Guide to Audit Process

August 2014. Version 2.0
Office of the Data Protection Commissioner

Guide to Audit Process

PREFACE

This guidance was originally published in 2009. This revised version has been updated to take account of legislative developments and to reflect any changes in the approach of the Office of the Data Protection Commissioner to the audit process. The guidance is designed to assist organisations selected for audit by the Office of the Data Protection Commissioner. It is hoped that this resource will provide organisations holding personal data with a simple and clear basis to conduct a self-assessment of their compliance with their obligations under Irish Data Protection Law.[1]

1. INTRODUCTION

An audit is essentially an independent evaluation of how certain organisational resources or assets are managed in relation to a particular set of standards or model. Audits were traditionally associated with the accounting sector and an organisation's financial operations but have since broadened out in scope. Today, audits are conducted across public, private and voluntary sectors on a variety of fronts *e.g.* value for money (VFM) audits, environmental practices, health and safety audits and quality control assurance audits.

Audits have become a standard assessment tool deployed by regulatory authorities and standards bodies when monitoring external organisations under their remit.

Audits referred to as 'self-checks' are frequently conducted in-house by internal control units within organisations themselves or with the assistance of external expertise. A data protection audit operates as a control mechanism regardless of whether an organisation self-assesses or is appraised by an independent third party or regulatory body. Checks and appraisals are conducted in order to detect any irregularities or system weaknesses regarding how the organisation handles the personal data of its customers and employees. The identification of measures required to ensure the compliant use of all personal data aims to reduce the potential risks faced by organisations such as inappropriate use made of the data, data breaches, data theft or loss, unlawful disclosure to third parties or inappropriate employee access.

1.1 Compliance Audits:

Audits of the kind carried out by the Office of the Data Protection Commissioner in Ireland are compliance based.

The Office of the Data Protection Commissioner has been conducting compliance audits since 2003. A compliance audit typically examines an organisation's procedures, policies, systems and records in order to assess whether the organisation is generally in compliance with requirements under data protection legislation. An audit also entails a general assessment of the organisation's level of awareness regarding data protection requirements based on existing policies and practices within that organisation.

[1] Data Protection Acts 1988 & 2003 and the ePrivacy Regulations 2011 (S.I. 336 of 2011).

1.2 Audit Focus:

Compliance with Data Protection Legislation:

The principal purpose of a compliance audit conducted by the Office of the Data Protection Commissioner is to ascertain whether the audited organisation is operating in accordance with the Data Protection Acts (1988 & 2003) and the ePrivacy Regulations 2011 (S.I. 336 of 2011.

In addition, an audit will aim to identify any risks or possible contraventions of applicable legislation.

Compliance with Data Protection Standards

A compliance audit reviews how effective an organisation is in its adherence to policies concerning the handling of personal data. An assessment will be made whether the organisation is operating in accordance with its own documented data protection or privacy-related policies, sectoral codes of practice, guidelines and procedures.

Gaps & Weaknesses:

A compliance audit will identify existing and potential gaps and weaknesses.

Remedial Action:

Immediate remedial action may be prescribed by the Office of the Data Protection Commissioner in order to ensure that the requirements of the Data Protection Acts are fully observed.

Improvements:

An audit will identify improvements that may be needed to ensure that the requirements of the Data Protection Acts are fully observed at all times.

Best Practice:

Organisations audited are encouraged to achieve “best practice” as opposed to mere compliance with data protection legislation. Best practice recommendations are of an advisory nature.

Positive Findings:

An audit will identify strengths and areas where data protection practices in an organisation are to be commended.

1.3 Potential Benefits for Organisation

Guidance:

An audit should be seen as an aid to the organisation concerned in ensuring that its data processing operations are conducted in compliance with the provisions of the Act. An audit report is produced, conclusions and findings are outlined and recommendations issued based on an examination of all key systems processing personal data within the organisation.

All organisations audited are provided with an opportunity during the audit process to raise any questions or issues they may have in relation to data protection. However, substantive queries are required to be submitted in writing as they are passed onto the Compliance Unit in the Office of the Data Protection Commissioner.

Training Aid:

The Office of the Data Protection Commissioner is always mindful to advise organisations targeted for audit of the ultimate outcome of the audit: a written expert report which contains recommendations aimed at achieving improvements in data protection practices throughout the organisation. Audit reports can be used internally as a valuable training aid.

Planning Tool:

An audit provides a marker in time or a 'baseline' as to where an organisation currently is in terms of data protection policies and practice. Recommendations contained in the final audit report offer a template for change and improvement.

Awareness Raising:

A compliance audit aims to gauge the level of awareness of data protection generally within the organisation. An audit should raise awareness levels within the organisation of data protection, however strong or weak awareness was before hand. This is a positive side-effect, as organisations that demonstrate senior management commitment to data protection compliance have consistently been shown to have the best data protection compliance records.

In addition to the content of the final report, the preparation, the input during the audit and exposure to the approach and questions of the Audit Team, should all serve to increase organisational awareness of data protection. In this way, compliance audits reinforce the 'educational' as opposed to 'punitive' overall approach of the Office in that they are designed to help raise awareness of data protection in organisations generally and encourage revised higher standards in terms of policies and procedures.

Policy Work:

Equally, audits help broaden the Office of the Data Protection Commissioner's knowledge and understanding of data protection issues affecting organisations on the ground across a wide variety of sectors. Issues and findings arising from audits can directly influence the future agenda and policy work of the Office of the Data Protection Commissioner. New audit targets, policy areas requiring further investigation and the need for new or updated guidance on particular topics may all be identified on foot of audit outcomes.

2. AUDIT MODEL

2.1 European & Irish Law:

All EU Member States essentially work from the same data protection directives (95/46/EC and 2002/58/EC), but there are some small differences once transposed into national legislation, in how the Directives are implemented and applied in each member state. Member states adopt different approaches to audits or inspections based on powers afforded to them under domestic data protection legislation. Sanctions deployed by each data protection authority also vary in type and severity. Some key aspects of the approach of the Office of the Data Protection Commissioner (ODPC) in Ireland regarding audits and associated instruments are as follows:

- The ODPC has specific 'investigative powers", such as the power of authorised officers to access data and obtain information necessary to perform their duties. These powers may be exercised in a variety of ways within the ODPC: through a scheduled audit or an 'on the spot' inspection (utilising powers conferred under section 10 and 24 of the Data Protection Acts). Alternatively, information may be sought as part of the formal investigation of a complaint by issuing a formal legal notice (section 12 of the Data Protection Acts – Power to require Information).

- As a general rule, the ODPC may seek corrective measures such as rectification, blocking or deletion of data. Best practice recommendations of an advisory nature may be issued as part of an audit report. Unlike some of its European counterparts, the ODPC does not issue administrative fines. Other sanctions such as public statements and warnings or the publication of the principal findings of an audit in the annual report of the Commissioner may be used by the ODPC. The potential harm to an organisation's reputation can be a sufficient deterrent in many cases. In rare cases, where it is not possible to reach agreement with an organisation recently audited, the Data Protection Commissioner would consider a use of his legal enforcement powers to bring about a change in policy or practice. The Commissioner exercises this power under section 10 of the Data Protection Acts, 1988 and 2003, by providing a written notice, called an "enforcement notice", to the data controller or data processor. This notice may contain instructions regarding correcting the data, blocking the data from use for certain purposes, supplementing the data with a statement which the Commissioner approves, or erasing the data altogether. A person who receives an enforcement notice has the right to appeal it to the Circuit Court.

