;

(c) erasure or;

(d) destruction of personal data?

7 Principle 7: Data Security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

For the Information Commissioner’s guidance in relation to this DPP, see Legal Guidance pp 40-3

7.1 Security Policy

7.1.1 Is there a Data Security Policy?

Yes No

If no, please indicate why not and then go to 7.1, question 5..

7.1.2 If yes, who / which department(s) are responsible for drafting and enforcing the Data Security Policy within the organisation?

7.1.3 Does the Data Security Policy specifically address data protection issues?

Yes No

7.1.4 What are the procedures for monitoring compliance with the Data Security Policy within the organisation?

7.1.5 Does the level of security that has been set take into account the state of technological development in security products and the cost of deploying or updating these?

7.1.6 Is the level of security appropriate for the type of personal data processed?

7.1.7 How does the level of security compare to industry standards, if any?

7.2 Unauthorised or unlawful processing of data

7.2.1 Describe security measures that are in place to prevent any unauthorised or unlawful processing of:

(a) Data held in an automated format (eg password controlled access to PCs)

(b) Data held in a manual record (eg locked filing cabinets)?

7.2.2 Is there a higher degree of security to protect sensitive personal data from unauthorised or unlawful processing?

Yes No

If yes, please describe the planned procedures. If no, please indicate why not.

7.2.3 Describe the procedures in place to detect breaches of security (remote, physical or logical)?

7.4 Destruction of Personal Data

Cross-reference with section 5.2

7.4.1 Describe the procedures in place to ensure the destruction of personal data no longer necessary?

7.4.2 Are there different procedures for destroying sensitive personal data?

Yes No

7.5 Contingency Planning - Accidental loss, destruction, damage to personal data

7.5.1 Is there a contingency plan to manage the effect(s) of an unforeseen event?

Yes No

7.5.2 Describe risk management procedures to recover data (both automated and manual) which may be damaged/lost through:

- human error
- computer virus
- network failure
- theft
- fire
- flood
- other disaster.

8 Principle 8: Overseas Transfer

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

For the Information Commissioner’s guidance in relation to this

DPP, see Legal Guidance pp 43-5

8.1 Adequate Levels of Protection

8.1.1 Are you transferring personal data to a country or territory outside of the EEA?

Yes No

If no, please go to Part III.

If yes, where?

8.1.2 What are the types of data are transferred? (eg contact details, employee records)

8.1.3 Are sensitive personal data transferred abroad?

Yes No

If yes, please provide details:

8.1.4 What are the main risks involved in the transfer of personal data to countries outside the EEA?

8.1.5 Are measures in place to ensure an adequate level of security when the data are transferred to another country or territory?

8.1.6 Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?

8.2 Exempt Transfers

8.2.1 Is your organisation carrying out any transfers of data where it has been decided that the Eighth Principle does not apply?

Yes No

If yes, what are they?

8.2.2 To which country / territory are these transfers made?

8.2.3 What are the criteria set by your organisation, which must be satisfied before a decision is made about whether the transfer is exempt from the Eighth Principle?

Eg consent, (See DPA 1998, Schedule 4, for a full list)

8.3 Choosing a Data Processor

8.3.1 What reasonable steps did you take to ensure that the Data Processor complies with data protection requirements?

8.3.2 How did you assess their data security measures?

8.3.3 How do you ensure that the Data Processor complies with these measures?

8.3.4 Is there an on-going procedure for monitoring their data security measures?

Yes No

If yes, please describe. If no, please indicate why not.

III DPP COMPLIANCE - CONCLUSIONS

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the DPPs. This could include indicating whether some changes or refinements to the project might be warranted.

_____________________ (Proponent) Date: ___________

_____________________(Data Protection Officer) Date: ___________

« Previous | Top of page | Next »

Back to ICO homepage

Appendix 3

Privacy and Electronic Communications Regulations Direct Marketing Compliance Check Template

This Checklist aims to assist organisations proposing change to marketing arrangements to investigate whether their project complies with the requirements of the Privacy and Electronic Communications Regulations 2003 (PECR). The Regulations are designed to be technology neutral, so will apply to most electronic communications.

