Information Governance Checklist and Privacy Impact Assessments

Authorship:	Chris Wallace – Information Governance Manager
Committee Approved:	Audit Committee
Approved date:	1 Feb 2014
Latest Review Date:	September 2015
Review Next Due	April 2017
Target Audience:	All Staff
Policy Reference No:	*N/A*
Version Number:	*V1.0*
Business Critical data	*Yes*
Business Critical System	*Yes*

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

Contents

STANDARD AMENDMENTS

Amendments to the Standard will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	Chris Wallace	First draft for comments	NR	
0.2	C. Wallace	Amendments to reflect ICO Guidance	Dec 2014	
1.0	I.G. Officer	• Refresh of Introduction and purpose of the privacy impact assessments • Addition of requirement to add information assets to Information Asset Register and complete associated Data Flow Maps.	Sept 2015	

Introduction

The organisation needs to ensure that they remain complaint with legislation and NHS requirements such as the Information Governance Toolkit with its use of Personal Confidential Data (PCD). The Information Governance Checklist and Privacy Impact Assessments (PIA) have been developed to provide an assessment prior to new services or new information processing/sharing systems being introduced.

Privacy Impact Assessments (PIAs) identify the most effective way to comply with data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow for the identification and remedy problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

A PIA enables an organisation to analyse how a particular project, process or system will affect the privacy of the individuals. Conducting a PIA does not have to be complex or time consuming.

PIAs should be carried out at the planning stage of any new processes or systems implementations where there is a risk that personal data may be compromised e.g. a new IT system for storing and accessing personal data or using existing data for a new and unexpected or more intrusive purpose.

Responsibilities

Responsibility for ensuring that Information Governance Checklists and Privacy Impact Assessments are completed, where required, resides with all Service Managers and Directorate Heads.

Line Managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of the Information Governance Checklist and Privacy Impact Assessment process.

On a day-to-day basis staff of all levels that are introducing a new system be it electronic or paper based, should use this document to ensure that processing remains compliant with current legislation.

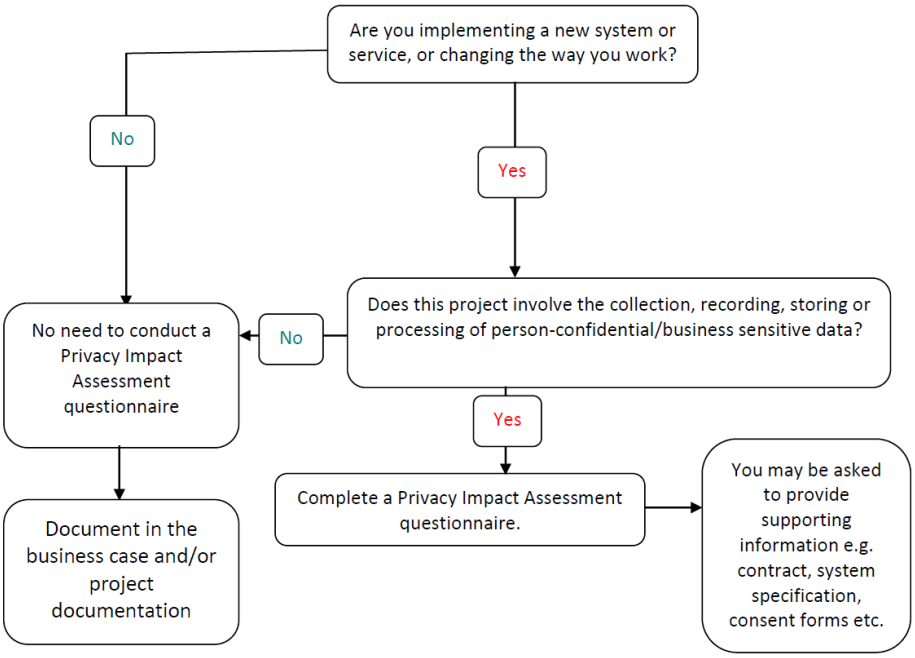
This guidance applies to all staff and all types of information held by the organisation. Further details of responsibilities are to be found in the organisation policies and procedures and in the Information Governance handbook.