- An audit by the ODPC checks for compliance against data protection laws only. Compliance with other areas of national law is not assessed, although other regulations and legislation will be taken into account for example where there may be an issue or difference of legislative interpretation as to why an organisation may have adopted a particular policy or practice. The Office of the Data Protection Commissioner is aware there may be other legal obligations and regulatory spheres within which organisations must operate.

  The Data Protection Commissioner is of the view and repeatedly asserts

  > "If an entity is customer and employee-focused and fully compliant with the letter and spirit of their immediate regulator's codes or industry standards then it is unlikely to have much difficulty complying with Data Protection principles"

The Office of the Data Protection Commissioner is aware that some organisations and sectors in Ireland lack an explicit regulatory oversight body and may not have a set of standards or code of practice in operation. Compliance with specific legislation across a variety of areas is therefore the sole barometer by which organisations may deem themselves compliant.

2.2 Selection of Audit Targets:

Ultimately, the intention of the audit function regarding targets is to produce a broad mix between the public, private and voluntary sector representative of all entities holding personal data.

An audit target list is maintained, reviewed and updated on a regular basis within the audit unit in the Office of the Data Protection Commissioner. Entities are selected for a wide range of reasons, including:

- Complaints received by the Office regarding a particular entity.
- An organisation that is an acknowledged holder of substantial repositories of personal data.
- A multi-national organisation who has established its European headquarters in Ireland.
- Media reports featuring specific allegations in relation to a particular organisation or sector.
- A policy area which is the focus of the Office of the Data Protection Commissioner but requires further clarification, may lead to an organisation being selected for audit in order for officers to gain a better understanding of data handling practices within that organisation or sector.
- Organisations who procure products which rely upon a large amount of personal data such as time and attendance systems, marketing database software or credit referencing tools may be chosen in order to assess their implementation of such products.
- Organisations who conduct or commission research involving human data subjects.
- Data Protection Codes of Practice are generally codes developed jointly by the Office of the Data Protection Commissioner and bodies representing particular agencies or sectors[2]. An organisation deemed representative of a particular sector may be selected for audit to assist in the development of a code of practice for that sector or to assess compliance with the provisions of a code.
- As a follow-up to an audit of a company operating within a particular sector, a similar entity from within the same sector may be selected for comparison purposes.

- [2] Insurance Sector Code of Practice (2013)
- Revenue Commissioners Code of Practice (2012)
- Vocational Education Committees Code of Practice (2012)
- Department of Education and Skills Code of Practice (2011)
- Injuries Board Code of Practice (2008)
- Personal Injuries Assessment Board Data Protection Code of Practice (2007)
- An Garda Síochána Data Protection Code of Practice (2007).

- In terms of the sharing of information, particularly within the public sector environment, an audit of one agency authorised to access a central database or data-feed administered by another agency may lead to the other agency being audited also.

- A need may emerge to target a company from a particular region or area that hasn't been audited previously by the Office in order to ensure regional balance.

2.3 Audit Format

The period of notice outlining the intention to audit and the type of compliance audit carried out by the Office of the Data Protection Commissioner depends on the circumstances and reasons as to why the organisation is being audited.

The standard practice within the Office of the Data Protection Commissioner is to issue a written notice of 'intention to audit' several weeks in advance of the on-site audit to the data controller or processor (see 4.1 below). However, in situations where a complaint is under investigation, the Office may choose to give a few days notice only. Section 24 of the Data Protection Acts 1988 & 2003 also confers authorised officers with powers to visit the premises of a data controller or processor and conduct on-the-spot inspections. In these situations, no advance warning or written notice is required to be provided and often will not be so provided.

Scheduled Audits:

The majority of audits are scheduled and dates agreed in advance with the organisation.
The Audit Team makes contact with the selected entity and signals their intention to audit, proposing a date and seeking agreement from the notified entity regarding the suitability of the date proposed.

Where large-scale audits are planned, a series of meetings and exchange of information may take place in advance of a formal 'intention to audit' notice being issued. These interactions are designed to facilitate the Audit Team in scoping the audit and may entail the compilation and submission of documentation by the data controller or data.

'On the Spot':

As indicated above, in some instances, the Commissioner may decide to utilise powers conferred under section 24 of the Data Protection Acts and order an inspection team comprised of authorised officers to arrive unannounced at the premises of a particular data controller or data processor. In such cases, authorised officers will carry official photo identification and a signed letter from the Commissioner on logo-headed paper. Authorised officers are then required to inform the data controller or data processor of their intention to audit the organisation immediately under the aforementioned powers designated to them in the Data Protection Acts 1988 & 2003.

2.4 Authorised Officers

The Data Protection Commissioner has the power to appoint an "authorised officer" which is defined in Section 24 of the Data Protection Acts 1988 and 2003, as "a person authorised in writing by the Commissioner to exercise, for the purposes of this Act, the powers conferred by Section 24".

The appointment of authorised officers by the Commissioner is not confined to permanent staff members of the ODPC. It may also extend to the appointment of staff members from other data protection authorities who are seconded to assist on the audit in either an on-site capacity, or assigned off-site to conduct a remote piece of analysis or testing based on the nature and scope of the audit.

Authorised officers may also be appointed by the Commissioner as a result of the external outsourcing of third parties by the Office on a commercial basis. In such cases, these external third parties are awarded specific areas of work requiring specialist skills.

In all of the cases outlined, authorised officers retain possession of the full spectrum of powers accorded to them in Section 24 of the Acts (see section 3.1 below).

3. LEGAL BASIS FOR AUDITS/INSPECTIONS

3.1 Powers of Entry & Access to Information

Section 10(1A) of the Data Protection Acts 1988 & 2003 states that

> *(1A) The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of this Act and the Electronic Communications Networks and Services Regulations of 2003 and to identify any contravention thereof.*

Under the terms of Section 24 of the Data Protection Acts 1988 & 2003, all authorised officers have specific powers and associated rights of access.

> ***24(2)*** *An authorised officer may, for the purpose of obtaining any information that is necessary or expedient for the performance by the Commissioner of his functions, on production of the officer's authorisation, if so required-*
>
> *(a) at all reasonable times enter premises that he reasonably believes to be occupied by a data controller or a data processor, inspect the premises and any data therein (other than data consisting of information specified in section 12 (4)(b) of this Act) and inspect, examine, operate and test any data equipment therein,*
>
> *(b) require any person on the premises, being a data controller, a data processor or an employee or either of them, to disclose to the officer any such data and produce to him any data material (other than data material consisting of information so specified) that is in that person's power or control and to give to him such information as he may reasonably require in regard to such data and material,*
>
> *(c) either on the premises or elsewhere, inspect and copy or extract information from such data, or inspect and copy or take extracts from such material, and*
>
> *(d) require any person mentioned in paragraph (b) of this subsection to give to the officer such information as he may reasonably require in regard to the procedures employed for complying with the provisions of this Act, the sources from which such data are obtained, the purposes for which they are kept, the persons to whom they are disclosed and the data equipment in the premises.*
>
> *(6) A person who obstructs or impedes an authorised office in the exercise of a power, or, without reasonable excuse, does not comply with a requirement, under this section or who in purported compliance with such a requirement gives information to an authorised officer that he knows to be false or misleading in a material respect shall be guilty of an offence.*

3.2 Inter-DPA Co-operation

As per Article 28(6) of the 95/46/EC Directive[3], the Data Protection Commissioner may decide to share details regarding an investigation or an audit report with other data protection supervisory authorities.

