

# Discussion Document

## The Business Case for Investing in Proactive Privacy Protection

25<sup>th</sup> August 2009 (version 1.2)



---

## Contents

This document is organised into the following major sections.

<b>Introduction</b>	<b>3</b>
<b>Discussion issues</b>	<b>5</b>
1 Thinking about privacy	5
Does privacy mean different things to different people? How well developed is thinking on the subject?	
2 Valuing personal information	6
What is the value of personal information to organisations or to the individual, and how might that be estimated?	
3 The benefits of protecting personal privacy	9
There are many possible different reasons for protecting privacy and these will carry different weights for different organisations.	
4 The costs of protecting personal privacy	13
All the effects on the organisation need to be considered, not just the financial outlays involved.	
5 Deciding on personal privacy protection options	15
Armed with an understanding of the benefits and the costs, how are these weighed up in the decision making processes organisations use?	
6 Approaches to providing privacy protection	17
What approaches, methods and measures do organisations typically use to protect privacy?	
<b>Providing contributions</b>	<b>20</b>
<b>Contacts</b>	<b>23</b>

## Introduction

### The project

Watson Hall Ltd and John Leach Information Security Ltd are jointly undertaking a project for the Information Commissioner's Office (ICO) to research and develop an easily understandable and compelling business case that will help organisations to justify and implement privacy protection within their business processes and systems.

The Privacy by Design report, commissioned by the ICO in 2008, identified the absence of a soundly argued business case for investing in privacy friendly systems and business processes as one of the barriers to more proactive privacy protection.

In order to address this aspect, the ICO has commissioned us to develop a document setting out the business case for investing in proactive privacy protection in existing and new business processes. This will involve understanding the organisational processes involved in procuring, implementing and changing information systems and processes across the public, private and professional services sectors, researching the value of personal information as an asset and quantifying the risk to personal information.

### Purpose of discussion document

The purpose of this discussion document is to gather a wide range of views on key topics relating to the project. We are seeking input from people who are experienced in the handling of personal information and/or are knowledgeable in the field. That is:

- People who are familiar with the ways that organisations think about personal information, use personal information, and protect the personal information they hold.
- People who might be accountable for investment, governance and strategy, and who understand how privacy-affecting decisions are made within their organisation.
- People who work on the implementation and operation of business processes and systems.
- People who are customers or clients and are affected by such processes and systems.

And people who are knowledgeable in the field of Privacy and especially in building privacy protection into business processes and systems.

We will be pleased to receive contributions relating to the topics laid out below, plus suggestions for other topics that are significant to the development or success of a business case for proactive privacy protection. As a result of this project we will be delivering a report aimed at a senior non-technical audience. Therefore, we are looking for short, succinct, clear input that will be accessible to the target readers, rather than formal definitions or lengthy treatises. We would welcome especially contributions which illuminate at an organisational, governance, policy, strategy or management level rather than at a technological level.

You might feel that some of the questions in different sections overlap to some degree. This is because we have to allow for different people seeing these issues in different ways, and because many of the issues are interlocking. Please bear with us on this and provide your input in response to the issue where you feel it fits best. If an issue does not apply exactly to your situation, or you feel

you have responded to it already under a different heading, then feel free to tell us about an adjacent issue which does relate to your situation, or to move on to the next issue.

### **Additional resources**

The following resources may provide useful additional background reading:

- Project website  
<http://watsonhall.com/privacy.protection>
- ICO appoints consultants to put a value on privacy protection  
Press Release, ICO, 7th August 2009  
[http://www.ico.gov.uk/upload/documents/pressreleases/2009/dp\\_tender\\_appointment\\_final.pdf](http://www.ico.gov.uk/upload/documents/pressreleases/2009/dp_tender_appointment_final.pdf)
- Privacy by Design report, ICO  
[http://www.ico.gov.uk/about\\_us/news\\_and\\_views/current\\_topics/privacy\\_by\\_design.aspx](http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx)
- Determining what is personal data, Data protection technical guidance, ICO  
[http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/personal\\_data\\_flowchart\\_v1\\_with\\_preface001.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf)
- Your personal information, ICO  
[http://www.ico.gov.uk/for\\_the\\_public/your\\_personal\\_information.aspx](http://www.ico.gov.uk/for_the_public/your_personal_information.aspx)

---

## Discussion issues

### 1 Thinking about privacy

Here we would like to understand what the privacy of personal information means to business leaders within data handling organisations, and how well developed their thinking is on the subject. The more sophisticated their thinking, the more sophisticated privacy business cases will need to be.

