BRITISH STANDARD
BS 10012:2009
Data protection – Specification for a personal information management system

BS 10012:2009

Data protection – Specification for a personal information management system

Publishing and copyright information
The BSI copyright notice displayed in this document indicates when the document was last issued.

ISBN 978 0 580 61550 4

ICS 01.140.30; 03.100.99; 35.020

The following BSI references relate to the work on this standard:
Committee reference IDT/1
Draft for comment 09/30175848 DC

Publication history
First published May 2009

Amendments issued since publication

Date	Text affected

Contents

Summary of pages
This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 24, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI and came into effect on 31 May 2009. It was prepared by Panel IDT/1/-/4, *Data protection*, under the authority of Technical Committee IDT/1, *Document management applications*. A list of organizations represented on this committee can be obtained on request to its secretary.

Information about this document

This British Standard has been produced to:

- form the basis of internal policies on data protection legislation and good practice compliance;
- facilitate the identification and drafting of internal procedures and processes;
- enable an organization to demonstrate compliance with data protection legislation and good practice to its clients;
- facilitate assessment of compliance with data protection legislation and good practice;
- provide a standardized benchmark for audits and process reviews.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Requirements are expressed in sentences in which the principal auxiliary verb is "shall".

Where optional recommendations are included, they are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

0 Introduction

0.1 Personal information management system

The objective of this British Standard is to enable organizations to put in place, as part of the overall information governance infrastructure, a personal information management system (PIMS) which provides a framework for maintaining and improving compliance with data protection legislation and good practice.

The key piece of legislation in this area is The Data Protection Act 1998 (DPA) [1]. This implements a European Directive (95/46/EC) [2] and applies to "personal data" which is defined in the DPA as information relating to identifiable living individuals. This British Standard uses the term "personal information" in place of the term "personal data".

The DPA is regulated and enforced by the Information Commissioner, who is responsible for promoting the protection of personal information. The Information Commissioner promotes good practice by the issue of guidance, rules on eligible complaints, provides information to individuals and organizations and takes appropriate action when the law is broken. The Information Commissioner has powers to investigate complaints, make assessments as to whether processing is compliant with the DPA, and issue information and enforcement notices.

0.2 Data protection principles

The DPA requires "data controllers" to comply with eight data protection principles, summarized as follows,[1)] which require personal information to be:

1st principle – fairly and lawfully processed;

2nd principle – obtained only for specified purposes and not further processed in a manner incompatible with those purposes;

3rd principle – adequate, relevant and not excessive;

4th principle – accurate and up-to-date;

5th principle – not kept for longer than is necessary;

6th principle – processed in line with the rights afforded to individuals under the legislation, including the right of subject access;

7th principle – kept secure;

8th principle – not transferred to countries outside the European Economic Area (EEA)[2)] without adequate protection.

---

1) The text given here is a summary of Schedule 1 of the Data Protection Act 1998 [1]. For the full text, see the DPA. The term "data controller" is also defined in the DPA, though this British Standard uses the term "organization" (see **2.1.5**).

2) The European Economic Area (at the time of publication of this British Standard) consists of the Member States of the European Union plus Norway, Iceland and Liechtenstein.

A number of exemptions from these data protection principles are permitted by the DPA. The majority of these exemptions fall into the following categories:

- exemptions from the non-disclosure principles;
- exemptions from the subject information provisions;
- exemptions relating to processing for historical and/or research purposes;
- miscellaneous exemptions, e.g. confidential references and exam scripts.

Reference should be made to the DPA, to guidance from the Information Commissioner and to other guidance and sector-specific advice for further details.

0.3 Notification

The DPA also requires organizations to notify the Information Commissioner of their processing to ensure openness, unless an exemption to notification is applicable.

1 Scope

This British Standard specifies requirements for a personal information management system (PIMS), which provides a framework for maintaining and improving compliance with data protection legislation and good practice.

NOTE The Standard applies the "Plan-Do-Check-Act" (PDCA) cycle. See Annex A.

This British Standard is for use by organizations of any size and sector. It is intended to be used by those responsible for initiating, implementing and maintaining a PIMS within an organization. It is intended to provide a common ground for the management of personal information, for providing confidence in its management, and for enabling an effective assessment of compliance with data protection legislation and good practice by both internal and external assessors.

2 Terms, definitions and abbreviations

2.1 Terms and definitions

For the purposes of this British Standard the following terms and definitions apply.

2.1.1 audit
systematic examination to determine whether activities and related results conform to planned arrangements and whether these arrangements are implemented effectively and are suitable for achieving the organization's policy and objectives

[BS EN ISO 9000:2005]

NOTE An audit may be conducted internally by, or on behalf of, the organization itself for management review and other internal purposes.

2.1.2 individual
person who is the subject of personal information

2.1.3 management system
system to establish policy and objectives and to achieve those objectives

[BS EN ISO 9000:2005]

2.1.4 nonconformity
non-fulfilment of a requirement

[BS EN ISO 9000:2005, **3.6.3**; BS EN ISO 14001:2004, **3.15**]

2.1.5 organization
legal entity that processes information

EXAMPLES
Natural persons, sole traders, companies, partnerships, bodies corporate, public sector bodies, voluntary associations and charities.