I BASIC INFORMATION – New or existing Project, System, Technology or Legislation

1. Organisation and Project

Organisation	
Branch / Division	
Project	

2. Contact Position and/or Name, Telephone Number and Email Address.

(This should be the name of the individual most qualified to respond to questions regarding the PIA)

Name, Title	
Branch / Division	
Phone Number	
E-Mail	

3. Description of the Program / System / Technology / Legislation (Initiative) being assessed.

If this is a change to an existing project, system, technology or legislation, describe the current system or program and the proposed changes.

4. Purpose / Objectives of the initiative (if statutory, provide citation).

5. What are the potential privacy impacts of this proposal?

6. Do you intend to send direct marketing messages by electronic means such as by telephone, fax, email, text message and picture (including video) message or by using an automated calling system?

Yes No

If yes, then you will need to complete this Checklist

IMPORTANT NOTE

‘direct marketing’ means ‘the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals’.
(Data Protection Act 1998 section 11)

7. Do you intend to send direct marketing messages only using Bluetooth?

Yes No

If yes, answer question 8, then go to Part III: PECR Marketing Compliance – Conclusions

IMPORTANT NOTE

The PEC Regulations only apply to messages sent over a public electronic communications network and Bluetooth messages are not sent using such a network.
(PECR 2003 section 2)

8. Do you intend to process personal data in order to send your direct marketing?

Yes No

If yes, then you will also need to complete the Data Protection Checklist

IMPORTANT NOTE:

‘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, section 1)

9. Are your direct marketing communications going to be aimed at individual subscribers or corporate subscribers?

Individual Corporate Both

If Individual or Both continue with Section II, if Corporate go to Section III

IMPORTANT NOTE

The PEC Regulations apply different rules to individual subscribers and corporate subscribers, although some rules apply to both. Where personal data is used the Data Protection Act 1998 always applies.

10. Your direct marketing communications should provide the recipient with information to make effective use of their rights as regards direct marketing communications. Describe the information to be provided and the mechanism by which it will be provided, particularly where the information provision is not via the same communication method as the direct marketing communication.

IMPORTANT NOTE

The e-Commerce Regulations 2002 require that the recipient of a e-Commerce service, including direct marketing, must be provided, in a form and manner that is easily, directly and permanently accessible certain information including:

the name of the service provider

the geographic address at which the service provider is established

the details of the service provider, including his email address, which make it possible to contact him rapidly and communicate with him in a direct and effective manner

The Regulations do not prescribe how the requirement to make information "easily, directly and permanently accessible" should be met.

II INDIVIDUAL SUBSCRIBERS

1. Are your marketing communications directly invited or unsolicited?

Directly Invited Unsolicited

2. By what mechanism have subscriber details been obtained?
How do you determine whether the details have been provided with the intention that you should send the subscriber direct marketing communications

IMPORTANT NOTE

If your marketing communications are directly invited (solicited) by the individual subscriber to whom they are sent, i.e. they have asked you to send them marketing communications then many of the PEC Regulations do not apply.

3. If you are to use an Automated Calling System for marketing communications do you have the prior consent of the subscriber?

Yes No

4. If you have the prior consent of the subscriber, how do you audit and verify the accuracy of your subscriber records? How will you address withdrawal of consent?

IMPORTANT NOTE

In order to use Automated Calling Systems for marketing communications to individual subscribers you must have prior consent. Prior consent on the other hand means that the subscriber has given some positive indication of intention; this does not necessarily require a tick box "opt-in" e.g. if the subscriber has clearly indicated their consent to the purposes and to the receipt of marketing communications in some other fashion i.e. clicking on an “Accept” button at the end of a marketing notice.

5. If you are to use faxes for marketing communications do you have the prior consent of the subscriber?

Yes No

6. If you have the prior consent of the subscriber, how do you audit and verify the accuracy of your subscriber records? Does your company currently subscribe to the Fax Preference Service? How will you address withdrawal of consent or a subscriber override of the FPS registration?

IMPORTANT NOTE

In order to use faxes for marketing communications to individual subscribers you must have prior consent, and check with the FPS on a regular basis unless the subscriber has notified you that such communications can be sent ‘for the time being’.

7. If you are to use live voice telephone for marketing communications have you been previously notified not to call certain subscriber numbers?

Yes No

8. How do you audit and verify the accuracy of your subscriber records? Does your company currently subscribe to the Telephone Preference Service? How will you address future “Do not call” requests, or a subscriber override of their TPOS registration?