#### 1.1 A practical definition of privacy

Firstly, what do people understand by the term Privacy?

We would like to have a punchy practical definition of privacy, free of formality and jargon, that can speak immediately to senior decision makers and leaders within organisations that handle personal data.

Is Privacy, for example, “The interest that an individual has in what information is held on them, and how it is collected, used, and shared”? Suggestions please.

#### 1.2 Maturity of approach

How advanced is thinking on the subject?

Information systems and processes are central to the conduct of people’s daily lives in the UK. Within this, personal information is central to the delivery of convenient and personalised services across all sectors.

Some organisations seem to consider personal information to be little different, if at all, from any other type of information they use. Some are aware that, due to its nature, personal information has a special role to play within their operations. And some have gone further and realise that personal information has a special role to play for the individual (the data subject) too and that this imposes important obligations on the data-handling organisation, obligations that stretch well beyond the requirement simply to comply with the Data Protection Act 1998 and other externally-imposed mandates.

We would like to hear about how mature different organisations are with respect to their thinking on:

- The role personal information plays within their operational systems.
- What the privacy of personal information means to them.
- Why personal privacy matters.
- What their accountability is for its protection.
- What governance structures and management practices would be needed for personal privacy protection to be effective.
- Do organisations tend to have a clear understanding of where personal information is collected, stored and used in all their business processes?

## 2 Valuing personal information

Here we would like to find out how organisations understand the value personal information has to their organisation, and how they might try to estimate or quantify that value. If a definite value can be assigned to personal information, then we can expect that privacy business cases can be convincing. If its value is anything but definite, building a business case becomes more of a challenge.

### 2.1 Putting a value to personal information

Personal information has a special role to play for the organisation using it. We would like to understand how that role is understood and how organisations gauge, estimate or measure the importance or value of the personal information they handle. Having a clear understanding of the value of personal information can help organisations to exploit their information better as well as help them to understand their risks and protect that information better.

- Do they view personal information as information they own, or is there some acknowledgement that the individual (the data subject) also has some claim to ownership?
- Is information generally considered to be a business asset like trade secrets and intellectual property?
- Do organisations put a value on personal information or do they regard it as the same as any other information they handle within their systems?
- What yardstick is used? Is the value of personal information measured in financial terms or in other terms?
- (Public sector) Is its value related in some way to the social need for the service or capability enabled by the information, or otherwise?
- (Private sector) Is its value related to the value of the business enabled (e.g. turnover, profit) by the information, or otherwise?
- Is its value related to the cost of gathering and handling the personal information?
  - What typically is the incremental cost of acquiring a customer for different sectors?
  - How much can different types of personal information be bought or sold for?
- Is its value related to the impact that might be suffered if a privacy breach were to arise?
- Does its value vary with the context, for example the quantity of the data held (e.g. the number of records held), the nature of the data subject (e.g. whether it relates to ordinary people, people in the public eye, vulnerable people), how it was collected (directly from the person or via a third party), the type of consent associated with the data, or the sensitivity of the data (e.g. general personal data such as address, financial data such as account details, intimate data such as health data)?
- Is personal information about staff valued differently to personal information about customers/citizens?

---

## 2.2 The impact of possible privacy failures

One way to value information is to look at the costs that would be incurred if something were to go wrong. How do organisations gauge or estimate the impact of the privacy failures which could arise?

- Do organisations attempt to estimate the impact of possible privacy failures or can they work on avoiding privacy failures without needing to estimate possible impacts?
- What yardstick is used? Is the impact measured in financial terms or in other terms?
- What aspects are considered and which generally are thought to be the most significant?
  - The cost of making good the effect on the compromised information (e.g. replacing the information if it were altered or deleted)?
  - The internal costs involved in managing the privacy failure (e.g. containment, recovery, notification, investigation, cause analysis, improving policies and systems to prevent a recurrence)?
  - The external costs involved in managing the privacy failure (e.g. regulatory enforcement costs, fines and penalties, legal fees, reporting, notifying affected data subjects, assisting affected data subjects,)?
  - The anticipated increases in the costs of running the business in the future (e.g. additional staff training, increased insurance premiums, increased transaction charges, higher cost to acquire new customers, increased spending to retain existing customers, lower staff retention, higher recruitment costs)?
  - The anticipated decrease in revenues from the business in the future (e.g. fewer new customers, less income from existing customers)
  - Other aspects?