2.1.6 personal information
personal data relating to an identifiable living individual

NOTE The definition of "personal data" can be found in the DPA, section 1 (1), along with qualifiers related to the identification of the individual. The DPA definition was modified by the Freedom of Information Act 2000 [3], section 68(1). Sensitive personal data, a sub-category of personal data, is also defined in section 2 of the DPA;

*this definition forms the basis for the definition of "sensitive personal information" in **2.1.12**. The Information Commissioner's Office (the ICO) has issued guidance entitled "Determining what information is 'data' for the purposes of the DPA [4]" and "Determining what is personal data" [5] which is available from www.ico.gov.uk*

2.1.7 personal information management policy
statement of overall intentions and direction of the organization as formally approved by senior management for maintaining and improving compliance with data protection legislation and good practice

NOTE Hereafter referred to as "policy".

2.1.8 personal information management system (PIMS)
part of the overall management framework that establishes, implements, operates, monitors, reviews, maintains and improves the management of personal information

2.1.9 procedure
documented set of actions which is the official or accepted way of doing something

2.1.10 process
series of actions taken in order to achieve a result

2.1.11 processing
obtaining, recording or holding personal information or carrying out any operation or set of operations on personal information

NOTE This includes collecting, organizing, adapting, altering, disclosing, sharing, disseminating, aligning, combining, blocking, erasing and destroying personal information.

2.1.12 sensitive personal information
personal information relating to the individual's:

a) racial or ethnic origin;

b) political opinions;

c) religious or other beliefs;

d) membership of a trade union;

e) physical or mental health or condition;

f) sexual life;

g) commission or alleged commission of any offence, including any proceedings, the disposal of such proceedings or the sentence of any court in such proceedings for any offence committed or alleged to have been committed by the individual

2.1.13 system
set of interrelated or interacting elements

[BS EN ISO 9000:2005]

2.1.14 workers
people working under the control of the organization

NOTE This includes employees, temporary staff, contractors, volunteers and consultants.

2.2 Abbreviations

BCR	binding corporate rule
DPA	Data Protection Act 1998 [1]
EEA	European Economic Area
FSA	Financial Services Authority
ICO	Information Commissioner's Office
PDCA	Plan-Do-Check-Act
PIMS	personal information management system

3 Planning for a personal information management system (PIMS)

Objective: To plan for the implementation of a personal information management system that will provide direction and support for compliance with data protection legislation and good practice.

3.1 Establishing and managing the PIMS

The organization shall develop, implement, maintain and continually improve a documented PIMS in accordance with **3.2** to **3.7**.

3.2 Scope and objectives of the PIMS

The organization shall define the scope of the PIMS and set personal information management objectives, with due regard to the:

a) requirements for the management of personal information;

b) organizational objectives and obligations;

c) organization's acceptable level of risk;

d) applicable statutory, regulatory, contractual and/or professional duties; and

e) interests of individuals and other key stakeholders.

3.3 Personal information management policy

The organization shall ensure that a senior management team is tasked with issuing and maintaining a policy which sets a clear framework and demonstrates support for, and commitment to, managing compliance with data protection legislation and good practice.

NOTE Senior management might consist of the Board of Trustees/Directors, the Chief Executive and senior workers, the partners of the organization or the owner of a sole trader company.

The policy shall state that it covers either:

a) the whole organization; or

b) an identified part of the organization.

The policy shall be communicated to all workers.

3.4 Policy content

The policy shall state the organization's commitment to compliance with data protection legislation and good practice, including:

a) processing personal information only where this is strictly necessary for legitimate organizational purposes;

b) collecting only the minimum personal information required for these purposes and not processing excessive personal information;

c) providing clear information to individuals about how their personal information will be used and by whom;

d) only processing relevant and adequate personal information;

e) processing personal information fairly and lawfully (see **4.7**);

f) maintaining an inventory of the categories of personal information processed by the organization (see **4.2**);

g) keeping personal information accurate and, where necessary, up-to-date;

h) retaining personal information only for as long as is necessary for legal or regulatory reasons or for legitimate organizational purposes;

i) respecting individuals' rights in relation to their personal information, including their right of subject access;

j) keeping all personal information secure;

k) only transferring personal information outside the EEA in circumstances where it can be adequately protected;

l) the application of the various exemptions allowable by data protection legislation;

m) developing and implementing a PIMS to enable the policy to be implemented;

n) where appropriate, identifying internal and external stakeholders and the degree to which these stakeholders are involved in the governance of the organization's PIMS; and

o) the identification of workers with specific responsibility and accountability (see **3.5**) for the PIMS.

3.5 Responsibility and accountability

A member of the senior management team shall be accountable for the management of personal information within the organization such that compliance with data protection legislation and good practice can be demonstrated (see also **4.1.1**). This accountability shall include:

a) approval of the policy by the senior management team;

b) development and implementation of the PIMS as required by the policy; and

c) security and risk management in relation to compliance with the policy (see also **4.13.1**).

One or more suitably qualified or experienced workers shall be appointed to take responsibility for the organization's compliance with the policy on a day-to-day basis (see also **4.1.2**).[3)]

All workers shall be required to comply with the policy by the implementation of the organization's processes and procedures, with sanctions, appropriate worker development, or procedures put in place to respond to any nonconformities.

3.6 Provision of resources

The organization shall determine and provide the resources needed to establish, implement, operate and maintain the PIMS.

3.7 Embedding the PIMS in the organization's culture

To ensure that the management of personal information becomes a part of the organization's core values and effective management, the organization shall:

a) raise, enhance and maintain awareness of the PIMS through an ongoing education and awareness programme for all workers;

b) establish a process for evaluating the effectiveness of the PIMS awareness delivery;

c) communicate to all workers the importance of:

   1) meeting PIMS objectives;

   2) complying with the policy;

   3) continual improvement of the policy; and

d) ensure that all workers are aware of how they contribute to the achievement of the organization's PIMS objectives and the consequences of nonconformity.