Privacy Impact Assessment

A PIA is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions. A PIA is necessary to identify and manage risks; to avoid unnecessary

costs; to avoid inadequate solutions to privacy risks; to avoid loss of trust and reputation; to inform the organisation's communication strategy and to meet or exceed legal requirements. There is no statutory requirement for any organisation to complete a PIA, however, central government departments have been instructed to complete PIAs by the Cabinet Office. The overall PIA process is operated under the supervision of the Information Commissioners Office (ICO) who is responsible for the production of guidance materials.

Is a PIA required for every project?



Not every project will require a PIA. The ICO envisages PIAs being used only where a project includes the use of personal data, or where there could be a risk to the privacy of the individual PIAs will usually be recommended where a change of the law will be required, new and intrusive technology is being used, or where private or sensitive information which was originally collected for a limited purpose is going to be reused in a new and unexpected way. The screening questions (see Annex A) help determine if a PIA is required and if so which of the two options will be suitable.

Purpose of a PIA

- Identify privacy risks to individuals;
- Identify privacy and Data Protection compliance liabilities;
- Protect the organisations reputation;
- Instil public trust and confidence in your project/product;
- Avoid expensive, inadequate "bolt- on" solutions; and
- Inform your communications strategy.

Following review of the screening questions it may be decided that a PIA is required. There are two types of PIA, a small scale and a full scale. Where it is thought that a PIA is needed

the small scale form, located at Annex B, will be used and submitted to the Information Governance Team who can review prior to the PIA being submitted to the IG Committee/Caldicott Guardian/SIRO the small scale form completed and advise on whether a full scale PIA needs to be completed.

When should I start a PIA?

PIAs are most effective when they are started at an early stage of a project, when:

- the project is being designed;
- you know what you want to do;
- you know how you want to do it; and
- you know who else is involved.

But it must be completed before:

- decisions are set in stone;
- you have procured systems;
- you have signed contracts/ MOUs/agreements; and
- while you can still change your mind.

Publishing PIA's

All PIA's will be included within the organisation's Publication Scheme.

It is acknowledged that PIA's may contain commercial sensitive information such as security measures or intended product development. It is acceptable for such items to be redacted but as much of the document should be published as possible given all information within a public organisation can be requested through the Freedom of Information Act and will be listed in the Publication Scheme.

Related Policies

Information Security Policy
Data Protection and Confidentiality Policy
Safe Haven Guidelines and Procedure
Network Security Policy
Records Management Information Lifecycle Policy

Relevant statutory legislation and law

Data Protection Act 1998
Human Rights Act 1998
Freedom of Information Act 2000

Common Law Duty of Confidentiality

Further reading and Guidance

- The ICO's Anonymisation: managing data protection risk code of practice may help identify privacy risks associated with the use of anonymised personal data. It's a short video covering the subject
- The ICO's Privacy Notices: Code of Practice.
- The ICO's Data sharing: code of practice may help to identify privacy risks associated with sharing personal data with other organisations.
- Caldicott 2 Review Report and Recommendations

ANNEX A – Privacy Impact Assessment Screening Questions

These questions are intended to help decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA is required. This is not an exhaustive list so if you have any concerns regarding the purposed project/changes please complete the PIA.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics, facial recognition or automated decision making.
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

Will the project require you to contact individuals in ways which they may find intrusive?

ANNEX B - Privacy Impact Assessment Proforma

This document must be completed for any new / or change in service which plans to utilise personal confidential information. It must be completed as soon as the new service / or change is identified by the Project Manager / System Manager or Information Asset Owner.

This process is a mandated requirement on the Information Governance Toolkit to ensure that privacy concerns have been considered and actioned to ensure the security and confidentiality of the personal identifiable information.