## 2.3 The impact of actual privacy failures

Rather than having to estimate what the costs of a potential privacy failure might be, organisations could be guided by the actual impact of the privacy failures they have suffered in the recent past.

- Do organisations detect, acknowledge or record the personal privacy failures or near misses that take place within their organisation? For those that do, how do they do this and how are the records used, what are the benefits and what are the issues?
- Do organisations assess the severity and the impact of the failures or near misses that take place? For those that do, how do they do this?
- Do organisations have a formal process in place to learn from the failures of near misses that occur? For those that do, what is involved?

## 2.4 The value to the individual

Personal information has a special role to play for the individual too. We would like to understand what people feel about the importance or value of their personal information.

- How concerned are people typically about the privacy of the personal data they provide? In which types of situation might they provide it hesitantly, and in which might they provide it without a care?

- What is the reason behind the concerns they feel? For example, are they most worried about malicious misuse of their information, that their information will get corrupted and they will have to deal with the consequences, or that their information is going to be used by poorly designed systems that will simply “get it wrong”?
- How concerned are people typically about the effect on their personal privacy of data that is gathered about them as they go about their daily lives (e.g. CCTV images, records of their Internet searches, records of the telephone calls they have made)?
- Are they concerned about the principle that such surveillance data is gathered, or are they happy for it to be gathered and concerned only to receive assurances that the data is protected and safeguarded against abuse?
- How concerned are people when data gathered in one context is used in an altogether different context (e.g. telephone call data is used not just for billing purposes but for assessing whether someone might pose a security threat to the nation)?
- What yardsticks do people use to gauge the importance of their personal information and their concern for its protection? Is its importance measured, for example:
  - In terms of their feelings of vulnerability (their view of the likelihood that at some stage it might be compromised)
  - Their view of the impact on them personally should it be compromised (e.g. the inconvenience, effort and distress of having to change to a new financial account)
  - In some other terms?
- What is the magnitude of the importance personal information has for the individual? Does the feeling that their information might one day get compromised generally cause people slight or major anxiety? Is the potential impact resulting from a privacy failure generally regarded as a minor tolerable inconvenience or could it be a source of outrage?

## 2.5 Examples of privacy incidents

We are looking for illustrative anonymised examples of actual privacy incidents involving organisations, or near misses — the ones that almost happened. Can you tell us one you know about? We would like a brief (one or two line) description of the incident with mention of the consequences and impact where known. Please tell us if your example is from first-hand knowledge or otherwise. You may send your example to us separately if you wish.

### 3 The benefits of protecting personal privacy

Having determined that personal information has a value for both the individual and the handling organisation, we can assume that there will be benefits for both the individual and the organisation in that information being protected. These benefits can go beyond simply maintaining the value or utility of the information. Here we would like to understand what those benefits might be and their typical magnitude.

#### 3.1 The benefits for the individual

We could claim that the primary benefit to the individual is a reduced risk that other parties might use their personal information in ways contrary to their better interests.

- Is this the main benefit for the individual or are there other dimensions involved?
- Even so, people might not articulate the benefit in this way. How would the typical individual express the benefits?
- What other or secondary benefits (e.g. to a community or to society) might there be?
- How would the benefits of having their personal information being better protected actually manifest themselves for the individual?
  - Greater peace of mind / reduced anxiety when having to provide personal information?
  - Greater willingness to engage with Government, service providers, shops on-line?
  - Less of a need to check their bank or credit card statements carefully?
  - Less frequent or less severe impacts from the breaches they do suffer?
  - Other ways?

#### 3.2 The benefits for the organisation

First we would like to look at the nature of the benefits for organisations, then to look at their magnitude.

From the perspective of the information-handling organisation, what do they see as the types of benefits they can gain from protecting personal privacy better? We would like to get to the heart of the many ways that privacy protection can bring real benefits to the organisation, so would ask you to apply the “So What?” test to any suggestions. We would be very grateful if you could provide any examples of which you are aware where improved privacy practices have led to any of these benefits (e.g. increased turnover and/or reduced costs).

- Improved compliance, i.e. having greater confidence in the organisation’s compliance with various internal and external mandates. How does this manifest itself for the organisation? Is this:
  - Less of a chance of censure or fine by the ICO or a regulator?
  - Less of a chance of having operations curtailed or a trading licence qualified?
  - Less of a chance of having to take on additional compliance controls imposed by a regulator?

