

Privacy by Design Report Recommendations: ICO Implementation Plan

Theme	Barriers to Privacy by Design	Desired Privacy Outcomes	Recommendations for Delivering Privacy by Design
ENGAGING EXECUTIVE MANAGEMENT	<ul style="list-style-type: none"> Executive managers don't always recognise or correctly prioritise their organisation's responsibility or their own accountability for protecting individuals' privacy. Executives and their staff often lack a shared language to discuss or to specify privacy requirements in a clear unambiguous way. As a result, poor privacy specifications deliver poor privacy controls. Commercial risks and benefits of managing personal information are often unclear, making it hard to justify privacy investment. In consequence privacy needs are often omitted from the business cases for new systems. 	<p>Executive managers understand their privacy duties and communicate their privacy management wishes across the organisation.</p> <p>Business cases for new systems incorporate privacy specifications that are understood by all members of staff.</p>	<p>The executive managers of public authorities and private organisations need greater awareness of their privacy responsibilities, and this should be supported by:</p> <ul style="list-style-type: none"> providing sample costs, risks and benefits cases to demonstrate the value of privacy compliance; and promoting a simple shared language for key privacy concepts such as data minimisation, identification, authentication and anonymisation to assist communication within and outside of organisations. <p>The ICO and other regulatory bodies have a role in making this happen.</p>
ICO action points	<ul style="list-style-type: none"> The report has rightly highlighted the importance of raising the awareness of executives of their responsibilities and own accountability for protecting people's privacy. We intend to develop a 'personal information promise' where senior executives make a personal commitment to protect people's privacy on their organisations behalf. The Ministry of Justice is proposing to make changes to the data protection notification arrangements. If possible, we will consider giving organisations the opportunity to say what they have done to protect personal information, for example if they have published a PIA. We will consider whether to commission research into setting out the business case for protecting privacy to develop greater understanding of the true cost of data losses, perhaps developing a model business case that puts a price on data protection risk. We are also looking at how business insurance premiums reflect risks to personal information and the steps taken by organisations to protect it. We will explore how to promote a common shared language to help people discuss and specify privacy requirements. We will do more to help explain key concepts, for example we could articulate what concepts such as "data minimisation" mean in practice; and the difference between identification and authentication. 		
PLANNING FOR PRIVACY BY DESIGN	<ul style="list-style-type: none"> Traditional risk management methodologies often fail to consider the value of personal information, and hence do not take privacy needs into account. Risk assessment approaches often fail to manage privacy needs throughout the systems lifecycle, so many bespoke and off-the-shelf systems are still built 	<p>Systems incorporate appropriate PETs based upon a rigorous Privacy Impact Assessment.</p> <p>Privacy needs are</p>	<ul style="list-style-type: none"> Organisations should be encouraged to implement high-level privacy management policies that will call for: <ul style="list-style-type: none"> - incorporating Privacy Impact Assessments throughout the systems lifecycle from business case to decommissioning; - managing privacy-related risks to within pre-defined levels; - potentially submitting Privacy Impact Assessments for the

	<p>without proper or innovative privacy controls.</p> <ul style="list-style-type: none"> • Privacy needs are often not rigorously considered at any stage of the systems lifecycle, so systems can be modified or re-used without consideration for privacy implications. • Systems do not always support automated Subject Access Requests, and hence information retrieval procedures can be onerous for organisations. 	<p>managed throughout the systems lifecycle.</p>	<p>most sensitive systems to the ICO for verification; and</p> <ul style="list-style-type: none"> - promoting greater transparency by publishing Privacy Impact Assessments (this possibly being mandatory for public sector organisations). • Organisations should be urged to demonstrate that all new systems support automated Subject Access Requests, and encouraged to implement online Subject Access Request services where appropriate.
ICO action points	<ul style="list-style-type: none"> • We support the recommendations that the management of privacy, including the use of Privacy Impact Assessments (PIAs), should be built in throughout the system lifecycle and we are taking this forward through our PIA Implementation Plan. • We shall continue to promote the use of PIAs and have published a 2 page summary overview of the PIA process to coincide with the publication of the report. We shall also publish a revised version of the PIA Handbook in early 2009. • We support and will promote the recommendation that all new systems should be able to support automated subject access requests where appropriate. 		
SHARING PERSONAL INFORMATION	<ul style="list-style-type: none"> • The pressure to share personal information within and outside of organisations can lead to privacy-related problems: <ul style="list-style-type: none"> - data from 'privacy-friendly' systems are shared with other systems that are less able to respect privacy needs; - copies of personal information in transit are not always appropriately secured; - organisations often aggregate data rather than sharing it; - identifiers are used as indices, making it hard to anonymise data thereafter; and - privacy metadata can be lost as information is shared between systems. • If system PIAs are conducted in isolation the results may fail to take into account the broader systemic implications of data sharing. 	<p>Organisations can share data internally and externally, and individuals have confidence that their privacy wishes will be respected when they do so.</p> <p>Individuals know who has their personal information and are able easily to access and amend it.</p>	<p>Government, regulators, industry and academia should reinvigorate research into standards for data sharing, including:</p> <ul style="list-style-type: none"> • formalising approaches for collecting and managing privacy metadata; • developing PIA processes that can take into account the privacy implications of sharing data across many different systems; and • defining acceptable information security controls for the exchange of personal information. <p>The ICO will be in a position to guide and support this work.</p> <p>Future awareness initiatives from the ICO and other relevant regulators should restate and promote principles of data minimisation across all organisations.</p>
ICO action points	<ul style="list-style-type: none"> • The Ministry of Justice, in its response to the Thomas/Walport data sharing review, has stated that separate legislation will be introduced requiring the ICO to publish a statutory code of practice on sharing personal information. The ICO published the <i>Framework Code of Practice for Sharing Personal Information</i> in October 2007 and this may form the basis for any statutory code the ICO may produce. This could take account of security, data standards and data minimisation. • Our revised PIA handbook will help organisations take account of the privacy implications of data sharing and we will endeavour to make a PIA part of the proposed statutory code. 		