There are 2 types of Privacy Impact Assessments – a small scale and full scale. This proforma is based on the Small Scale PIA. Following completion of this proforma, it may be necessary to conduct a Full Scale PIA. Full details are available in the Information Commissioner's handbook Privacy Law compliance checks and Data Protection Act compliance checks are part of the PIA process – the questions to assess this are included in the proforma.

Please complete all questions with as much detail as possible and return the completed from to: infogov.nyhcsu@nhs.net

Further guidance on specific items can be found on the Information Commissioner's website.

www.ico.gov.uk

Section A: New/Change of System/Project General Details

Name:		
Objective:		
Background: Why is the new system / change in system required? Is there an approved business case?		
Benefits:		
Constraints:		
Relationships: (for example, with other Trust's, organisations)		
Quality expectations:		
Cross reference to other projects:		
Project Manager:	Name:	
	Title:	
	Department:	
	Telephone:	
	Email	
Information Asset Owner: (All systems/assets must have an Information Asset Owner (IAO). IAO's are normally the Heads of Departments and report to the SIRO)	Name:	
	Title:	
	Department:	
	Telephone:	
	Email	

Information Asset Administrator: (All systems / assets must have an Information Asset Administrator (IAA) who reports the IAO as stated above. IAA's are normally System Managers / Project Leads)	Name:	
	Title:	
	Department:	

	Telephone:	
	Email	
Deputy Information Asset Administrator: (It is necessary that there is a deputy in place for when the IAA is absent from the workplace for whatever reason)	Name:	
	Title:	
	Department:	
	Telephone:	
	Email	
Customers and stakeholders:		

Ensure that this information asset is added to the CCG Information Asset Register.

Section B Privacy Impact Assessment Key Questions

Question	Response	Ref to key req. e.g. IGTK, Small scale PIA etc
1. Will the system/project/process (will now be referred to thereafter as 'asset') contain Personal Confidential Data or Sensitive Data? If answered 'No' you do not need to complete any further information as PIA is not required.	☐ No ☐ Patient ☐ Staff ☐ Other (specify)	
2. Please state purpose for the collection of the data: for example, patient treatment, health administration, research, audit, staff administration		
3. Does the asset involve new privacy–enhancing technologies? Encryption; 2 factor authentication, pseudonymisation, e.g. smartcard and pin code	☐ Yes ☐ No If yes, please give details:	SS PIA (1)
4. Please tick the data items that are held in the system **Personal** **Sensitive**	☐ Name ☐ Address ☐ Post Code ☐ Date of Birth ☐ GP ☐ Consultant ☐ Next of Kin ☐ Hospital (District) No. ☐ Sex ☐ NHS Number ☐ National Insurance Number ☐ Treatment Dates ☐ Sex ☐ Diagnosis ☐ Religion ☐ Occupation ☐ Ethnic Origin ☐ Medical History ☐ Staff data (Pay, Union etc) Other (please state here):	

5. Will the asset collect new personal data items which have not been collected before?	☐ Yes ☐ No If yes, please give details:	SS PIA (5)
6. What checks have been made regarding the adequacy, relevance and necessity for the collection of personal and/or sensitive data for this asset?		SS PIA (2 & 10)
7. Does the asset involve new or changed data collection policies that may be unclear or intrusive?	☐ Yes ☐ No	SS PIA (9)
8. Is the third party contract/supplier of the system registered with the Information Commissioner? What is their notification number?	☐ Yes ☐ No Data Protection Act Notification Number:	
9. Has the third party supplier completed an Information Governance Toolkit Return?	☐ Yes ☐ No If yes, please give percentage score:	
10. Does the third party/supplier contracts contain all the necessary Information Governance clauses including information about Data Protection and Freedom of Information?	☐ Yes ☐ No	IG TK 110
11. Does the asset comply with privacy laws such as the Privacy and Electronic Communications Regulations 2003 (see appendix for definition)	☐ Yes ☐ No	Privacy Law Check
12. Who provides the information for the asset?	☐ Patient ☐ Staff ☐ Others – Please specify e.g. Interfaces from PAS	
13. Are you relying on individuals (patients/staff) to provide consent for the processing of personal identifiable or sensitive data?	☐ Yes ☐ No	