- 
- Less of a chance that the organisation might be taken to task, or taken to court, for processing personal data illegally (e.g. for the public sector, for overstepping the organisation's statutory powers or relevant legislation such as the Human Rights Act) or for not complying with contractual obligations?
  - Fewer audit points raised when assessing compliance to internal mandates such as a strategic or political priority or target, policies, ethical values or management targets?
  - Other forms?
  - Reduced assurance risk. How does this manifest itself? Is this:
    - Greater confidence that all significant risks have been identified?
    - Less frequent disruptions to plans and operations?
    - Lower costs / losses attributable to privacy failures?
    - More effective response to, and recovery from, privacy failure incidents?
    - Less troublesome and more mutually beneficial relationships with customers/citizens, suppliers, sub-contractors, outsourcers, etc?
    - Other forms?
  - Enhanced corporate social responsibility programmes and other activities leading to increased community goodwill?
  - Enhanced community engagement?
  - Enhanced stakeholder trust and goodwill, and hence greater co-operation and engagement and increased business value?
  - Enhanced generation of public value and social inclusion?
  - Increased take-up of services as a result of enhanced (internal and external) customer/citizen experience and improved service delivery?
  - Enhanced brand value?
  - Enhanced customer/citizen trust and goodwill, and hence greater co-operation and engagement and, for the private sector, greater competitive advantage, market share, customer retention, customer loyalty in the face of competition?
  - Would stakeholder value increase as a result of better privacy protection? Would a private sector organisation's share price increase (e.g. in anticipation of increased revenues)? Would a public sector organisation see a measurable improvement in its status in any broadly comparable way?
  - Enhanced ability to attract new customers (e.g. by referral) and hence a larger customer base?
  - Enhanced ability to win contracts by product or service differentiation in an internal or business-to-business marketplace?
  - Improved customer/citizen data offering better targeted personalised enhanced services or a more accurate ability to apply price differentiation?
-

- Increased transparency to individuals about transactions leading to opportunities to increase prices?
- The ability to negotiate more favourable contracts?
- Enhanced operational effectiveness and efficiency? In particular, is this:
  - Better targeted / better quality / more focused / more flexible / more adaptable business processes achieved by having a greater understanding of customer/citizen identity, personal data, consent?
  - The ability to respond more promptly or at a lower cost to compliance requirements (including responding to Subject Access Requests (SAR), e-disclosure requests, Freedom of Information (FOI) requests)?
  - Better targeting of information security resources to higher risk assets and systems?
  - Reduced storage/archival costs?
  - Avoidance of the costs of collecting, storing and using inaccurate, excessive or irrelevant information?
  - Reducing the spread of personal information unnecessarily through the organisation and therefore simplifying data destruction/deletion at the end of its life?
  - Lower customer/citizen service overheads?
  - Other components?
- Better staff culture and morale, leading to lower staff churn, greater ability to attract high-calibre staff, greater staff productivity, lower levels of staff sickness?

### 3.3 The drivers behind personal privacy protection

Whilst focussing strongly on the wide range of benefits, we need to remain open to the possibility there might be reasons for protecting privacy which do not fall easily into the category of benefits.

The issue of compliance with legislation is a vexed question here. Private sector organisations might be comfortable seeing greater confidence in their compliance with legislation as a benefit (which is why it was mentioned above). By contrast, public sector organisations might see it more as an absolute imperative, not at all optional and hence not easily thought of in relative terms as a benefit. We are very interested in views on this.

- Are there other, additional reasons for protecting personal privacy which do not fall into the category of benefits (e.g. ethical or social reasons)?
- What are the relative priorities of all the various benefits and other reasons in the public sector (for example, using the list of benefit types shown in 3.2 above, can you give a score to each of the ones you consider most influential)?
- What are the relative priorities of all the various benefits and other reasons in the private sector (for example, can you give a score to each of the ones you consider most influential)?
- How easily are any of these drivers ignored or overridden or given a reduced priority when the costs or the burden of indicated privacy protections go up?

### 3.4 Assessing expected benefits

Having looked at the range of different types of benefit or driver behind privacy protection, here we would like to understand how the magnitude of these benefits can be gauged or estimated.