> *6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.*
>
> *The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.*

Similar provisions exist in Convention 108 of the Council of Europe (Chapter IV)[4]:

The text in Convention 108 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' below specifically provides that the parties to the Convention (which covers all EU countries and beyond this all countries who have ratified the Convention) "agree to render each other mutual assistance in order to implement this convention" and proceeds to outline

> *2. For that purpose:*
> *a. each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;*
>
> *b. each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.*
>
> *3. An authority designated by a Party shall at the request of an authority designated by another Party:*
> *a. furnish information on its law and administrative practice in the field of data protection;*
> *b. take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.*

Section 15 of the Irish Data Protection Acts designates the Data Protection Commissioner for the purposes of mutual assistance under the Convention:

> *15.*
> *(1) The Commissioner is hereby designated for the purposes of Chapter IV (which relates to mutual assistance) of the Convention.*
> *(2) The Minister may make any regulations that he considers necessary or expedient for the purposes of enabling the said Chapter IV to have full effect.*

Outside of Europe, the ODPC has signed memoranda of understanding with the Federal Trade Commission in the United States[5] as well as with the data protection authorities of Canada[6] and Australia[7]. Memoranda of understanding (MOUs) support increased co-operation and communication between the ODPC and these authorities in their efforts to ensure better oversight of data protection and consumer rights. These memoranda are viewed by all signatories as frameworks for voluntary cooperation and they do not change existing law in any of the jurisdictions.

---

[3] http://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapters-3-to-7-Final-Provisions/94.htm
[4] http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm
[5] http://www.dataprotection.ie/documents/MOU/MOU.pdf
[6] https://www.dataprotection.ie/docimages/documents/MOU%20with%20Canada.pdf
[7] https://www.dataprotection.ie/docimages/documents/MOU%20with%20Australia.pdf

3.3 Confidentiality

In terms of the confidentiality of any information exchanged with other data protection supervisory authorities, Article 28(7) of the 95/46/EC Directive states

> *7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.*

In addition, all officers of the ODPC carry corresponding obligations of confidentiality in terms of personal data they view or copy as part of their investigations. Under the Second Schedule of the Data Protection Acts 1988 & 2003:

> *10 (1) A person who holds or held the office of Commissioner or who is or was a member of the staff of the Commissioner shall not disclose to a person other than the Commissioner or such a member any information that is obtained by him or her in his capacity as Commissioner or as such a member that could reasonably be regarded as confidential without the consent of the person to whom it relates.*
>
> *(2) A person who contravenes subparagraph (1) of this paragraph shall be guilty of an offence.*

4. PRE-AUDIT PROCEDURES:

4.1 Letter of Intention to Audit:

The letter of intention to audit provides a general outline as to the function or purpose of audits conducted by the Office, indicating that the inspection process of the audit will have a focus on areas and systems within the company where personal data is held and processed. If there are any areas or issues of particular concern in advance of the audit, these may also be highlighted in the letter. In some cases an indication will be given as to why the organisation has been selected for audit.

In the event of the audit of a large organisation, particular areas may also be singled out for inspection in the letter of intention or by way of a follow-up communication closer to the audit date. This practice helps ensure the Audit Team meet with the appropriate personnel on the day itself and facilitates the completion of the inspection within a specified timeframe.

A letter of intention to audit is issued to the organisation selected for inspection. The letter of intention to audit will specify a date for the inspection to take place and request that the data controller contact the Office of the Data Protection Commissioner to confirm whether the date is agreeable. Requests for an alternative date are considered and facilitated where possible but requests to reschedule which involve a significant deferral are only considered in exceptional circumstances.

4.2 Requested Documentation:

The letter of intention to audit will contain a request that the organisation forward to the inspection team in advance of the inspection

> "any documented data protection policies, governance and reporting procedures, codes of practice, guidelines, website privacy statements or privacy-related training materials"

The letter will also request

> "If your organisation has devised policies outlining data handling practices in terms of internal user management and access controls please forward any such documentation in advance of the inspection."

4.3 Pre-Audit Review by ODPC Officers:

The list below is intended to assist organisations selected for audit with their own preparation by signalling what checks may be undertaken in advance by the Audit Team.

- Search in-house Office of the Data Protection Commissioner databases (Complaints, Policy/Guidance & Registration) for any references to the organisation/sector being audited.
- Review case studies in annual reports.
- Review any previous audit reports focusing on organisations operating within the same sector.
- Review media articles, published reports, parliamentary references.
- Check with Registration Unit in the Office of the Data Protection Commissioner regarding any outstanding registration requirements/issues.
- Check the website of the organisation to be audited to ascertain whether personal data is being collected online.
- Check the website of the organisation to be audited for reference to Privacy or Data Protection policies.
- Check the website homepage of the organisation to be audited to ascertain if the consent of the user in terms of any cookies usage is sought and whether there is a means for the user to give or refuse consent.
- Review any documentation submitted by the organisation in advance of the audit as requested in the letter of intention to audit.
- Audit Team convene internally in advance of the audit to highlight possible areas of interest emerging from the pre-audit review.

5. Audit Methodology:

The methodology used by the Audit Team during the actual inspection is primarily a questionnaire-based approach. This is supplemented by visual inspections and examinations of selected uses of personal data within the organisation, including manual interrogation by the Team of databases containing personal information. A physical inspection of security procedures will also typically be conducted.

There may also be a substantive technical inspection element to the audit which entails the use of additional methodologies.

5.1 Questionnaire-based approach

The questionnaire-based approach focuses on the flow of personal data within and outside the organisation. Depending on the focus and duration of the audit, the majority of questions will be typically structured around any one or several of the 8 data protection principles.

- Fair obtaining and processing of personal data
- Ensuring data is kept for one or more specified, explicit and lawful purposes
- Disclosure / further processing / transfer of data to a Third Country
- Ensuring the data processed is accurate, complete and up-to-date
- Ensuring the data processed is adequate, relevant and not excessive
- Data Retention: ensuring personal data is kept for no longer than necessary
- Safety & Security of Data
- Access Requests

(see appendices 8.1 and 8.2 below for sample questions that may be of assistance to data controllers/data processors preparing for an audit or self-assessment exercise)

5.2 Audit Scope

The questionnaire-based approach centred on the 8 Data Protection principles is usually confined to a set number of areas chosen for discussion and inspection. In terms of larger organisations, the scope of the audit may be defined well in advance and limited to named functional areas *e.g.* the human resources unit of a large retailer or the Planning, Waste Management and Motor Tax Office divisions of a local authority. Areas or units selected for inspection may be selected based on their physical suitability or for reasons relating to the technical infrastructure in place e.g. a new in-house customer services system or a large physical filing area containing a high volume of original documentation supplied by prospective customers/employees.