4 Implementing and operating the PIMS

4.1 Key appointments

Objective: To ensure that the organization appoints the appropriate accountable and responsible workers as specified in the organization's policy.

4.1.1 Senior management

A member of the senior management team shall be designated as accountable for the management of personal information within the organization such that compliance with data protection legislation and good practice can be demonstrated.

[3)] The senior manager accountable (see **4.1.1**) and the worker(s) responsible for day-to-day compliance (see **4.1.2**) could be the same person.

4.1.2 Day-to-day responsibility for compliance with the policy

One or more suitably qualified or experienced workers shall be designated as responsible for compliance with the policy on a day-to-day basis. This responsibility can be designated on either a full-time or a part-time basis depending on the size of the organization and the nature of the processing of personal information.

The appointed worker(s) shall have the following responsibilities:

a) overall responsibility for compliance with the policy;

b) development and review of the policy;

c) ensuring implementation of the policy;

d) management reviews of the policy (see **5.2**);

e) training and ongoing awareness as required by the policy (see **4.3**);

f) approval of procedures where personal information is processed, such as:

   1) the management and communication of privacy notices (see **4.7.1**);

   2) the handling of requests from individuals (see **4.12.1**);

   3) the collection and handling of personal information (see **4.7.1**);

   4) complaints handling (see **4.12.2**);

   5) the management of security incidents (see **4.13.6**); and

   6) outsourcing and off-shoring (see **4.14**).

g) liaison with those responsible for risk management and security issues within the organization (see **4.13**);

h) provision of expert advice and guidance on DPA matters;

i) the interpretation and application of the various exemptions applicable to the processing of personal information (see **Introduction** and **4.8.1**);

j) provision of advice in relation to data sharing projects (including security issues when data are off site) (see **4.8.3**);

k) ensuring the organization has access to legislative updates and appropriate guidance related to data protection legislation (see **4.5**);

l) continuously checking that the PIMS reflects changes in legislation, practice and technology (see **4.5**);

m) completing, submitting and managing notifications to the Information Commissioner where required under the DPA (see **4.6**); and

n) implementing, as appropriate, the practices related to the processing of personal information outlined in any mandatory or advisory sectoral codes which apply to the organization.

4.1.3 Data protection representatives

Where the organization comprises multiple departments or systems which process personal information, the organization shall determine whether it would be appropriate to establish a network of data protection representatives which:

a) represent departments or systems which are recognized as high-risk in relation to the management of personal information (see **4.2.2** for examples of personal information in high-risk categories); and

b) assist the worker(s) with day-to-day responsibility for compliance with the policy.

4.2 Identifying and recording uses of personal information

Objective: To ensure that the organization understands the categories of the personal information that it processes and the level of risk related to the processing of that information.

4.2.1 General

An inventory of the categories of personal information processed by the organization shall be maintained. This inventory shall also document the purposes for which each category of personal information is used.

NOTE The inventory should support accurate notification of processing to the Information Commissioner's Office.

The organization shall document where the personal information flows throughout the organization's processes.

4.2.2 High-risk personal information

The inventory (see **4.2.1**) shall allow for the explicit identification and documentation of the high-risk categories of personal information processed by the organization.

High-risk categories of personal information can include:

a) sensitive personal information (as defined in Section 2 of the DPA);

b) personal bank account and other financial information;

c) national identifiers, such as national insurance numbers;

d) personal information relating to vulnerable adults and children;

e) detailed profiles of individuals;

f) sensitive negotiations which could adversely affect individuals.

NOTE The level of risk can increase where high volumes of personal information are processed.

4.3 Training and awareness

Objective: To ensure that all workers are aware of their responsibilities when processing personal information.

The organization shall ensure that the worker(s) with day-to-day responsibility for enabling the demonstration of compliance with data protection legislation and good practice (see **4.1.2**) is able to demonstrate competence in their understanding of data protection legislation and good practice and how this should be implemented within the

organization. The organization shall also ensure that this worker(s) remains informed about issues related to the management of personal information, where appropriate, by contact with external bodies.

The organization shall be able to demonstrate that all workers understand their responsibility to ensure that personal information is protected and processed in accordance with the applicable procedures, taking into account the related security requirements.

All workers shall be given training to enable them to process personal information in accordance with the applicable procedures. This training shall be relevant to the role which each worker performs within the organization.

4.4 Risk assessment

Objective: To ensure that the organization is aware of any risks associated with the processing of particular types of personal information.

The organization shall implement a process for assessing the level of risk to individuals associated with the processing of their personal information. Such assessments shall include processing undertaken by other organizations. The organization shall manage any risks which are identified by the risk assessment in order to reduce the likelihood of a nonconformity with the policy.

The risk assessment process shall include procedures whereby any processing of personal information that could cause damage and/or distress to the individuals can be escalated for review to those responsible and accountable (see **3.5**) for the management of personal information.

NOTE The organization's own risk assessment methodology may be used. Additionally, guidance on privacy impact assessments has been issued by the ICO (http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx).

4.5 Keeping PIMS up-to-date

Objective: To assess whether the PIMS continues to provide an infrastructure for maintaining and improving compliance with data protection legislation and good practice.

The worker(s) with day-to-day responsibility for compliance with the policy (see **4.1.2**) shall continuously assess whether the PIMS is and will continue to enable demonstration of compliance with the data protection legislation and good practice; making changes where necessary.

This assessment shall include the review of the PIMS where changes in the organization's requirements and/or technology occur.