- Do organisations try to assess the benefits they can expect from protecting personal privacy better or is privacy protection not optional and therefore provided regardless of the magnitude of any benefit?
- What yardstick is used? Are benefits assessed in financial terms or in other terms?
- Which benefits can be expressed easily in financial terms and which are more difficult to assess that way?
  - Out of interest, what is a typical cost for responding to a Subject Access Request (SAR), person-related e-disclosure request, Freedom of Information (FOI) request and how much can this cost be driven down by optimising processes?
- How are other intangible benefits quantified?
- How are intangible assets valued (e.g. information, community engagement, goodwill, brand value, customer service levels). Which of these are recognised as assets on the balance sheet?
- How convincing are financial estimates of intangible benefits?
- As well as trying to estimate the magnitude of expected benefits, organisations can try to assess the magnitude of the actual benefits they have achieved in the past through previous protection efforts. How do organisations measure the benefits they might have achieved from previous efforts to protect personal privacy better, either in general or from particular privacy protection measures they have implemented?

## 4 The costs of protecting personal privacy

The other side to the business case equation is the cost of providing the indicated privacy protection, where the cost includes not just the outlays incurred but all forms of burden placed on the organisation as a result of its protection of personal privacy. This is what we would like to cover here.

### 4.1 The different types of costs

Protecting privacy is not just about encrypting personal data when it moves outside a controlled environment. It is centrally about building privacy-protecting safeguards and privacy-related capabilities into processes and systems, and putting in place appropriate governance and management arrangements so that personal information is handled correctly and securely at all stages in its lifecycle. To get a full picture of the costs, we need to identify all the main components that contribute to the costs. What are these components?

- Governance arrangements – how might these introduce additional costs?
- Assessing privacy needs – this would include the staff costs of conducting privacy needs assessments (e.g. Privacy Impact Assessments (PIAs) or informal substitutes). Anything further?
- Building personal privacy protection in to systems – this would include the costs of designing and developing the required privacy solutions, developing procedures and documentation, and procuring any specific software or hardware components if these are needed. Anything further?
- Operating privacy protection processes – this would include any additional day-to-day staff costs associated with performing privacy-protecting and monitoring / auditing activities.
- Operating normal processes – any additional staff costs involved in performing normal operations due to the fact that personal privacy is being protected. (Of course, this could be negative if the addition of proper privacy protection reduces operational costs.)
- Mission limitation – are there any aspects of any normal legitimate business or service operation that are essentially privacy-invading and that could not be continued in a reasonable or sensible manner if personal privacy protection were to be considered paramount? If so, how is this conflict of interests addressed or resolved?
- Are there other cost components additional to those above? Are there any additional aspects to the components identified above?

### 4.2 Assessing expected costs

Unlike the benefits, expected costs can normally be assessed quite readily in financial terms.

- What, generally, are the relative cost contributions of the various cost components. Is the all-in cost of protecting personal privacy dominated by one component or are the costs more evenly spread?
- For those organisations who have cost figures for the personal privacy implementations they have been involved with in the past, what are the broad representative costs (as an all-in cost,

a cost per component, a cost per record, or in whichever form seems most appropriate) you have experienced?

- Are there cost components which cannot normally be assessed readily in financial terms (where, as above, we are using the term “costs” to include the burden in all its forms attributable to the protection of personal privacy)?

## 5 Deciding on personal privacy protection options

Armed with an understanding of the expected benefits and costs of protecting personal privacy within the organisation or one of its systems, the organisation then has to incorporate these into the methodology it uses for deciding whether or how to go ahead with a particular personal privacy protection proposal. A business case, which we would describe as that part of the process in which the various options are laid out and the opportunities, risks, alternatives, benefits or rewards are shown to be adequate (or not) to justify the costs, is often a central part of the methodologies organisations use. It is these decision-making methodologies we would like to cover here.

### 5.1 The decision-making process

Firstly, a look at the processes.

- What is the organisation's definition of business value? How is this measured?
- How is compliance with external mandates (of all types) considered when creating business cases?
- How are enterprise risk management practices included in business case development?
- Are the risks associated with suppliers, contractors, outsourcers, etc taken into account in business cases? If so, how?
- In outline, what are the various models and methodologies organisations would use and what are the basic requirements they would have for a privacy protection business case?
- Are there situations or times in which an organisation might decide on its privacy proposal without creating a privacy protection business case? When do these arise and how common are they?
- Is privacy treated in much the same way within the decision methodology as any other security requirement, or differently, and if so, how?
- Is privacy treated in much the same way within the decision methodology as, say, some quality requirement or non-functional requirement, or differently, and if so, how?
- Is privacy functionality treated in much the same way within the decision methodology as other aspects of desirable business functionality, or differently, and if so, how?
- Are business cases developed differently for changes to existing systems than for new systems, and if so, how?
- Are business cases developed differently depending on the range and scale of the project, and if so, in what ways?
- How is consultation on the options undertaken and what process is used to assess these?
- How are the implications on other processes addressed?
- What are the key factors for deciding to make an investment or ranking different investment opportunities against each other? What metrics are necessary (e.g. return on investment, net present value). How do less tangible benefits affect these? What degree of certainty is

required?

