



Information Commissioner's Office

Promoting public access to official information
and protecting your personal information

The Business Case for Investing in Proactive Privacy Protection

**Tendering brief on the production of a report and supporting
business case materials**

June 2009

1. Background

In 2008 the ICO commissioned and published a report into [Privacy by Design](#). The ICO's aim with the promotion of the 'Privacy by Design' concept is to ensure that as information systems which hold personal information and allied business processes are developed, privacy concerns are identified and addressed from first principles. In short, this means designing in privacy and data protection compliance not ignoring it or bolting it on as an inadequate afterthought.

The Privacy by Design report has identified one of the barriers to more proactive privacy protection as being the absence of a soundly argued business case for expending money on privacy friendly systems and business processes. Organisations do not put an appropriate value on privacy protection when procuring new systems and adopting new business processes or identify the potential cost to the organisation of having poor privacy protection controls in place. High profile data losses and continued media interest in the vulnerability of individuals to the unwarranted exploitation of their personal information highlight the increased level of data protection risk that needs to be addressed by organisations if their customers trust and confidence is to be maintained and strengthened.

Technological capabilities have advanced and these are fully utilised to exploit personal information for the benefit of an organisation but there has not been a similar effort to exploit technology to protect personal privacy. This gap needs closing and this will require those procuring systems and implementing business processes to understand the benefits and the value of investing in privacy friendly systems.

2 Objectives

The aim of the project is to develop and articulate a sound and persuasive business rationale for an organisation investing in privacy friendly features when procuring new systems and implementing business processes even though these may not represent the cheapest option at first sight. Putting an appropriate value on personal information as an asset, quantifying the risk to it and the cost to an organisation and its reputation if problems occur, will be important aspects.

It is important that this financial rationale stands up to scrutiny by those who are unfamiliar with data protection requirements or wider privacy concerns. The end product would be a document setting out the business case for investing in proactive privacy protection that those procuring information systems or implementing new business processes can readily use when specifying, acquiring and implementing these systems and processes. The

rationale should also be relevant when organisations are considering developing and improving current systems and processes.

The aim of the project is to make a business case that is readily understandable by those who make expenditure decisions within an organisation's corporate governance structure and assist those who are involved in preparing such cases to identify the value of effective privacy protection and provide them with materials to help them make a persuasive business case.

3 Methodology and component elements

It is anticipated that the project would be undertaken by those with expertise in developing business cases and other such justifications for expenditure. Knowledge of data protection legislation, wider privacy concerns and technological developments would also be essential attributes. It would be up to bidders to set out their planned methodology as much would depend upon their own existing expertise in these fields. However the following are likely to be significant features within the approach adopted:

- To gain an understanding of the organisational processes involved in procuring information systems and implementing new business processes (e.g. public and private sector organisations, professional services organisations, systems developers, OGC, etc) in order to develop an appropriate approach and materials
- To research and detail the value of personal information as an asset, studying any materials that are available and contacting those who are already active in this field
- To quantify the potential risk to personal information, developing an understanding of the associated cost of these risks including those arising from changes to the data protection regulatory regime to permit the imposition of monetary penalties
- Soliciting feedback from some organisations who may benefit from the work in future to see if the report findings and materials would be effective in practice

We will expect the successful bidder to undertake the bulk of any necessary research work based upon their own knowledge, experience and contacts. The ICO will also make available suggested contacts that may be able to assist in this work. Additionally the ICO will put out a general statement on the ICO website and in our e-newsletter inviting those with an interest to contact us and these contacts can be passed on to the successful bidder.

4 Deliverables and Timings

The main deliverable is a short report that could be published in a document of up to 25 pages written in an accessible and engaging style meeting the objectives mentioned above. The primary distribution format will be electronic, downloadable from the ICO website. As with any report commissioned by the ICO it must be impartial and conclusions based upon a reasonable assessment of the information and evidence collected. The report should also be accompanied by further materials that would be of assistance to those compiling business cases such model formats for conveying the necessary information and be customisable to a users needs. The report and allied materials will need to be written in a manner consistent with the ICO's role as a respected regulator adopting a considered and evidence based approach.

The final text of any report and materials will need to be agreed with the ICO who will retain full editorial control and make all decisions as to format and publication. The ICO will retain all the intellectual property rights to the report and materials but the author will be given credit for their work in any published document. The ICO use a standard form of research project contract to cover such details and this is available as part of the tender materials.

The report will also need to be written in a manner consistent with the ICO's own style guide covering the use of written english. This will be made available to the successful bidder.

During the progress of the work a regular update will need to be provided on a fortnightly basis to the ICO manager responsible for overseeing the work. ICO advice and appropriate assistance will be available through out the progress of the work. A payment schedule will be agreed in advance and any staged payments will need to be linked to completed work items.

The finished report **must** be delivered to the ICO by the 2 November 2009 at the latest. A final draft should be submitted by 16 October 2009 at the latest to allow for any editorial changes to be discussed and incorporated. Meeting these deadlines is essential as a launch event may be held in early December 2009

5 Tendering process

A written proposal should be lodged with the ICO by 1000 on 20 July 2009 with 5 copies of any documentation included. It should be addressed to:

Christian Senior
Research Project 2009BC
ICO
Wycliffe House
Water Lane

Wilmslow SK9 5AF
United Kingdom

The proposal can also be sent by e-mail to christian.senior@ico.gsi.gov.uk by the same deadline. The proposal must include the bidders' expertise in the field, clearly defined deliverables and timescales together with the methodology to be employed. The cost of the work (including VAT and any relevant additional items of expenditure) and proposed payment schedule should also be clearly set out. The proposal documentation should be concise and expressed in clear English as this will be a criterion relevant to the awarding of the contract. It should also make clear whether the organisation has or intends to sign the ICO's Personal Information Promise. The full criteria are set out below.

In awarding this contract the following criteria will be taken into account:

- The expertise and experience of the bidder in the areas of developing business plans and other such justifications for expenditure together with their knowledge of UK data protection legislation, wider privacy concerns and technological developments
- Track record of undertaking similar projects on time and on budget
- Methodology to be employed including testing out emerging results
- The proposed deliverables and dates for completion
- Ability to write documents in clear English free from unnecessary jargon
- Cost and value for money. A budget in the region of £50,000 has been allocated for this work
- Where there are bids that cannot be separated on the above grounds, whether the bidding organisation has signed or intends to sign the [Personal Information Promise](#)

The proposals will be considered in week commencing 20 July 2009 in accordance with the ICO's tendering procedures. A small panel will be convened to decide upon the successful bidder. This panel will not have access to submitted proposals until after the close of the tendering exercise. The bidders will be contacted before 25 July 2009 to let them know the outcome of their proposals.

If further information is required prior to submitting a proposal then Jonathan Bamford, the Assistant Information Commissioner who is leading this work, can be contacted on jonathan.bamford@ico.gsi.gov.uk in the first instance.

JB BCIPPP v.1
11.06.09