4.6 Notification

Objective: To ensure that the organization notifies details of its processing of personal information to the Information Commissioner as required by the DPA.

The PIMS shall incorporate procedures to trigger the notification procedure (unless the organization is exempt from the requirement to notify under the DPA) and to ensure that such notifications are kept accurate and up-to-date.

4.7 Fair and lawful processing

Objective: To ensure that personal information is processed fairly and lawfully and that the legal grounds for processing of personal information have been clearly identified before processing commences.

4.7.1 Collection and processing of personal information

The PIMS shall incorporate procedures which ensure that:

a) the organization processes personal information fairly and lawfully;

b) the organization processes personal information only where this is justified, in accordance with Schedule 2 of the DPA;

c) the organization processes sensitive personal information only where this is necessary for the organization's purposes and is justified in accordance with Schedules 2 and 3 of the DPA;

d) any individual supplying personal information to the organization is provided with a "privacy notice" or online privacy statement, either presented in full or as an extract along with a link or reference to the full notice, which clearly communicates the following information:

   1) the identity of the organization;

   2) the purposes for which personal information will be processed;

   3) information about the disclosure of personal information to third parties;

   4) information about an individual's right of access to personal information;

   5) whether personal information is transferred outside the EEA to countries without adequate protection;

   6) details of how to contact the organization with queries related to the processing of personal information;

   7) details of any technologies, such as cookies, used on a website to collect personal information about the individuals;

   8) any other information that would make the processing fair.

Where the personal information is collected for marketing purposes or might be used in the future for marketing purposes, the PIMS shall incorporate procedures that ensure that the means by which an individual can object to such marketing is clearly explained to that individual.

The PIMS shall incorporate procedures that indicate, where processing has been based upon consent and the consent is withdrawn, that consent has been withdrawn and that processing based on that consent will cease.

Where other sectoral requirements or legislation require explicit consent for marketing, the PIMS shall contain procedures for collecting this consent.

Where sensitive personal information is being collected for a particular purpose(s), the PIMS shall incorporate procedures which ensure that the privacy notice explicitly states the purpose(s) for which sensitive personal information is or might be used.

The PIMS shall incorporate procedures which ensure that new collection methods are reviewed and signed off by an appropriately qualified or experienced worker (see **4.1.2**) to ensure that such methods can be demonstrated as compliant with data protection legislation and good practice.

4.7.2 Record of privacy notices and statements

The PIMS shall incorporate procedures for maintaining records of privacy notices and online privacy statements. These records shall be retained for at least as long as the personal information to which they relate is retained.

4.7.3 Timing of privacy notices and statements

The PIMS shall incorporate procedures which ensure that, where the organization collects personal information directly from an individual, any privacy notice or online privacy statement required to be given to the individual is provided or made available to the individual prior to any personal information being collected.

4.7.4 Accessibility of privacy notices and statements

The PIMS shall incorporate procedures which ensure that the content of any privacy notice or online privacy statement is presented in a way which allows it to be easily understood by, and accessible to, its intended audience.

NOTE Privacy notices intended to be used with the collection of personal information from vulnerable adults, people with learning difficulties or children need to be presented in a language and format which are readily understandable and are accessible to them.

4.7.5 Third parties

The PIMS shall incorporate procedures which ensure that personal information is collected from third parties fairly and lawfully.

The PIMS shall incorporate procedures which ensure that, where necessary, the individual is provided with a privacy notice and, where appropriate, an online privacy statement (see **4.7.1**), unless doing so would involve disproportionate effort.

NOTE "Disproportionate effort" in this context does not merely mean "considerable effort", as the organization could be required to go to considerable lengths to provide privacy notices and, where necessary, online privacy statements where the processing is likely to have a prejudicial effect on the individual.

4.8 Processing personal information for specified purposes

Objective: To ensure that personal information is obtained only for one or more specified purposes, and is not further processed in any manner incompatible with that purpose or those purposes.

4.8.1 Grounds for processing

The PIMS shall incorporate procedures which ensure that processing of personal information is not carried out in a way which breaches or potentially breaches any legal obligations, including statutory provisions, common law or contractual terms.

The PIMS shall incorporate procedures which ensure that personal information collected for specified purposes is not used for another incompatible purpose, unless:

a) a relevant exemption from the legislation applies; or

b) the individuals whose personal information is to be processed for the new purpose have consented to the processing for this new purpose.

The PIMS shall incorporate procedures which ensure that, where sensitive personal information is to be used for an incompatible new purpose, the individual's explicit consent is obtained for this prior to processing, unless a relevant exemption applies.

4.8.2 Consent to new purposes

The PIMS shall incorporate procedures which ensure that any consent for new purposes is freely given and informed.

The PIMS shall incorporate procedures which ensure that:

a) positive indications of an individual's consent to the use of their personal information for a new purpose is obtained; and

b) records of the consent obtained for a new purpose are maintained.

4.8.3 Data sharing

The PIMS shall incorporate procedures which ensure that, where the organization shares personal information with another organization, the responsibilities of both parties with regard to the personal information are formally documented in a written agreement or contract as appropriate.

The PIMS shall incorporate procedures which ensure that, where the other organization will be using the personal information for its own purposes:

a) the written agreement or contract describes both the purposes for which the information may be used and any limitations or restriction on the further use of the personal information for other purposes; and

b) the other organization provides an undertaking or other evidence of its commitment to processing the information in a manner which will not contravene the DPA.