## **5.2 Resource constraints**

All implementations are subject to time, budget and resource constraints.

- Are these constraints applied in any way differently for implementations of privacy protection measures compared with implementations of other types of security measure, or quality measure, or business functionality?
- Are there other constraints which affect the way privacy protection implementations proceed? What would these be and what affect do they have?

## **5.3 Implementation and operation**

- What further development and evaluation of business cases are undertaken once a project has been started?
- How is the effect of greater privacy protection on other activities, processes, partners and stakeholders managed?
- What steps are undertaken to ensure the planned benefits will be realised on completion of the project?
- How are the benefits and costs actually achieved monitored and compared to the estimated values in the business plan? What would these be for privacy protection?

## 6 Approaches to providing privacy protection

Once the decision has been made to protect the privacy of the personal information used within the organisation, or within a specific process or system, the focus moves on to putting the necessary measures in place. However, to be effective, privacy protection measures need to be considered holistically rather than just as the selection of a number of individual point solutions. The organisation needs to have the governance and management arrangements in place, and sensible methodologies developed, if the specific measures implemented are to be worthwhile. Here we would like to cover the holistic approach to privacy protection.

### 6.1 Governance

What governance arrangements are appropriate to the protection of personal information?

- Where should ultimate accountability for the protection of personal information reside – with the CEO, the Chairman, other C level member of staff, other Director?
- Should operational accountability and the authority to make privacy-affecting decisions flow down through the business operations management structure or otherwise?
- How should major privacy-affecting initiatives or decisions be identified and handled?
- How should privacy-affecting decisions be made (by a senior Privacy Management Committee, the Risk Management Committee, by budget holders, by process owners, by business line management)?
- How should privacy-affecting decisions be reviewed (by a Privacy Management Committee reporting to the Board, by reference to a security function, by a periodic privacy audit)?
- Who should be responsible for setting privacy protection policy and standards within the organisation?
- Should privacy protection policy and standards be advisory or mandatory on those developing or enhancing internal systems and processes?
- What reporting structures are appropriate to informing stakeholders about the status of personal privacy protection within the organisation? Should the Annual Report have a section on Protecting Personal Privacy? Should organisations perform an annual audit of their arrangements and measures?
- Which sector-specific regulators have a track record of enforcing privacy protection standards within their sector, and what enforcement measures have they been seen to bring to bear?
- Which industry member accreditation bodies have a track record of enforcing privacy protection standards within their membership, and what levels of success have they been seen to have?

### 6.2 Methodologies

Once the governance arrangements have been set, those staff with privacy-related responsibilities will then be expected to execute those responsibilities in an appropriate manner. To do that, they will need to follow suitable methodologies to ensure that the privacy protection measures implemented into processes and systems are appropriate. What privacy methodologies do organisations employ?

- Do organisations tend to have a set of enterprise-wide privacy protection principles they try to

adhere to or is the approach to privacy protection more ad-hoc? When they do, what do these principles cover? Are they likely to be documented or just understood as part of the culture of the organisation?

- Do organisations typically take a risk-based approach to privacy protection, where privacy measures are applied to personal information according to an agreed view of risk, or a non-risk based approach where, for example, privacy measures are applied uniformly as standard to all personal information regardless of the risk?
- If taking a risk-based approach, is privacy considered within the organisation's enterprise-wide risk management practices or outside it? If outside, how then is it considered?
- Do organisations maintain a register of personal data - defining where, how and from whom it was collected, what consent is associated with it, where it is stored, how it is protected, where it is used, where it is transferred and its retention requirements?
- Do organisations conduct privacy impact assessments or privacy risk assessments? What form do these take, who is responsible for them, how formal or informal are they, and how much weight do they carry within the organisation?
- Are privacy risks discussed with system owners, risk owners or business leaders, and how much interest do people in these roles tend to have in the protection of personal privacy? Do people in these roles back up their expressed interest with adequate budget and timely action? Is privacy stated as an objective in their contracts of employment? Is their remuneration dependent on protecting personal information they are responsible for?
- Do organisations have a way of checking that all the personal information they collect has been gathered using legal and fair methods and that appropriate data subject consent has been obtained for the processing they will perform? In outline, how is this done?
- How are the results of privacy risk assessments actioned? Are formal monitored action plans agreed under which the required privacy protection measures will be implemented within a given time period, or is it left for the system owner, risk owner or business leader to implement a better level of privacy protection before the next review is conducted?
- How are privacy protection implementations assessed for suitability and completeness (e.g. as part of an acceptance test, periodically?) and which job function has the role of conducting these reviews?
- How are privacy issues addressed with suppliers and other organisations with whom personal information may be disclosed or shared, and especially how are privacy issues addressed when the third party is an organisation outside the EEA or an outsourced service provider? Do organisations impose contractual liability?
- Do organisations maintain a privacy incident handling process to ensure that incidents are always properly managed and that appropriate lessons are learned each time? Are staff and other parties encouraged to report possible incidents, confirmed or otherwise?