14. If yes, how will that consent be obtained? Please state:		
15. How will consent and non consent be recorded?		
16. If consent is not the basis for processing which legal justification is being used?	☐ Court Order ☐ Public Interest ☐ Other (detail below)	
17. Have the individuals been informed of and have given their consent to all the processing and disclosures? **Have both the CCG's Data Protection Registration and Privacy Notice been updated to include this information processing**	☐ Yes (explicit) ☐ No ☐ Yes (implicit in leaflets, on website) ☐ Yes ☐ No	IGTK
18. How will the information be kept up to date and checked for accuracy and completeness?		
19. Who will have access to the information within the system?		
20. Do you intend to send direct marketing messages by electronic means? This includes both live and pre-recorded telephone calls, fax, email, text message and picture (including video)? **Is the intention to use direct marketing included in the information leaflet / consent form**	☐ Yes ☐ No ☐ Yes ☐ No	Privacy Check
21. If applicable, are there procedures in place for an individual's request to prevent processing for purposes of direct marketing in place?	☐ Yes ☐ No	Privacy Check
22. Is automated decision making	☐ Yes ☐ No	Privacy

used? **If yes, how do you notify the individual?**			Check
23. Is there a useable audit trail in place for the asset. For example, to identify who has accessed a record?	☐ Yes	☐ No	IGTK
24. Have you assessed that the processing of personal/sensitive data will not cause any unwarranted damage or distress to the individuals concerned? What assessment has been carried out?	☐ Yes	☐ No	
25. What procedures are in place for the rectifying/blocking of data by individual request or court order?			
26. Does the asset involve new or changed data access or disclosure arrangements that may be unclear?	☐ Yes	☐ No	SS PIA (12)
27. Does the asset involve changing the medium for disclosure for publicly available information in such a way that data become more readily accessible than before? (For example, from paper to electronic via the web?)	☐ Yes	☐ No	SS PIA (14)
28. What are the retention periods (what is the minimum timescale) for this data? (please refer to the Records Management: NHS Code of Practice)			SS PIA (13)
29. How will the data be destroyed when it is no longer required?			IGTK
30. Will the information be shared with any other establishments/ organisations/Trust's?	☐ Yes	☐ No	IGTK, PIA 4

31. Does the asset involve multiple organisations whether public or private sector? Include any external organisations. Also include how the data will be sent/accessed and secured. **Has the requirement for an Information Sharing Agreement been considered and documented where necessary**	☐ Yes ☐ No	
32. Does the asset involve new linkage of personal data with data in other collections, or is there significant changes in data linkages?	☐ Yes ☐ No	SS PIA (8)
33. Where will the information be kept/stored/accessed?	☐ On paper ☐ On a database saved on a network folder/drive ☐ Website ☐ On a dedicated system saved to the network ☐ Other – please state below:	
34. Will any information be sent off site **If 'Yes' please detail the data flows. This can be on a separate page if flow charts are to be used.**	☐ Yes ☐ No	IGTK 208 & 308
35. Please state by which method the information will be transported	☐ Fax ☐ Email ☐ Via NHS Mail ☐ Website ☐ Via courier ☐ By hand ☐ Via post – internal ☐ Via telephone ☐ Via post - external ☐ Other – please state below:	IGTK 208 & 308
36. Are you transferring any personal and / or sensitive data to a country outside the	☐ Yes ☐ No	IGTK 209