The PIMS shall incorporate procedures which ensure that, wherever possible, any new processing which involves the sharing of personal information with third parties is compatible with the organization's notification (see **4.6**) and with the terms of the privacy notice or online privacy statement [see **4.7.1**d)] provided to the individual.

Where this is not possible, the organization shall ensure that it has:

1) a legal basis for the data sharing; and

2) if required, the individual's consent to the data sharing.

Where data sharing with third parties is allowed without the consent of the individual, the PIMS shall incorporate procedures which ensure that an auditable record of the protocols and controls for this data sharing is documented.

Where data sharing with a third party is required, for example, by law, the PIMS shall incorporate procedures which ensure that the protocols and controls for the data sharing are documented.

4.8.4 Data matching

Where personal information is matched with other personal information to create, for example, an enhanced profile of an identifiable individual, the PIMS shall incorporate procedures which ensure that the matched personal information is only used for notified and compatible purposes, as required by law or where consent has been obtained.

4.9 Adequate, relevant and not excessive

Objective: To ensure that personal information is adequate, relevant and not excessive.

4.9.1 Adequacy

The PIMS shall incorporate procedures which ensure that the personal information collected by the organization is adequate for the organization's purposes.

The PIMS shall incorporate procedures for regular reviews of technology and processes involving the processing of personal information, which ensure that the information continues to be adequate for those purposes.

4.9.2 Relevant and not excessive

The PIMS shall incorporate procedures which ensure that:

a) the organization processes the minimum amount of personal information required to meet its legitimate purposes;

b) additional personal information which is not relevant or is excessive for the stated purposes is not processed, unless provision of this information is optional and only processed with the consent of the individual;

c) new systems and processes involving the processing of personal information are reviewed in order to ensure that the information being processed is relevant and not excessive.

Where it is not relevant or necessary to process personal information for the organization's purposes, the PIMS shall ensure that the personal information is not processed.

4.10 Accuracy

Objective: To ensure that personal information is accurate and, where necessary, kept up-to-date.

The PIMS shall incorporate procedures which ensure the maintenance of the integrity and accuracy of personal information being processed.

The PIMS shall incorporate procedures to allow individuals to challenge the accuracy of their personal information and to have it corrected where necessary. Where personal information is inaccurate and unable to be corrected, for example in relation to a historical record, the PIMS shall incorporate procedures for noting the reported inaccuracy and, where appropriate, the accurate personal information.

The PIMS shall incorporate procedures which check whether alleged inaccuracies are truly inaccurate.

The PIMS shall incorporate procedures which ensure that workers are informed of the importance of recording personal information accurately and of using only up-to-date personal information to make important decisions about individuals.

The PIMS shall incorporate procedures for:

a) informing any third party to whom the organization has passed inaccurate or out-of-date personal information that the information is inaccurate and/or out-of-date and is not to be used to inform decisions about the individuals concerned; and

b) passing any correction to the personal information to the third party where this is required.

The PIMS shall incorporate procedures for the review of new systems and processes involving the processing of personal information in order to:

1) confirm that these systems or processes prevent as far as possible the recording of inaccurate or out-of-date personal information, and

2) allow corrections to be made to inaccurate or out-of-date personal information.

4.11 Retention and disposal

Objective: To ensure that personal information is not kept for longer than is necessary.

The PIMS shall reference retention schedules for personal information which shall:

a) include any minimum retention periods required by law, as well as by the organization;

b) make clear the justification and basis for the retention periods; and

c) document any applicable justification for retaining personal information for a longer period than the stated minimum retention period, e.g. where it might be retained for historical and/or research purposes.

The PIMS shall incorporate procedures for the implementation of the retention schedules and the communication of the schedules to all relevant workers.

The PIMS shall incorporate procedures which ensure that personal information no longer required by the organization is disposed of.

The PIMS shall incorporate or reference disposal procedures which are managed:

1) using approved processes;

2) with a level of security appropriate to the sensitivity of the personal information; and

3) in line with the organization's information security risk assessment.

NOTE In some instances, it might be appropriate to dispose of the personal information by transferring it for permanent preservation to an archiving facility.

4.12 Individuals' rights

Objective: To ensure that procedures are in place to enable the rights of individuals to be respected.

4.12.1 Rights of individuals

The PIMS shall include procedures which ensure that individuals' rights in relation to their personal information are respected and that requests to exercise such rights are dealt with within any statutory time limits.

NOTE Such rights include access to information, objection to processing, and review of automated processing.

4.12.2 Complaints and appeals

The PIMS shall incorporate a complaints procedure which ensures that complaints about the processing of personal information are handled correctly. This shall include procedures for considering appeals by individuals about the way their complaints have been handled.

4.13 Security issues

Objective: To ensure that personal information is protected against loss or damage and unauthorized or unlawful processing by the implementation of appropriate technical and organizational security measures.

4.13.1 Security controls

The PIMS shall specify security controls as appropriate:

a) to the type of personal information being processed; and

b) to the risk of damage or distress to the individuals if the information is compromised (see **4.4**).

*NOTE 1 The risk assessment (**4.4**) will establish an appropriate level of control. Over-specifying security requirements can be as damaging as under-specifying.*

Where high-risk personal information (see **4.2.2**) is processed, the PIMS shall ensure that the security measures specified and implemented are appropriate to the assessed risks, and that they remain so.

NOTE 2 Where appropriate, the organization may wish to consider compliance with BS ISO/IEC 27001. Certification to BS ISO/IEC 27001 by an external body in order to demonstrate compliance is also a possibility.

4.13.2 Storage and handling

The PIMS shall incorporate procedures which ensure that personal information is stored and handled securely, with precautions appropriate to its confidentiality and sensitivity.

