

BRITISH STANDARD

BS 10012:2009

Data protection – Specification for a personal information management system



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.

© BSI 2009

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

Foreword *ii*

0 Introduction 1

1 Scope 3

2 Terms, definitions and abbreviations 3

3 Planning for a personal information management system (PIMS) 5

4 Implementing and operating the PIMS 7

5 Monitoring and reviewing the PIMS 20

6 Improving the PIMS 21

Annexes

Annex A (informative) The Plan-Do-Check-Act (PDCA) cycle 23

Bibliography 24

List of figures

Figure A.1 – PDCA cycle applied to the management of personal information 23

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.