European Economic Area (EEA)? **If yes, where?**		
37. What is the data to be transferred to the non EEA country?		IGTK 209
38. Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?	☐ Yes ☐ No ☐ Not applicable	IGTK 209
39. Have you checked that the non EEA country has an adequate level of protection for data security?	☐ Yes ☐ No ☐ Not applicable	IGTK 209
40. Is there a Security Management Policy and Access Policy in place? Please state policy titles.	☐ Yes ☐ No	SS PIA (11)
41. Has an information risk assessment been carried out and reported to the Information Asset Owner (IAO)? **Where any risks highlighted – please provide details and how these will be mitigated?** **Was process approved by SIRO?**	☐ Yes ☐ No	Risk Ass
42. Is there a contingency plan / backup policy, or business continuity plan in place to manage the effect of an unforeseen event? Please provide a copy.	☐ Yes ☐ No	Risk Ass
43. Are there procedures in place to recover data (both electronic /paper) which may be damaged through: • **Human error**	☐ Yes ☐ No	Risk Ass

• **Computer virus** • **Network failure** • **Theft** • **Fire** • **Flood** • **Other disaster** **Please provide policy titles.**		

Evaluation

44. Is the PIA approved? **If not, please state the reasons why and the action plan put in place to ensure the PIA can be approved**	☐ Yes	☐ No

Ensure the information flow is mapped and assessed.

Form completed by:

Name: .....

Title: .....

Signature: .....

Date: .....

Information Governance Group Approval

Name: .....

Title: .....

Signature: .....

Date: .....

Appendix A– Glossary of Terms

Item	Definition
Personal Data	This means data which relates to a living individual which can be identified: A) from those data, or B) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also 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
Sensitive Data	This means personal data consisting of information as to the: A) racial or ethnic group of the individual B) the political opinions of the individual C) the religious beliefs or other beliefs of a similar nature of the individual D) whether the individual is a member of a trade union E) physical or mental health of the individual F) sexual life of the individual G) the commission or alleged commission by the individual of any offence H) any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings
Direct Marketing	This is “junk mail” which is directed to particular individuals. The mail which are addressed to “the occupier” is not directed to an individual and is therefore not direct marketing. Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you. Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.
Automated Decision Making	Automated decisions only arise if 2 requirements are met. First, the decision has to be taken using personal information solely by automatic means. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second requirement is that the decision has to have a significant

	effect on the individual concerned.
European Economic Area (EEA)	The European Economic Area comprises of the EU member states plus Iceland, Liechtenstein and Norway
Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.
SIRO (Senior Information Risk Owner)	This person is an executive who takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board
IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.
IAA (Information Asset Administrator)	There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers
Implied consent	Implied consent is given when an individual takes some other action in the knowledge that in doing so he or she has incidentally agreed to a particular use or disclosure of information, for example, a patient who visits the hospital may be taken to imply consent to a consultant consulting his or her medical records in order to assist diagnosis. Patients must be informed about this and the purposes of disclosure and also have the right to object to the disclosure.
Explicit consent	Express or explicit consent is given by a patient agreeing actively, usually orally (which must be documented in the patients casenotes) or in writing, to a particular use of disclosure of information.
Anonymity	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases

	the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.
Pseudonymity	This is also sometimes known as reversible anonymisation. Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Information Risk	An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further information.
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, new and sound threatening are a concern and hence represent a risk
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can very the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.
Records Management: NHS Code of Practice	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.

Data Protection Act 1998	This Act defines the ways in which information about living people may be legally used and handled. The main intent is to protect individuals against misuse or abuse of information about them. The 8 principles of the Act state The fundamental principles of DPA 1998 specify that personal data must: • be processed fairly and lawfully. • be obtained only for lawful purposes and not processed in any manner incompatible with those purposes. • be adequate, relevant and not excessive. • be accurate and current. • not be retained for longer than necessary. • be processed in accordance with the rights and freedoms of data subjects. • be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage. • not be transferred to a country or territory outside the European Economic Area unless that country or territory protects the rights and freedoms of the data subjects.
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.

Appendix B – Example risks

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Corporate risks

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Compliance risks

- Non-compliance with the DPA.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.