NOTE Particular attention should be paid to storage of personal information on media and portable devices, such as backup tapes, removable USB drives, removable hard drives, laptops and hand-held devices.

4.13.3 Transmission

The PIMS shall incorporate procedures which ensure that, where personal information is transferred electronically or manually within the organization or to other organizations, this transmission is secured by appropriate means defined by the organization in order to safeguard the information during transfer.

4.13.4 Access controls

The PIMS shall incorporate procedures which ensure that, where access by workers to personal information is allowed, this access is restricted to those workers who require such access as part of their role.

The PIMS shall incorporate procedures which ensure that it is made clear to workers that, where access is legitimately granted, this is for work purposes only and information should only be accessed for legitimate purposes.

Where high-risk personal information is processed (see **4.2.2**), the PIMS shall incorporate procedures which ensure that access controls reflect the sensitivity of this information.

The PIMS shall incorporate procedures which ensure that all accesses to personal information are monitored and assessed in line with the organization's information security risk assessment.

4.13.5 Security assessments

The PIMS shall incorporate procedures which ensure that security assessments are routinely undertaken.

These assessments shall establish whether existing security controls are adequate and make recommendations for improvements where necessary.

These assessments shall take into account the risk of harm, damage and/or distress to individuals in the event of a security incident.

4.13.6 Managing security incidents

The PIMS shall incorporate procedures:

a) which assess and manage security incidents involving personal information, including procedures to mitigate the damage caused by any security incident;

b) for documenting each security incident, including an assessment of how the incident occurred, what corrective action was taken, and what can be learned from the incident;

c) for making decisions as to whether or not a security incident is referred to a relevant regulator [for example, the Information Commissioner or the Financial Services Authority (FSA)] or notified to the individuals; and

d) for keeping records of any such referrals and notifications issued.

4.14 Transfer of personal information outside the EEA

Objective: To ensure an adequate level of protection where personal information is transferred or processed outside the EEA.

Where the organization transfers personal information outside the EEA, the PIMS shall incorporate procedures for ensuring that the rights of the individuals are protected, for example:

a) by including within contracts conditions which ensure the protection of the information and the processing, e.g. using model contracts, and/or putting in place an internal binding corporate rule (BCR);

b) in the case of a transfer to the United States, by establishing whether the organization to which the personal information is to be transferred has certified its compliance with the US Federal Trade Commission as being compliant with the Safe Harbor principles;

c) by establishing whether the country or territory has been assessed by the European Commission as providing adequate protection; and

d) where the processing is to be performed by another organization, by carrying out due diligence on that other organization.

The PIMS shall incorporate procedures for ensuring that the worker(s) responsible and accountable for compliance with data protection legislation and good practice (see **4.1.2**) reviews all new initiatives

involving the transfer of personal information outside the EEA. This review shall establish whether adequate protection can be provided for such transfers.

The PIMS shall incorporate procedures for ensuring that subcontractors based outside the EEA who process personal information on behalf of the organization operate model contracts as required by the European Commission for ensuring adequate protection for personal information, unless other adequate procedures have been agreed to protect the personal information.

4.15 Disclosure to third parties

Objective: To ensure that disclosures to third parties are managed in compliance with data protection legislation and good practice.

The PIMS shall incorporate procedures which ensure that third parties provide evidence of:

a) their right to access the personal information; and

b) where necessary, their identity.

The PIMS shall incorporate procedures which ensure that a check is made to ensure that there are legal grounds for disclosing any information to a third party. Only the minimum amount of personal information necessary shall be disclosed to third parties.

The PIMS shall incorporate procedures for the maintenance of records of disclosures of personal information. These records shall demonstrate that disclosure was lawful and shall enable the organization to keep track of where personal information has been disclosed.

NOTE Where access to personal information by third parties is granted under legislation such as the Freedom of Information Act 2000 [3], verification of identity and minimization of the information disclosed might not be necessary.

4.16 Sub-contracted processing

Objective: To ensure that personal information processed by another organization on behalf of the organization is managed in compliance with data protection legislation and good practice.

The PIMS shall incorporate procedures which ensure that, where information is processed on its behalf by another organization(s):

a) the organization selects only other organizations that can provide technical, physical and organization security which meet the requirements of the organization for all the personal information they process on its behalf;

b) an assessment of appropriate security is undertaken as part of due diligence before another organization is engaged and, if deemed necessary because of the nature of the personal information to be processed or because of the particular circumstances of the processing, an audit of the other organization's security arrangements is conducted before entering into the contract;

c) once the other organization has been selected, the organization puts in place a written agreement to provide the service as specified and requiring the other organization to provide appropriate security for the personal information which it will process;

d) the contract with the other organization enables regular audits of the other organization's security arrangements during the period in which the other organization has access to the personal information;

e) the other organization is under a contractual obligation to obtain the organization's permission to use further subcontractors to process the personal information;

f) contracts with subcontractors of the other organization require the subcontractors to comply with at least the same security and other provisions as the other organization; and

g) contracts with the other organization(s) (which are flowed down to any subcontractors) specify that, when the contract is terminated, related personal information will either be destroyed or passed to the organization or to another organization as specified by the organization.

4.17 Maintenance

The PIMS shall incorporate procedures which ensure that procedures and technology components are maintained to ensure their correct and appropriate functioning. These procedures shall ensure that such maintenance is planned and performed on a regular, scheduled basis.

5 Monitoring and reviewing the PIMS

Objective: To ensure that the effectiveness and efficiency of the PIMS is monitored and reviewed.