The on-site inspection process seeks to concentrate on those areas of activity of an organisation which are considered likely by the Office of the Data Protection Commissioner to be indicative of the broader policies and practices in relation to data protection within the organisation.

The focus of the inspection team may switch to other areas depending on what issues emerge or practices they encounter on the day.

A ‘targeted’ compliance audit will focus on a particular issue(s) of concern that the Audit Team has been alerted to in advance, such as illegal leaks of information by employees to third parties. A targeted compliance audit may also select additional areas of focus such as physical and technical security or current data-sharing practices within and outside the organisation.

6. INSPECTION DAY[8]

6.1 Procedural Matters:

On the day of the inspection,

- Authorised officers will arrive at the premises of the data controller or data processor at the pre-appointed time (with the exception of 'on the spot' inspections).
- Authorised officers will present their official photo identification to the data controller/processor.
- If the audit is an unplanned inspection taking place without prior notice a signed letter from the Commissioner on headed paper with the office logo will also be produced by authorised officers.

6.2 Critical success factors

The most important element of an inspection from the perspective of the Audit Team is that access to key systems and data is provided by the organisation on the day and that questions posed on the day by the Audit Team are answered comprehensively and accurately.

Mutual Co-operation:

A successful audit is a two-way process – the organisation subject to the audit is expected to volunteer information freely and to assist the authorised officers wherever possible. There is a corresponding obligation on authorised officers to assist the organisation being audited at all times if there is a lack of clarity as to what information is being sought by the officers.

Access to in-house data and databases:

With respect to confidential personal data held on company databases or sensitive commercial documents, authorised officers are entitled to view and/or request copies of such data or documentation including third party contracts (as per designated powers conferred under section 24 of the Data Protection Acts 1988 & 2003). The ODPC will keep such requests to the minimum required.

Access to confidential documentation involving third parties:
All relevant policies and contractual agreements with third parties processing personal data on behalf of the organisation should be provided to the inspection team, where sought, in advance or on the day of the inspection in order to allow the Audit Team conduct as comprehensive an assessment as possible.

[8] The actual duration of an audit will vary depending on the extent and complexity of the use of personal data in an organisation.

7. AUDIT REPORT

7.1 Draft Audit Report:

At the close of the inspection, the Audit Team will indicate to the organisation that a draft report will issue within a given time frame (usually 6-8 weeks). The Audit Team will outline that the draft report may contain requests for further clarification and involve re-checking of facts and statements regarding certain operations or practices. The draft report will also provide the organisation audited with the opportunity to submit their own view of the areas and practices assessed. Generally, the draft report will issue with a response date deadline.

7.2 Final Report:

The final report will contain an introduction or overview of the organisation followed by an account of the units or areas visited by the Audit Team and a description of practices which normally will refer to relevant data protection principles such as 'fair processing'/'fair obtaining' or data retention.

The final section of the report will contain an overall conclusion, set of findings and a series of recommendations.

The Audit Team will aim to achieve agreement with the audited entity regarding the text of the final report, but this is not always possible. On receipt of the response to the draft report, the Audit Team will examine the response with a view to incorporating as much of the clarifications as appropriate. All factual inaccuracies will be amended by the Audit Team. Disagreement between the two parties may occur regarding recommendations. Ultimately, it is a matter for the Data Protection Commissioner to determine the content of his final report.

By its very nature and irrespective of its duration, an audit of an organisation processing a substantial volume of personal data cannot be deemed to be conclusive. An audit is a 'snapshot' of how an organisation processes personal data at a particular time within a specific environment which will undoubtedly change over the course of time. Final report findings and recommendations should always be viewed in this context. As previously stated, the Audit Team does not set out to examine each piece of personal data processed by the organisation, proceed through each of the eight data protection principles in minute detail or obtain a complete view of security within an organisation.

A final audit report is merely indicative of an organisation's level of compliance with the Data Protection Acts in a given number of areas. The final draft of an audit report agreed by both parties is not a definitive account of an organisation's data processing activities or an endorsement of that organisation's adherence to data protection policies.

7.3 Confidentiality of Audit Reports

In line with its overall approach to confidentiality, it is the Office's practice to treat audit reports as confidential documents. They are therefore not published, though the organisation concerned is free to do so. This possibility led to the decision by Facebook to publish the high profile Facebook audit report in 2011 and the follow-up review report in 2012.

Many organisations within the public sector are subject to Freedom of Information (FOI)[9] legislation and a complete copy of an audit report may be sought by interested parties using this mechanism.

[9] http://www.oic.gov.ie/en/About-Us/Legislation-FOI-Acts-Regulations/

Perhaps in anticipation of a substantial number of FOI requests but also to demonstrate a commitment to transparency, An Garda Síochána, the Institute of Technology, Carlow, the Revenue Commissioners and the Department of Social Protection have all taken the decision in recent years to publish in full the final reports of audits conducted by the Office of the Data Protection Commissioner[10]. The Commissioner welcomes this approach, which can also serve to reassure the customers/clients of an organisation that it is taking its data protection responsibilities seriously.

The Commissioner reserves the right however to comment on any aspect of a particular named audit in the annual report and has absolute privilege in this respect. Section 14 of the Data Protection Acts states

> **Annual Report**
> 14.—(1) The Commissioner shall in each year after the year in which the first Commissioner is appointed prepare a report in relation to his activities... in the preceding year and cause copies of the report to be laid before each House of the Oireachtas.
>
> (3) For the purposes of the law of defamation, a report under subsection (1) shall be absolutely privileged.

All organisations audited within a given year will be listed in the Commissioner's annual report for that same year.

The Commissioner may confirm the fact that an audit report has issued in the intervening period between an audit being conducted and the publication of the annual report. Detailed queries regarding the findings are generally referred to the organisation audited.

7.4 Audit Follow-up

Organisations audited by the Office of the Data Protection Commissioner can expect to be contacted by staff from the ODPC some time after the final report has issued, with a particular focus on establishing what actions have been taken by these organisations to implement the recommendations as set out in the final audit report.

Follow-up enquiries will usually be conducted in writing and will typically involve the provision of additional documentation or sample datasets to an authorised officer.

Audit follow-up procedures may necessitate a repeat inspection of the same organisation originally audited.

---

10 http://www.dataprotection.ie/docs/Audit-Reports/1293.htm

8. APPENDICES

8.1 Sample Illustrative Audit Questions

Note: The sample questions listed below are indicative only. Not all areas listed below will be covered in one single audit.

Fair Obtaining and Processing of Personal Data:
[Emphasis may differ depending on whether customers or employees merit particular focus].

Customers/Clients

Q. How do you obtain personal data?

Q What types of personal data do you obtain?

Q. Do you record the Personal Public Service Number - PPSN?

Q. Is verification documentation sought? If so, what happens to verification documentation? Is a copy made and retained for your records?

Q. What procedures are in place to ensure that a person's data is being recorded accurately?

Q. For how long is personal data retained both in computer and manual form?

Q. Do you record incoming or outgoing telephone calls? If so, how do you inform the customer that this is being done?

Q. Can we view the physical filing area and look at a random sample of files?

Employees:

Q. How do you obtain personal data?

Q What types of personal data do you obtain?