IMPORTANT NOTE

In order to use live voice telephone calls for marketing communications to individual subscribers you must honour subscriber “Do not Call” requests, and check with the TPS on a regular basis unless the subscriber has notified you that such communications can be sent ‘for the time being’.

9. If you are to use e-mail/SMS for marketing communications do you have ‘opt-in consent’ of the subscriber?

Yes No

10. If you do not have ‘opt-in consent’, can communications be permitted under the ‘soft opt in’ test

Yes No

11. How do you collect, audit, and verify the accuracy of your opt-in subscriber records?

12. If 'soft opt-in' is to be used, provide details of how this will be recorded and verified and describe how opt-out mechanisms will be provided

IMPORTANT NOTE

In order to use e-mail/SMS for marketing communications to individual subscribers you have the opt-in consent of subscribers OR' meet the soft-opt-in test:

Contact details are obtained during negotiation or sale of goods or services to the recipient;
AND
marketing is conducted by the same entity as previous dealings with the individual;
AND
marketing relates to "similar products and services";
AND
an opt-out mechanism is provided at the point of data collection and is provided with each new communication.

III CORPORATE SUBSCRIBERS

1. Are your marketing communications directly invited or unsolicited?

Directly Invited Unsolicited

2. By what mechanism have subscriber details been obtained? How do you determine whether the details have been provided with the intention that you should send the subscriber direct marketing communications

IMPORTANT NOTE

If your marketing communications are directly invited (solicited) by the corporate subscriber to whom they are sent, i.e. they have asked you to send them marketing communications then many of the PEC Regulations do not apply.

3. If you are to use an Automated Calling System for marketing communications do you have the prior consent of the subscriber?

Yes No

4. If you have the prior consent of the subscriber, how do you audit and verify the accuracy of your subscriber records? How will you address withdrawal of consent?

IMPORTANT NOTE

In order to use Automated Calling Systems for marketing communications to corporate subscribers you must have prior consent.

5. If you are to use faxes for marketing communications have you been previously notified not to call certain subscriber numbers?

Yes No

6. If you have the prior consent of the subscriber, how do you audit and verify the accuracy of your subscriber records? Does your company currently subscribe to the Fax Preference Service? How will you address future “Do not fax” requests? or a subscriber override of the FPS registration?

IMPORTANT NOTE

In order to use faxes for marketing communications to corporate subscribers you must honour subscriber “Do not Fax” requests, and check with the FPS on a regular basis unless the subscriber has notified you that such communications can be sent ‘for the time being’.

7. If you are to use live voice telephone for marketing communications have you been previously notified not to call certain subscriber numbers?

Yes No

8. How do you audit and verify the accuracy of your subscriber records? Does your company currently subscribe to the Telephone Preference Service? How will you address future “Do not call” requests?

IMPORTANT NOTE

In order to use live voice telephone calls for marketing communications to corporate subscribers you must honour subscriber “Do not Call” requests, and check with the TPS on a regular basis unless the subscriber has notified you that such communications can be sent ‘for the time being’.

9. If you are to use e-mail/SMS for marketing communications to corporate subscribers, describe what measures will you take if corporate subscribers request to opt-out from future e-mails, or override their TPS registration?

IMPORTANT NOTE

There are currently no consent requirements applicable to the sending of e-mail/SMS marketing communications to corporate subscribers. However, it is good practice to provide and opt-out mechanism.

IV PECR DIRECT MARKETING COMPLIANCE – CONCLUSIONS

Please provide a summary of the conclusions that have been reached in relation to this project’s overall compliance with the Direct Marketing provisions of the PECR. This could include indicating whether some changes or refinements to the project might be warranted.

____________________ (Proponent) Date: ___________

____________________(Data Protection Officer) Date: ___________

« Previous | Top of page | Next »

Back to ICO homepage

Privacy strategies

What is a privacy strategy?

For many organisations that depend upon personal data, privacy has become a strategic factor. Completing a PIA can be 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. The role of PIAs must be defined within the organisation's privacy strategy and the privacy strategy must be part of the organisation's broader strategic planning.

However, a privacy strategy must be broader than PIAs and help to address potential media controversies which might occur and the need to respond to enquiries from individuals, their representatives, or elected officials.