5.1 Internal audit

5.1.1 Audit planning

An audit programme which monitors and reviews the effectiveness and efficiency of the processing of personal information by the organization shall be planned, established and maintained, taking into account the policy.

The audit programme shall explicitly include any processing of high-risk personal information (see **4.2.2**) and shall include any processing of personal information by other organizations (see **4.16**).

5.1.2 Selection of auditors

The objectivity and the impartiality of the audit program shall be ensured by the appropriate selection of auditors and the conduct of audits.

*NOTE Regular audits by external parties should be considered by larger organizations and those processing high-risk personal information (see **4.2.2**).*

5.1.3 Audit requirements

Audits shall be conducted at planned intervals to determine whether the PIMS:

a) is operating in accordance with the policy and established procedures; and

b) has been implemented and maintained in accordance with technology requirements.

Audit reports detailing any significant departure from the policy and/or established procedures shall be provided to management.

Audit reports shall also identify issues related to technology or processes which could affect compliance with the policy.

5.2 Management review

A management review of the PIMS shall be carried out at regular, scheduled intervals, and when major changes take place, to ensure the system's continuing suitability, adequacy and effectiveness.

The management review shall be based on:

a) feedback from users of the PIMS;

b) risks identified and escalated by workers;

c) results of audits;

d) records of procedural reviews;

e) results of technology upgrades and/or replacements;

f) formal requests for assessment by regulatory bodies;

g) complaints handling; and

h) breaches/security incidents that have occurred.

The management review shall provide detailed information regarding potential changes to the PIMS by, for example, identifying modifications to policy, procedures and/or technology that might affect compliance.

Where major changes in the PIMS are implemented, an audit shall be completed as soon as possible after implementation.

6 Improving the PIMS

Objective: To improve the effectiveness and efficiency of the PIMS by the implementation of corrective actions.

6.1 Preventive and corrective actions

6.1.1 General

The organization shall improve the PIMS through the application of preventive and corrective actions.

All proposed changes and/or improvements shall be assessed prior to implementation to ensure that the requirements of the policy are met.

Changes that could affect the ability to demonstrate compliance with data protection legislation and good practice (such as the conversion of personal information to a new storage file format) shall be reviewed to determine whether they affect compliance.

Changes arising from preventive and corrective actions shall be documented and retained in accordance with the retention schedule.

6.1.2 Preventive actions

The organization shall take action to guard against potential nonconformities in order to prevent their occurrence. A procedure shall be established for:

a) identifying potential nonconformities and their causes;

b) determining and implementing preventive action needed;

c) recording results of, and reviewing, action taken;

d) identifying changed risks; and

e) ensuring that all those who need to know are informed of the potential nonconformity and the preventive action put in place.

6.1.3 Corrective actions

Where a nonconformity is identified, a procedure shall be established for reviewing each nonconformity and, based on a risk assessment, either:

a) eliminating the cause of the nonconformity;

b) reducing the level of nonconformity; or

c) where the risk assessment determines that a reduction in the level of nonconformity is not warranted, documenting this position in detail.

The risk assessment shall be conducted at regular intervals to determine whether the position has changed and the nonconformity needs to be rectified (see **4.4**).

The organization shall ensure that all newly identified risks to personal information (either from within the organization or in the wider national perspective) are assessed using proactive procedures such as privacy impact assessments.

6.2 Continual improvement

The organization shall continually improve the effectiveness of the PIMS through the audit results, preventive and corrective actions, and management review.

Complaints, security incidents, subject access requests and other issues shall be used as an aid to improving the effectiveness of the PIMS.

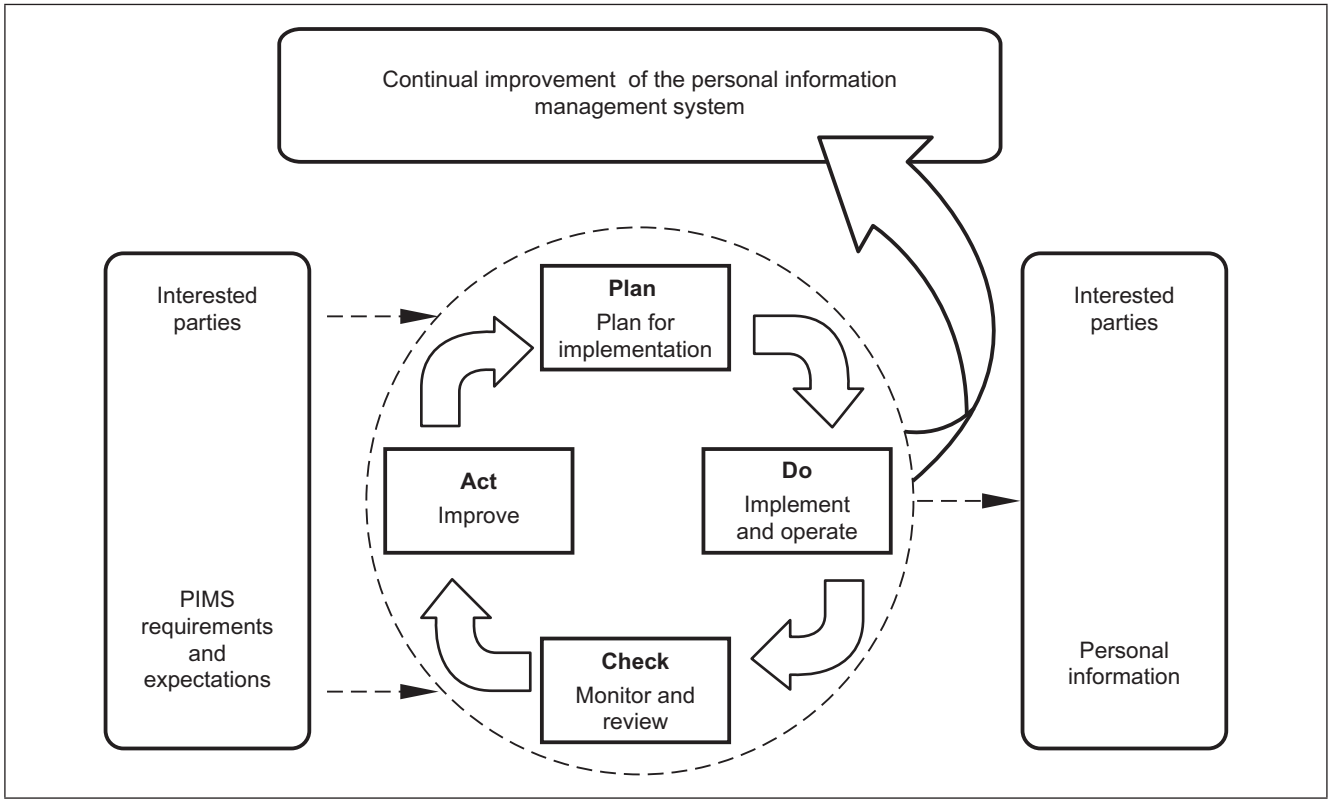
Annex A (informative) The Plan-Do-Check-Act (PDCA) cycle