Q. Is verification documentation sought? If so, what happens to verification documentation?

Q. What do you do with approved and rejected application forms?

Q. Are all details received input on computer system?

Q. What procedures are in place to ensure that a person's data is being recorded accurately?

Q. For how long is personal data retained both in computer and manual form?

Q. Do you record incoming or outgoing telephone calls? If so, how do you inform staff this is being done?

Q. How long are personnel files held (computer and manual) after the staff member has left employment?

Q. Can we view the physical filing area and look at a random sample of files?

Sensitive Personal Data

Q. Do you process any sensitive personal data, e.g., medical data or data regarding nationality/ethnic origin?

Q. Under what circumstances do you obtain sensitive data?

Q. Who has access to sensitive data?

Q. What constitutes a business need to access medical data?

Q. Who controls what staff may gain access to the data?

Q. Is sensitive personal data transmitted internally / externally?

Q. How is the data transmitted? Encrypted e-mail? Secure fax?

Q. Is the Data Subject aware that his/her sensitive personal data is being processed in this way?

Q. For how long is sensitive personal data retained in both computer and manual form?

Service Application Forms

[may or may not be relevant depending on type of organisation]

Q. Do you conduct reviews of service application forms to ensure that the information sought is not excessive?

Q. Do you clearly explain on all service application forms why certain information is being sought?

Q. Do you ever use the information gathered on service application forms for other uses besides the original purpose for which the information is sought? Is the consent of the data subject sought to do so?

Third Party Requests for Disclosure

Q. Do you receive requests from third parties seeking data regarding your customers/employees?

Q. Is there a legislative basis cited by any of these third parties seeking information?

Q. Are there procedural guidelines to deal with requests for personal data from third parties?

Q. Do you document all requests handled and responded to?

Q. How do you handle law enforcement requests for disclosure of information?

Staff Training and Awareness

Q. Are there set down procedures / reference documents for staff for dealing with day to day Data Protection issues?

Q. Is there a Data Protection Committee or working group within the organisation?

Q. Is data protection a fixed/frequent or rare agenda item on meeting agendas at senior management level?

Q. How often is such training provided and is there ongoing refresher training?

Q. Are information security skills addressed in any of your organisation's training programmes?

Q. Are staff aware that unauthorised access to personal data of customers is not allowed?

Q. How do you check that no internal unauthorised access to personal data has been undertaken?

Q. Are staff leaving employment aware that any customer data remains subject to confidentiality?

Q. Is there something to this effect built into the contract of employment?

Q. Can we have a copy of a typical staff contract?

Marketing

[may or may not be relevant depending on type of organisation]

Q. Can you describe how a typical marketing campaign operates?

Q. What media do you use for marketing? [Online, mobile, Bluetooth, mailing, cold-calling]

Q. Do you outsource marketing activities? If so, is there a contract in place? Does the contracted entity handle personal data of your customers/clients? Does the contracted entity procure new customers for you?

Customers

Q. How can customers opt-out of such campaigns?

Q. How does a customer change his/her opt-out preference?

Prospective Customers

Q. Do you purchase any third party direct mail listings or commission tailored lists of prospective customers?

Q. If you engage in phone or e-mail marketing activities can you show us how a National Directory Database (NDD) check is undertaken?

Project Management Activities:

Q. Are all new projects and initiatives that entail processing of personal data 'privacy-proofed' at planning stage?

Q. Is a Privacy Impact Assessment conducted at development, testing and delivery stage i.e. pre and post-implementation?

Information & Knowledge Management Practices:

Q. Have you ever conducted an information and/or knowledge audit?

Q. Do you have a list or register of information assets for your organisation?

Q. If so, can you distinguish personal data repositories from non-personal data within your organisation?

Contracts with Data Processors

Q. Do you outsource any processing of personal data?

Q. How are customers made aware that their personal data may be outsourced to a third party?

Q. Do you have contracts in place with such data processors?

Q. Can we see a couple of sample contracts?

Q. In relation to transfers of data abroad, what type of data is involved?

Access Requests

Q. How do you handle Access Requests received under section 4 of DP Acts?

Q. What procedures are in place to amend inaccurate data when you are notified of same on foot of request received under section 6 of DP Acts?

Q. Are there procedures set out for handling such requests?

Q. How are staff made aware of these procedures and how is compliance with the procedures checked?

Computer Systems & Security[11]

Personal Computers of Employees

Q. Are passwords in use?

Q. How often are passwords changed?

Q. Who can change a password?

Q. Are there access level restrictions?

Q. Who assigns access levels?

Q Are documents sent externally by email encrypted or password protected?

Removable Media:

Q. Are ports such as CD & USB drives enabled? Are such drives capable of copying files?

Q. In relation to the use of laptops, under what circumstances is personal data held on them?

Q. Do laptops have remote access to company databases?

Q. Are laptops password protected etc.?

Q. Are laptops encrypted?

Q Do staff have secure remote access to data when they are offsite so that personal data does not need to be stored elsewhere?

[11] More extensive security related questions are contained in appendix 8.7 and 8.8

Network Security

Q. What type of back-up system operates?

Q. Is there a set daily/weekly procedure?

Q. Where are back-ups kept?

Q. Is this a secure location?

Q. Are all entry routes to server rooms / computer centre subject to security checks?

Q. Do existing measures relating to computerised data ensure that data may only be accessed by persons whose remit it is to access such data?

Q. Is there a log created of access to data? Footprints? Audit trails

Q. Are patterns of abnormal usage identifiable?

Q. What security measures are in place relating to facsimile transmissions?

Biometrics

Are there any plans for a biometric time and attendance system to be put in place and do you understand the data protection implications?

CCTV

Q. Is CCTV in operation?

Q. Do you have a policy with regard to the operation of CCTV?

Q. What is the retention period for CCTV footage?

Q. Are equipment and tapes/discs stored securely?

Q. Who has access to CCTV equipment?

Q. Is CCTV used for reasons other than security?

Q. Is there appropriate signage in relation to the uses made of CCTV?

Q. Are staff / customers aware of the purpose of CCTV?

8.2 Self-help Checklist on Data Protection Policy[12]

You should be able to answer YES to all of the questions below. If you can, your organisation is likely in good shape from a data protection viewpoint. If you don't have a clean sheet, the checklist can help you identify the areas where you need to improve.

MAIN RESPONSIBILITIES

Rule 1: Fair obtaining:

•At the time when we collect information about individuals, are they made aware of the uses for that information?

•Are people made aware of any disclosures of their data to third parties?

•Have we obtained people's consent for any secondary uses of their personal data, which might not be obvious to them?

•Can we describe our data-collection practices as open, transparent and up-front?

Rule 2: Purpose specification

•Are we clear about the purpose (or purposes) for which we keep personal information?

•Are the individuals on our database also clear about this purpose?

•If we are required to register with the Data Protection Commissioner, does our register entry include a proper, comprehensive statement of our purpose? *[Remember, if you are using personal data for a purpose not listed on your register entry, you may be committing an offence.]*

•Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each?

Rule 3: Use and disclosure of information

•Are there defined rules about the use and disclosure of information?