	<ul style="list-style-type: none"> We will look at the concept of privacy metadata to see what needs to be done to promote this in practice. 		
DEVELOPING PRACTICAL PRIVACY STANDARDS	<ul style="list-style-type: none"> Organisations are often uncertain how to implement systems that comply with data protection law, and are left to manage privacy in accordance with 'best efforts', with each system approaching the issue on a case-by-case basis. There are no internationally-recognised standards to guide organisations in implementing privacy controls. 	<ul style="list-style-type: none"> Organisations are able to operate in compliance with consistent, affordable, provable privacy standards, in much the way they already do with information security standards. 	<ul style="list-style-type: none"> Government, regulators, industry and academia should be encouraged to develop practical standards for privacy implementation, supported by guidelines for the functionality and specific technologies that should be considered for incorporation into new systems. This initiative has to come from the organisations themselves so that they contribute and collaborate to ensure that resultant standards meet their needs. The work should not be in isolation, but rather should engage with similar emerging initiatives elsewhere. The ICO has a role to play in guiding and supporting the initiative.
ICO action points	<ul style="list-style-type: none"> Whilst some standards are set out in the codes of practice that we and others have produced, we recognise that there is value in the further development of common practical standards but agree with the report that this needs to be dealt with on an international basis. ISO are already doing work in this area. It has been suggested that standards could be used to bridge the gap between different data protection regulatory regimes and we shall play our part in discussions on this within the international privacy and data protection commissioner community. 		
PROMOTING PRIVACY ENHANCING TECHNOLOGIES	<ul style="list-style-type: none"> PETs have yet to find widespread adoption in 'real world' environments because organisations and vendors are fearful of committing to specific PETs in case these quickly prove to be obsolete as technologies develop. Web 2.0, Cloud Computing and Service Oriented Architecture developments will most likely add further complexity to this problem. 	<ul style="list-style-type: none"> Vendors are encouraged to incorporate PETs and privacy functions into their off-the-shelf systems and to promote these as selling points. Organisations adopt PETs into their systems where appropriate. PETs are recognised as valuable tools to support the management of personal information. 	<p>Government, regulators, industry and academia need to work together to support existing and future PETs research, and in particular encourage research into:</p> <ul style="list-style-type: none"> mechanisms to simplify obtaining and managing consent, revocation and data minimisation; 'privacy-friendly' identification and authentication systems; and methodologies to test and prove the effectiveness of privacy controls in systems and across organisations. <p>Successful initiatives should be developed into practical standards, and buyers encouraged to demand better privacy functionality from vendors.</p>
ICO action points	<ul style="list-style-type: none"> We agree that there is a need to continue to build knowledge in this area and we will redouble our efforts to promote this based upon the findings of the report. The European Commission is promoting the wider use of PETs through funding research. We want to build on what is being done by European Commission in our future work. We shall actively encourage buyers and suppliers of systems to consider PETs as a natural part of acquiring information systems that process personal information. We will continue to promote awareness of different forms of privacy friendly identity management and will publish additional information to raise awareness still further. 		

<p>MANAGING COMPLIANCE AND REGULATION</p>	<ul style="list-style-type: none"> • The ICO lacks the necessary resources and powers to detect, investigate and where necessary enforce compliance through punitive sanctions. In consequence, individuals perceive organisations as unaccountable when privacy problems arise. • Many organisations treat the DPA as ‘just another compliance issue’, which is not necessarily enough to ensure effective privacy management controls. • Despite the ICO’s guidance, organisations are sometimes uncertain about what constitutes personal information or what powers individuals have over that data. • Privacy professionals operate in an unregulated environment where there are few recognised qualifications or accreditation bodies. This makes it hard for organisations to gauge the level of competence of the individual practitioner, or to trust that person’s work. 	<ul style="list-style-type: none"> • Individuals know that organisations will be held to account for proper management of personal information. • Organisations have a clear understanding of what information is considered to be personal and what powers individuals have over it. • Privacy professionals are trained and accredited to known standards. 	<ul style="list-style-type: none"> • Regulators and government should explore the idea of obliging organisations to nominate an executive-level representative who will be held accountable for proper management of personal information. • The government needs to recognise the realistic increased funding requirements of an empowered ICO that can both promote and enforce privacy practices. • The ICO should examine whether there is a need for any further guidance on what constitutes personal information, and continue to deliver practical advice for organisations about what powers individuals have over their data. • There is a pressing need for the development of a professional body for privacy practitioners (possibly under the aegis of an existing chartered body). The aim of this body will be to train, accredit and promote the work of privacy professionals. Clearly the ICO will have an important role in supporting this.
<p>ICO action points</p>	<ul style="list-style-type: none"> • We welcome the key findings and recommendations relating to the management of compliance and regulation. • We have already made a persuasive case for increased powers and penalties and the Ministry of Justice is proposing to introduce legislation to provide significant new powers for the ICO. • We will continue to ensure our regulatory action strategy is targeted on data protection risk as new technologies and uses develop. • We will continue to make sure that we provide clear advice on whether personal information is processed in new developments where there is confusion. • We will consider whether more needs to be done to ensure that there are skilled privacy professionals to help organisations take privacy protection seriously. 		

26/11/08