### 6.3 Measures

What measures might be considered part of "Good Standard Practice" and therefore can be expected to be found within most privacy protecting organisations? In particular:

- 
- Do organisations tend to provide system designers with privacy awareness training and train them in building privacy capabilities into processes and systems?
  - Do organisations tend to provide staff with privacy awareness training and train them in using the privacy controls built in to processes and systems?
  - Are the ICO's Good Practice Notes, Codes of Practice and Technical Guidance Notes used to guide the development of policies, standards and procedures?
  - Do organisations tend to provide meaningful information, code of business ethics, privacy notices, information charters and the like to customers/citizens or is the aim simply to tell the customer to put a tick in the consent box or else they will not be able to receive the service.
  - Is privacy consent (explicit and implicit) tracked within processes or systems to ensure that personal information is processed only for stated purposes and is shared only with accepted recipients?
  - Is privacy consent enforced on third parties such as suppliers, outsourcing partners, agency workers, etc?
  - Do organisations apply data minimisation techniques to reduce the amount of personal information collected, and to avoid non-personal data becoming tainted if it becomes associated with individual identifying information?
  - Are data de-identification and anonymisation techniques used to reduced the scope of personal information protection measures needed?
  - What measures are used to ensure that personal information is stored securely?
  - Is the reliability of personal information for its intended use checked? Do organisations proactively check their personal information is accurate and up-to-date?
  - Do organisations tend to make provision for people to access the information held about themselves and to request or make corrections to wrong or incomplete information?
  - Do organisations tend to make provision for people to instigate a complaints procedures when information access or corrections are denied?
  - What measures are used to ensure that access to personal information is restricted and controlled?
  - What measures are used to ensure that personal information is processed securely?
  - Do organisations track information retention requirements and undertake regular data disposal or deletion when it is no longer of use, or required?
  - Do organisations tend to carry privacy/data protection insurance?
  - Are data protection audits undertaken, either at a system-by-system level or at a business unit level?
  - Do organisations share privacy protection knowledge, experience and lessons learned from privacy breaches internally, and externally through collaborations, trade organisations and public dissemination?.

---

## Providing contributions

This document aims to describe and expand on some of the central issues that we believe need to be addressed within the project. We hope it will stimulate thought and discussion, and will give you a way to volunteer your contributions to this work. We are seeking your input on the issues covered and your thoughts on other issues which you believe to be central to the project's objectives. Your knowledge, experience and views will strengthen the field work that is taking place elsewhere within the project, and may be reflected in the final report.

### How to provide input

Owing to time constraints, we do not expect to be able to meet with contributors, so we would ask you to send your input by email to:

[privacy.protection@jlis.co.uk](mailto:privacy.protection@jlis.co.uk)

with "Discussion Document Contribution" in the subject line. You can send plain text responses, or a file attachment such as a word processing document or PDF.

We would ask for all responses to be submitted by **15 September 2009** and would like to thank all contributors in advance for their input to this important work.

We would welcome you providing us with general descriptive information about you and your organisation, though this is entirely at your discretion. We would also be pleased if you would provide contact details to us in case we want to follow up with you on any of the points you have raised.

We will acknowledge receipt of all contributions, where an email address is provided. We will not be able to acknowledge contributors by name in the final report, supporting documents or on the project website.

If you have any questions, please do not hesitate to contact the consultants (see Contacts below).