•Are all staff aware of these rules?

•Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them? Consider whether the consent of the individuals should be obtained for these uses and disclosures.

•If we are required to register with the Data Protection Commissioner, does our register entry include a full list of persons to whom we may need to disclose personal data? *[Remember, if you disclose personal data to someone not listed on your register entry, you may be committing an offence.]*

Rule 4: Security

•Is there a list of security provisions in place for each data set?

•Is someone responsible for the development and review of these provisions?

---

[12] http://www.dataprotection.ie/docs/Self_Assessment_Data_Protection_Checklist/22.htm

•Are these provisions appropriate to the sensitivity of the personal data we keep?

•Are our computers and our databases password-protected, and encrypted if appropriate?

•Are our computers, servers, and files securely locked away from unauthorised people?

Rule 5: Adequate, relevant and not excessive

•Do we collect all the information we need to serve our purpose effectively, and to deal with individuals in a fair and comprehensive manner?

•Have we checked to make sure that all the information we collect is relevant, and not excessive, for our specified purpose?

•If an individual asked us to justify every piece of information we hold about him or her, could we do so?

•Does a policy exist in this regard?

Rule 6: Accurate and up-to-date

•Do we check our data for accuracy?

•Do we know how much of our personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?

•Do we take steps to ensure our databases are kept up-to-date?

Rule 7: Retention time

•Is there a clear statement on how long items of information are to be retained?

•Are we clear about any legal requirements on us to retain data for a certain period?

•Do we regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?

•Do we have a policy on deleting personal data as soon as the purpose for which we obtained the data has been completed?

Rule 8: The Right of Access

•Is a named individual responsible for handling access requests?

•Are there clear procedures in place for dealing with such requests?

•Do these procedures guarantee compliance with the Act's requirements?

Registration

•Are we clear about whether or not we need to be registered with the Data Protection Commissioner?

•If registration is required, is the registration kept up to date? Does the registration accurately reflect our practices for handling personal data? *[Remember, if your data-handling practices are out of line with the details set out in your register entry, you may be committing an offence.]*

•Is a named individual responsible for meeting our registration requirements?

Training & Education

•Do we know about the levels of awareness of data protection in our organisation?

•Are staff aware of their data protection responsibilities - including the need for confidentiality?

•Is data protection included as part of the training programme for our staff?

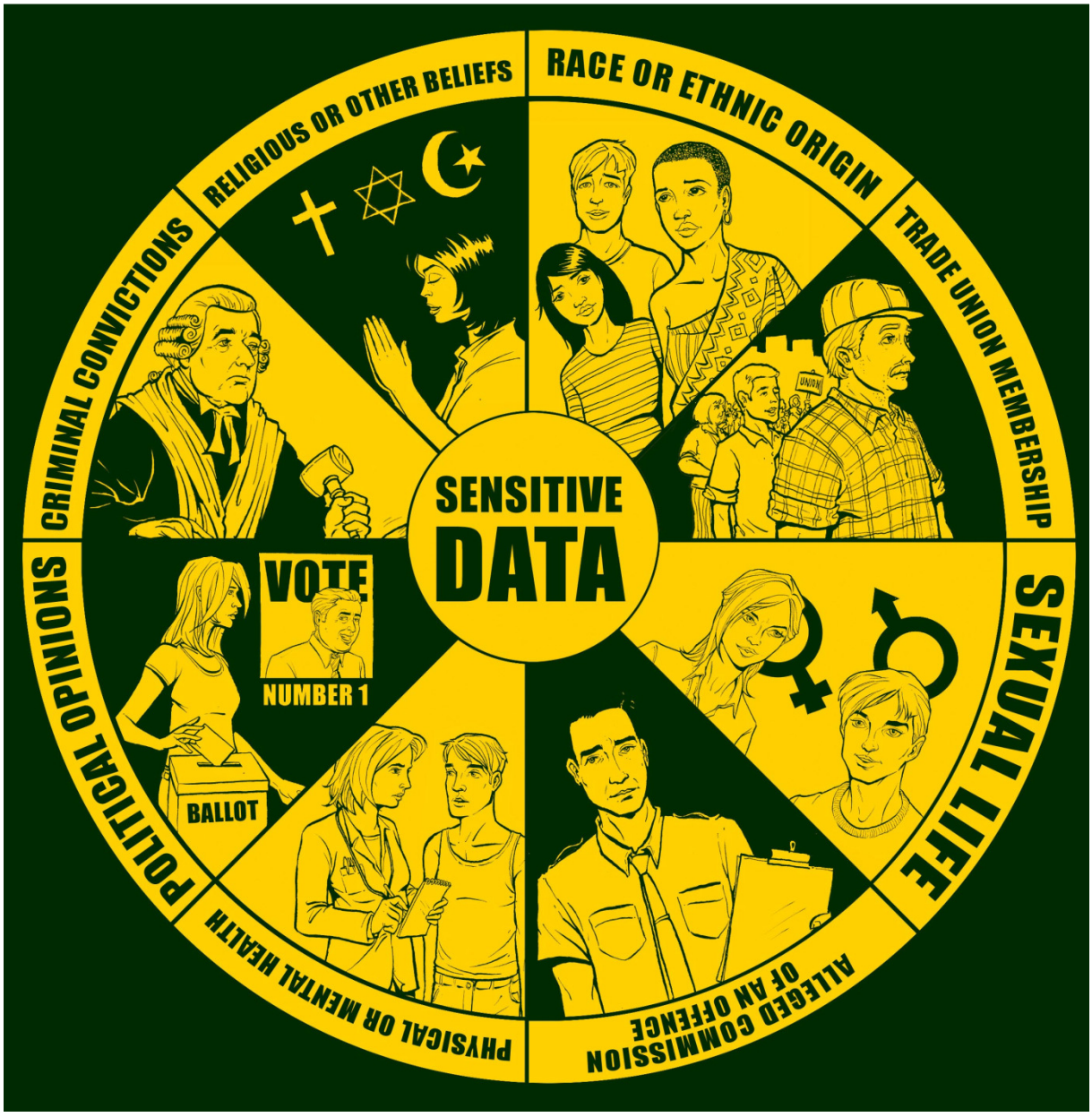
Co-ordination and Compliance

•Has a data protection co-ordinator and compliance person been appointed?

•Are all staff aware of his or her role?

•Are there mechanisms in place for formal review by the co-ordinator of data protection activities within our organisation?

8.3 Sensitive Data



The Data Protection Acts 1988 & 2003 place a particular focus on any sensitive data that may be processed by an organisation

“sensitive personal data” means personal data as to –

(a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject,
(b) whether the data subject is a member of a trade-union,
(c) the physical or mental health or condition or sexual life of the data subject,
(d) the commission or alleged commission of any offence by the data subject, or
(e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Section 1. Interpretation and application of Act - Data Protection Acts 1988 & 2003

8.4 Direct Marketing Guidance

If an audited entity requires clarification regarding direct marketing and the various different regulations according to the direct marketing channel utilised, the Audit Team may include the guidance below in the audit report itself.