This British Standard applies the "Plan-Do-Check-Act" (PDCA) cycle to establishing, implementing, operating, monitoring, exercising, maintaining and improving the effectiveness of the organization's PIMS. This ensures a degree of consistency with other management system standards, thereby supporting consistent and integrated implementation and operation with related management systems. Other management system standards include:

- BS EN ISO 9001 (Quality Management Systems);
- BS EN ISO 14001 (Environmental Management Systems);
- BS ISO/IEC 27001 (Information Security Management Systems);
- BS ISO/IEC 20000 (IT Service Management).

Figure A.1 illustrates how a PIMS takes as inputs the various requirements of this British Standard and, through the necessary actions and processes, produces data protection outcomes (i.e. managed personal information) that meet those requirements.

Figure A.1 **PDCA cycle applied to the management of personal information**



Plan	To plan for the implementation of a PIMS	Clause **3**
Do	To implement and operate the PIMS	Clause **4**
Check	To monitor and review the PIMS	Clause **5**
Act	To improve the PIMS	Clause **6**

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS EN ISO 9000:2005*, Quality management systems – Fundamentals and vocabulary*

BS EN ISO 9001*, Quality management systems – Requirements*

BS EN ISO 14001:2004*, Environmental management systems – Requirements with guidance for use*

BS ISO/IEC 20000*, Information technology – Service management – Code of practice*

BS ISO/IEC 27001*, Information technology – Security techniques – Information security management systems – Requirements*

BIP 0012*, Data Protection: Guide to practical implementation*

European Standards Committee CEN/ISSS Personal data protection audit framework

Other publications

[1] GREAT BRITAIN. Data Protection Act 1998, London: The Stationery Office. 1998.

[2] PARLIAMENT AND COUNCIL OF THE EUROPEAN COMMUNITY. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *OJ L 281, 23.11.1995, p. 31–50 (ES, DA, DE, EL, EN, FR, IT, NL, PT, FI, SV)*.

[3] GREAT BRITAIN. Freedom of Information Act 2000, London: The Stationery Office. 2000.

[4] INFORMATION COMMISSIONER'S OFFICE.[4)] *Data Protection Technical Guidance: Determining what information is 'data' for the purposes of the DPA*. 2009.

[5] INFORMATION COMMISSIONER'S OFFICE. *Data Protection Technical Guidance: Determining what is personal data*. 2007.

[6] INFORMATION COMMISSIONER'S OFFICE. *Data Protection Audit Manual*. 2001.

[7] INFORMATION COMMISSIONER'S OFFICE. *Data Protection Act 1998: Legal Guidance*.

[8] PARLIAMENT AND COUNCIL OF THE EUROPEAN COMMUNITY. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. *OJ L 105, 13.4.2006, p. 54–63 (ES, CS, DA, DE, ET, EL, EN, FR, IT, LV, LT, HU, MT, NL, PL, PT, SK, SL, FI, SV)*.

4) This and the other Information Commissioner's Office (ICO) documents in this bibliography, together with further guidance on fair processing, privacy notices, data security breach management and the notification of such breaches, etc., are available on the ICO's website: http://www.ico.gov.uk/

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

You may also buy directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop**

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library.

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com**

Copyright

BSI

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™

This British Standard specifies requirements for a personal information management system (PIMS), which provides a framework for maintaining and improving compliance with data protection legislation and good practice.
This British Standard is for use by organizations of any size and sector. It is intended to be used by those responsible for initiating, implementing and maintaining a PIMS within an organization. It is intended to provide a common ground for the management of personal information, for providing confidence in its management, and for enabling an effective assessment of compliance with data protection legislation and practice by both internal and external assessors.

389 Chiswick High Road
London W4 4AL
United Kingdom

Tel: +44 (0)20 8996 9001
Fax: +44 (0)20 8996 7001
Website: www.bsigroup.com
Email: info@bsigroup.com

ISBN 978-0-580-61550-4
9 780580 615504