### What we will use the information for

Contributions provided will remain confidential to us and will not be shared with the ICO or any other party. However, we may wish to refer to or quote from contributions though we would ensure that the source of the contribution (either individual or organisation) was not and could not be identified unless the source provided their express consent. Please also read our privacy notice at the end of this document.

## About you (optional)

We would welcome you providing us with general descriptive information about you and your organisation, though this is entirely at your discretion. This will help us identify differences between organisation sector and size.

We would like to know:

- Whether you are responding to this document as an individual or on behalf of an organisation that handles data or in some other capacity.
- If you are responding on behalf of an organisation, which is that?
- In which geographical area are you/your organisation based (country name and county/region if in the UK)?
- If you are an organisation that handles personal data:
  - In what capacity are you responding (e.g. job title, roles and whether officially or unofficially)
  - Please provide a description of your organisation's legal status (e.g. charity, partnership, listed company, government department), sector and business activities
  - What is the size of your organisation?
    - Micro (<10 staff or ≤ €2 million annual turnover)
    - Small (<50 staff or ≤ €10 million)
    - Medium (<250 staff or ≤ €50 million)
    - Large
    - Not applicable
- If you would like confirmation that we have received your response, please tell us which email address to send the confirmation of receipt to.
- If you want to be contacted by us, perhaps to follow up with you on any of the points you have raised, please provide an email address and/or telephone number.

## Privacy notice

We (Watson Hall Ltd and John Leach Information Security Ltd) want to protect the privacy of individuals and other parties providing input to the "Business Case for Investing in Proactive Privacy Protection" project (the project) by responding to this discussion document, taking part in interviews or other discussions and correspondence. This privacy notice explains how we use any personal information collected.

### What information do we collect?

There are no mandatory parts of the response, but some people may give us personal information if they wish. By submitting your input by email we will know the sender's email address.

**What do we do with the information?**

We use the information solely for the purpose of the project. It will remain confidential to us and will not be shared with the ICO.

We do not use it for any marketing purposes. We do not sell, share or otherwise pass on any of the information onto any other individuals or organisation, unless you have asked us to or we are obliged to do so by law. We do not keep information indefinitely and will dispose of it when it is of no further use within the project or 12 months after the completion of the project, whichever is sooner. The information is stored only in the United Kingdom.

We utilise the project website usage information to monitor general activity, identify trends, and to investigate problems or errors.

**Inaccuracies and corrections**

We like to keep all information accurate and up to date. If you become aware of any errors or inaccuracies please let us know.

## Contacts

The project website is:

<http://watsonhall.com/privacy.protection>

For further information about the project, please contact either:



John Leach Information Security Ltd

Dr John Leach

Email [privacy.protection@jlis.co.uk](mailto:privacy.protection@jlis.co.uk)

Telephone 01264 332 477 / 07734 311 567

Web <http://www.jlis.co.uk/>



Watson Hall Ltd

Mr Colin Watson

Email [privacy.protection@watsonhall.com](mailto:privacy.protection@watsonhall.com)

Telephone 020 7183 3710 / 07811 132 972

Web <http://www.watsonhall.com>

Watson Hall Ltd is a company registered in England under number 60004969, whose registered office is at North Bastle, Gatehouse, Northumberland NE48 1NG. John Leach Information Security Ltd is a company registered in England under number 4602412, whose registered office is at Aldwych House, Winchester Street, Andover, Hampshire SP10 2EA.

This is a working document and we will be releasing updated versions from time to time as contributions come in. Please check the project website periodically.

<b>Date</b>	<b>Version</b>	<b>Change</b>
14 Aug 2009	1.0	First version issued available at <a href="http://watsonhall.com/resources/downloads/pp-dd-10x.pdf">http://watsonhall.com/resources/downloads/pp-dd-10x.pdf</a>
17 Aug 2009	1.1	Minor text changes and additions highlighted in <a href="http://watsonhall.com/resources/downloads/pp-dd-11c.pdf">http://watsonhall.com/resources/downloads/pp-dd-11c.pdf</a> Clean version available at <a href="http://watsonhall.com/resources/downloads/pp-dd-11x.pdf">http://watsonhall.com/resources/downloads/pp-dd-11x.pdf</a>
25 Aug 2009	1.2	Deadline change, minor text changes and additions highlighted in <a href="http://watsonhall.com/resources/downloads/pp-dd-12c.pdf">http://watsonhall.com/resources/downloads/pp-dd-12c.pdf</a>

<b>Version</b>	1.2
<b>Status</b>	Issued
<b>Date issued</b>	25 Aug 2009