	Mail-based Direct Marketing	**Text/Email Marketing #**	**Phone Marketing ✸**
Existing Customers#	An opt-out opportunity must be offered to the recipient of the marketing message.	An opt-out opportunity must be offered to the recipient of the marketing message at the time the details are collected and on the occasion of each message. Marketing can take place until such time as an opt-out is conveyed by the customer provided that contact has taken place within a 12 month period.	Must respect any preferences which the customer must have been given an opportunity to indicate regarding the receipt of marketing calls in advance of such calls. Marketing can then take place until such time as an opt-out is conveyed by the customer.
Individuals who request a quote for example	An opportunity to opt-out must be provided to the recipient of the marketing message.	An explicit opt-in to receive the marketing message is required from the individual.	Must respect any preferences conveyed by the customer regarding the receipt of marketing calls. Marketing can take place until such time as opt-out conveyed. An explicit opt-in is required if person is on the NDD.
Individuals with no relationship with company whatsoever	An opportunity to opt-out must be provided to the individual on the basis that their details were collected in line with the Data Protection Acts.	An explicit opt-in to receive the marketing message is required from the individual.	Must respect any preferences conveyed by the customer regarding the receipt of marketing calls. Marketing can take place until such time as an opt-out is conveyed. An explicit opt-in is required if person is on the NDD
Business Customer	Not covered by Data Protection unless a sole trader.	Marketing can take place until such time as opt-out conveyed by the recipient.	Marketing can take place until such time as an opt-out is conveyed. Must respect the NDD or any preferences conveyed by the customer.

8.5 Common Audit Recommendations[13]

Compliance

- A centralised function with responsibility for data protection matters should be identified within the organisation.

Staff Training and Awareness

- A formal training structure to draw attention to requirements under data protection legislation should be in place at induction stage for all employees. Further opportunities to develop knowledge of data protection and privacy issues should be offered at various stages throughout an employee's career.

Ensuring all personal data is fairly obtained and processed, purpose limitation.

- Under the Data Protection Acts 1988 and 2003, there must be clear and legitimate purposes for collecting personal data and customers have a right to know what those purposes are. The personal data sought and kept by data controllers should be sufficient to enable them to achieve their stated purposes and no more.

Ensuring all personal data processed is adequate, relevant and not excessive

- The Office of the Data Protection Commissioner requires that organisations have specific criteria in place to judge what is adequate, relevant and not excessive in terms of personal information held.

Marketing

- Consistency with regard to marketing opt-ins and opt-outs should be applied across all channels.

Security

- All significant data protection incidents of security breach should be reported to the Office of the Data Protection Commissioner immediately.

- A laptop security policy should be in place accompanied by an inventory listing the type of personal information held on each laptop. The laptop security policy should outline access controls in place including encryption.

- All disk and USB ports on all staff computers should be disabled, unless there is a clearly defined and compelling business reason that they should be accessible.

- A formal review of all access management and user provisioning based on the 'Need to Know' principle should be conducted. Appropriate audit trails to log access as well as amendments to personal data should be implemented on all relevant systems within the organisation. It is a requirement of data protection that access to personal information be in line with business need.

- It is recommended that appropriate measures be put in place to limit access to sensitive personal data to a strictly direct business need. It is also recommended that strong controls be put in place where sensitive personal data are being sent/received by email and fax.

[13] Note these recommendations are not relevant to all organisations. Their relevance is influenced by factors such as the size and scale of the organisation and whether sensitive data is processed.

- Where telephone conversations are being recorded, the customer should be made clearly aware of this practice at the outset of the call. The message at the beginning of the phone call should outline to the customer all of the reasons and uses to which the recording might be put.

Disclosures

- The organisation is ultimately responsible as the data controller for any personal data passed to third parties and care must be given to procedures and security at all times.

- All requests from external bodies and agencies not specifically provided for in legislation including An Garda Síochána, should be in writing.

- Only in exceptional circumstances should information be provided to law enforcement and regulatory bodies as a result of a phone call. Urgent requests such as these should always be followed by a written communication confirming it is for the investigation or detection of a crime or other relevant matter.

PPSN

- The Personal Public Services Number (PPSN) is today increasingly demanded by public agencies as a condition for providing a wide range of services. Section 2 (1) (c) of the Data Protection Acts 1988 & 2003 states inter alia that data "shall have been obtained only for one or more specified, explicit and legitimate purposes".

- Legislation regulating the use of the PPSN (principally, the Social Welfare Consolidation Act 2005) provides that the PPSN can be used either by the specified bodies named in the Social Welfare Acts or by any person or body authorised by these bodies to act on their behalf. It is the Commissioner's interpretation of the Acts that equally it should only be used by such bodies for particular transactions and where the transaction relates to a public function of a public body. The use of the PPSN for purposes not specified in Social Welfare legislation or for a purpose not referred to in the PPSN Register of Users (PPSN Register) maintained by DSFA could be deemed excessive and unwarranted under the Data Protection Acts 1988 and 2003.

Retention Policies

- Section 2(1)(c) of the Data Protection Acts 1998 and 2003 provides that a data controller shall not retain personal data longer than is necessary for the purpose or purposes it was obtained. Accordingly, it is recommended that organisation **X**

  (i) deletes any personal data that is no longer required for legitimate business purposes and

  (ii) implements, as soon as possible, a defined policy on retention periods for all items of personal data kept by the company.

- A records management policy should be devised that takes account of all the types of information held by various units within the organisation. The records management policy for the organisation

should contain a set of data retention periods including disposal and destruction schedules for non-archival records.

- Organisations have an obligation to be clear about the length of time for which personal data will be kept and the reasons why the information is being retained. In determining appropriate retention periods for personal information, data controllers must have due regard for any statutory obligations. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner. It is not justifiable to store the personal data of customers on the 'off-chance' that a use might be found for it at a future date.

Third Party Contracts

- It is recommended that where any data is being transmitted to a third party for processing, a contract should be put in place designating the third party as a data processor. The contract should also contain comprehensive data protection and confidentiality provisions. Organisations should satisfy themselves that all contracts currently in place contain adequate data protection and non-disclosure clauses.

Privacy Policy & Privacy Statements

It is important that the organisation distinguish a website 'Privacy Statement' from a 'Privacy Policy'.

- A Privacy Policy documents an organisation's application of the eight data protection principles to the manner in which it processes data organisation-wide. The policy applies to all personal data processed by the organisation, including customer data, third party data and employee data. A Privacy Policy can, in some instances, be a very complex document, having to apply the data protection principles to an organisation's own environment and practices. This Office recommends a Privacy Policy be drawn up by the organisation on foot of an Information Audit which will identify and categorise all personal information and sensitive data held by the organisation.

- A Privacy Statement is a public declaration of how the organisation applies the data protection principles to any personal data processed on its website. It is a more narrowly focused document and by its public nature should be both concise and clear.

  Organisations who collect personal information from their website are legally obliged to inform data subjects of the purpose and uses to which this information will be put. The Office of the Data Protection Commissioner recommends a 'Privacy Statement' be inserted as a key link on the organisations website home page if personal information is being collected from that website. The Office has issued a guidance document for the preparation of privacy statements[14].

Biometrics

- It is recommended that the organisation satisfies itself fully that it has complied with guidelines[15] issued by the Office of the Data Protection Commissioner prior to any planned procurement or implementation of a biometric time and attendance system.