A privacy strategy works best when it is expressly stated and is proactive and articulated into a plan, with adequate resources and effective monitoring of performance against the plan.

Why have a privacy strategy?

Organisations will find starting and completing a PIA much easier when a privacy strategy is in place. This is because staff will be more aware of the kinds of issues, implications, public concerns and risks. Organisations whose operations have considerable impacts on the privacy of their customers, their staff, or indeed any other categories of people, may find that they need to undertake PIAs more frequently. A privacy strategy helps to manage multiple PIAs being conducted within an organisation and ensure consistency in relation to the type of projects which are subject to a PIA.

Different types of privacy strategy

The scope of a privacy strategy should reflect the nature of the organisation and its mission. This section should help determine the appropriate scope of the strategy depending on the organisation's needs. It identifies four broad approaches, ranging from the very narrow to the very broad.

- A minimalist information privacy strategy.
- A comprehensive information privacy strategy.
- A broad privacy strategy.
- A social impacts or public policy strategy.

A minimalist privacy strategy

The most basic approach is to develop a privacy strategy which helps the organisation to meet legal requirements and obligations in relation to information privacy. A minimalist information privacy strategy will have the following basic aims.

- To develop an organisational understanding of privacy and data protection, and of the key privacy issues that arise in the organisation's relationships with individuals (generally its staff and customers)
- To conduct a review of the organisation's holdings of personal

data and the processes relating to that data.

- To build recognition of privacy matters into its project processes (eg as a component of project scoping documents, or budget approvals). This should include:
    - a requirement that PIAs be considered where appropriate;
    - a requirement that legal compliance checks are completed; and
    - a requirement that data protection compliance checks are completed.

A comprehensive information privacy strategy

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 is likely to encompass the following aims in additions to those in a minimalist information privacy strategy.

- 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 ‘identity silos’, by avoiding the use of the same identifier in multiple organisations, systems and programmes.
- An active commitment to avoid 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.
- A commitment to use of authentication rather than identification in determining an individual’s entitlement to services, benefits or access.
- Approval for and facilitation of anonymous and pseudonymous transaction services in all circumstances where appropriate.
- Avoidance of prejudice to the person’s access to services, or their ability to exercise other rights, because of the exercise of privacy rights.
- Individual control over identification and authentication mechanisms, such as chip-cards and digital signature keys.

A broad privacy strategy

People are concerned about other dimensions of privacy other than just information privacy, and organisations may judge it to be advantageous to define the scope of their privacy strategy to reflect broader concerns.

A broad enterprise privacy strategy would also encompass impacts on other types of privacy, such as privacy of the person, personal behaviour and personal communications.

A social impacts/ public policy strategy

Some organisations may judge it to be advantageous to adopt a scope that is broader than privacy alone, but encompasses it. A 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 compulsion, or other forms of 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; and
- the accessibility of information.

One of the advantages of a social impacts/public policy strategy which includes privacy is that the privacy elements of your strategy are part of the fabric of policy-making.

Meeting the requirements of a privacy strategy

A successful privacy strategy needs direction and leadership from a senior executive level. The following measures are advised in order to ensure that any privacy strategy is met and exceeded.

- Establish and maintain a focal point that ensures executive attention to the matter, including commitment by senior executives to a privacy programme.
- Appoint a Chief Privacy Officer at a senior level within the organisation.
- Regular inclusion of privacy matters in executive committee agendas.
- Ensure that business process engineering and re-engineering activities have privacy sensitivity embedded into them. This could involve changing:
  - provisions within supplier contracts;
  - the organisation’s project management framework and methodology; and
  - the organisation’s audit processes.
- Structure a programme that builds privacy respect into the organisation’s philosophy, mindset and business processes. This programme could include:
  - staff training schemes;
  - internal audit of personal data practices.
- Establish and maintain an internal communications programme.
- Establish and maintain an external communications programme, which may include targeting your organisation’s privacy messages at:
  - affected individuals (including staff as well as clients);
  - relevant representative and advocacy organisations.
- Create channels to and from relevant representative and advocacy organisations; and
- Ensure your organisation has the capacity to receive and handle incoming communications, through procedures for handling incidents, enquiries, submissions and complaints.