[14] see Guidance on Privacy Statements
http://www.dataprotection.ie/docs/PrivStatements/290.htm

[15] http://www.dataprotection.ie/docs/Biometrics_in_the_workplace./244.htm and

CCTV

- It is recommended that a retention period of no longer than 28 days is employed in the use of CCTV.
- It is recommended that CCTV signage be erected immediately clearly stating the purpose for which the cameras have been erected. The default purpose can be deemed to be security but if the cameras are being deployed for any other purpose then the wording should encompass all purposes and uses. If staff monitoring is taking place, signage should reflect this.

8.6 "Need to know" access control policies.

Recommended Steps

- conduct an audit identifying the types of personal data held within your organisation, listing all information repositories holding personal data and their location;
- chart personal information data flows both within an organisation, and outside it, listing all third parties to which information is disclosed and assess these disclosures to ensure they are legitimate;
- examine access rights to personal data across the various different repositories identified in the information audit;
- break the organisation down into functional units, and assess whether access rights are appropriate, based on the needs of each unit. Within individual units, assess whether access rights could be limited in some cases;
- based on an analysis of personal data repositories and data flows, investigate with your IT team the possibility of installing filters, and creating tiered access to subsets of data;
- review logging and reporting functionality for all systems holding personal data;
- examine other system controls, for example, those that facilitate the copying and pasting of records into word processing applications or emails, and connections to printers. Also consider whether ports for USB memory sticks or disks are disabled, and if not, why not? Ask whether there are justifiable reasons as to why these ports should remain enabled.
- conduct regular reviews of access control and user provisioning policies, especially with regard to situations where a user's role and duties within the organisation changes.

---

http://www.dataprotection.ie/docs/Biometrics_in_Schools,_Colleges_and_other_Educational_Instit/409.htm

8.7 Internal Access Security Checklist

Access Control Policy			
		Findings	**Further Information required / to be provided**
1	Do you have a policy for deciding when an account is created / deleted?		
2	Has an access control policy been establish, documented & signed off based on business & security requirements?		
3	Does the policy take into account the removal of access rights?		

User Registration			**Is there a formal user registration & de-registration procedure for granting and revoking access to all information systems & services?**
		Findings	**Further Information required / to be provided**
4	Is there a user registration & removal procedure in place		
5	Are user ids unique		
6	Are users required to sign an AUP prior to having an account created?		
7	Are access roles used or defined?		
8	Is there a generic administrator account?		

Privilege management			**Is the allocation & use of privileges (AUP) restricted & controlled?**
		Findings	**Further Information Required / to be provided**
9	Is the allocation of privileges controlled in a formal manner		
10	Is there a record of the authorisation process and the privileges assigned		
11	Do the AUP cover keeping passwords secure?		
12	Is there a procedure to verify the identity of the user prior to resetting or sending a password to them.		

Review of user access rights			**Does management review users' access rights at regular intervals using a formal process**
		Findings	**Further Information Required / to be provided**
13	Does management conduct a review of access rights allocated a periodic intervals using a documented process		
14	Are user access rights re-allocated when they move groups within the organisation		

User Responsibilities			**Does the organisation prevent unauthorised user access and is this sufficient to prevent the compromise or theft of information**
		Findings	**Further Information Required / to be provided**
	Password use		
15	Are users advised to;		
	- Keep passwords secure / not share passwords		
	- Not write down their passwords on post-its and store them on the side of their pc on keyboard		
	- Select quality passwords of a minimum length (e.g. alpha-numeric passwords)		
16	Are users advised to / enforced;		
	- Change passwords regularly		
	- change temporary passwords at first log-on		
	User authentication for external connections		Are appropriate authentication methods in place to control access by remote users (e.g Citrix)
17	Are suitable controls in place to authenticate remote (external) users, e.g. VPN with or without tokens/fobs, certificates, dial back for RAS		

Password Management System			**Do password management systems provide an effective means of ensuring quality password?**
		Findings	**Further Information Required / to be provided**
18	Is the password management system configured in line with best practice? This would include:		
	- Enforcing the use of individual username / passwords		
	- Does it maintain a password history and prevent re-use of previous passwords		
	- Allow users to select / change their own passwords		
	- Does it enforce secure passwords, higher / lower case letters, numbers etc and greater than 8 characters		
	- force periodic changes, i.e. every 40 – 60 days		
	- Store and transmit passwords securely		
Monitoring			**Are logs of user activity kept?**
		Findings	**Further Information Required / to be provided**
19	Are Audit logs recording user activities, exceptions, and information security events produced and kept for an agreed period to assist in future investigations and access control monitoring		
20	Do procedures for monitoring use of information processing systems exist? Are the results of such monitoring activities reviewed regularly		

8.8 Technical Questionnaire

This questionnaire is intended to supplement security questions covered as part of a general audit. Typically, this questionnaire would be utilised if a more detailed investigation of security practices is required, such as when a significant data breach occurs.

Technical Questionnaire - Main Questions			
Are web services (WS*) communications secured?	Are production equipment, corporate laptops and mobiles all asset tracked (asset owner is tracked)?	Is communication between workstations and infrastructure encrypted? How?	How are engineering services communications encrypted?
Is email transmitted over Transport Layer Security (TLS) - is this optional or required?	Is there a policy of securing communications for services requiring credentials, sensitive data or that requires integrity?	Has PCI Data Security Standard compliance been achieved?	What security is in place for corporate data transfers?
Do internal tools use https or other encryption?	Is there a clear desk policy?	Is there a 'Bring Your Own Device' (BYOD) policy - how is it implemented, managed, reviewed?	Is there centralised management of all desktop systems?
Describe network management.	Do corporate networks have anti-virus installed?	What restrictions are there on the use of applications on networks?	
Describe wireless networks.	Is there a formal or informal process for managing vulnerabilities found during scanning?		
Describe access rights, control authorisation for employee and engineering tools.	Are access rights of employees reconciled on a periodic basis (what happens if existing accounts do not have corresponding	Is badge access required for all facilities?	Is there a documented employee exit process - gathering assets assigned to the employee?

	HR entries?)		
Describe cryptographic key management.			
How is communication equipment stored and access controlled?	Do data centres all have standard environmental controls?		
Does an Information Security policy exist?	Is it approved by senior management?	Is it reviewed on a regular basis and amended as required?	Is there a documented secure destruction policy?
Is there any Information Classification Policy in place that highlights what user account Information and personal data is classified as confidential?	Are information classifications reviewed on a regular basis? Are they formally audited?		
Are all employees subject to the Info Security/Info Classification/Secure Destruction Policies?	Details of any pre-employment checks performed on job candidates upon hire (except where not permitted by local law)?		
Is there a Security Team in place?	Are roles and responsibilities within the Security Team formally documented?	Is security awareness training performed for new employees in orientation?	

Is there is a chief Privacy Officer?	Are privacy considerations the responsibility of all engineers and security personnel or not? If so, how? If not, why not?		
Is there a documented third party audit process (is security a vendor selection criterion?)	Do contracts with third parties (data processors) contain security and privacy requirements?	Is third party compliance reassessed annually?	Are access rights of contractors audited?