BS 10012:2017

BSI Standards Publication

Data protection —

Specification for a personal information management system

bsi.

Publishing and copyright information

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

Published by BSI Standards Limited 2017

ISBN 978 0 580 93774 3

ICS 01.140.30, 03.100.99, 35.020

The following BSI references relate to the work on this document:
Committee reference IDT/1
Draft for comment 16/30339452 DC

Amendments/corrigenda issued since publication

Date	Text affected

Contents

Summary of pages
This document comprises a front cover, and inside front cover, pages i to ii, pages 1 to 42, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 31 March 2017. It was prepared by Technical Committee IDT/1, *Document Management Applications*. A list of organizations represented on this committee can be obtained on request to its secretary.

Supersession

This British Standard supersedes BS 10012:2009, which will be withdrawn on 25 May 2018.

Information about this document

This is a full revision of the standard, and introduces the following principal changes:

- requirements have been revised in line with the European Union General Data Protection Regulation 679/2016 (GDPR [1])[1];
- the structure has been updated to follow the ISO management system structure (see Annex A).

Presentational conventions

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

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

Requirements in this standard are drafted in accordance with *Rules for the structure and drafting of UK standards*, subclause **J.1.1**, which states, "Requirements should be expressed using wording such as: 'When tested as described in Annex X, the product shall ...'". This means that only those products that are capable of passing the specified test will be deemed to conform to this standard.

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.

1 See http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf [last accessed on 28 March 2017]

0 Introduction

0.1 General

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 requirements and good practice.

In many cases, a PIMS will address the management of personal information that is held across a wide range of operational units and information technology based application systems. Much of this personal information might also be within the scope of other management systems within the organization [e.g. quality management (BS EN ISO 9001), environmental management (BS EN ISO 14001), asset management (ISO 55001), information security management (BS EN ISO/IEC 27001)]. Where the organization has such multiple overlapping management systems, consideration needs to be given to utilizing a common approach such as that described in PAS 99, *Specification of common management system requirements as a framework for integration*.

This new edition of BS 10012 has been written in recognition of the publication of the European Union General Data Protection Regulation (GDPR) [1], which was approved by the European Parliament on 14 April 2016. This replaces the European Directive (95/46/EC) on 25 May 2018 [2], which was implemented in the UK by the Data Protection Act 1998 [3]. The GDPR will be directly applicable to the UK and member states retain the ability to introduce national level derogations where these are required for specific purposes. However the results of the referendum on the UK's membership of the European Union make it unclear how the GDPR will be implemented – such issues will be monitored and updates to this British Standard will be issued where necessary.

NOTE 1 Annex B compares UK practice under the DPA 1998 [3] and the GDPR 2016 [1].

Compliance with EU and UK data protection legislation is monitored, regulated and enforced by the Information Commissioner (the UK's "supervisory authority"), 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 (acting as controllers and/or processors) 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 national legislation, and issue information and enforcement notices.

NOTE 2 Articles 57 and 58 of the GDPR [1] detail the requirements and powers for supervisory authorities.

This British Standard is drafted using the rules specified for management system standards in the ISO Directives, Annex SL, and follows the common structure and core text (see Annex A). This enables compatibility with ISO management system standards.

0.2 Data protection principles

The GDPR requires personal information to be processed according to six data protection principles[2], which require personal information to be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are, in accordance with Article 89(1), not considered to be incompatible with the initial purposes ("purpose limitation");

2 The text given here is a summary of Article 5 of the GDPR [1]. For the full text, see the GDPR.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ("data minimization");

d) accurate and, where necessary, kept up to date; every reasonable step is taken to ensure that personal information that is inaccurate, with regard to the purposes for which it is processed, is erased or rectified without delay ("accuracy");

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information is processed; personal information can be stored for longer periods so far as the personal information is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject ("storage limitation"); and

f) processed in a manner that ensures appropriate security of the personal information, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality").

There is a seventh principle which requires data controllers to be accountable for, and be able to demonstrate compliance with, the six principles above.

In summary:

Principle (a) Lawfully, fairly and transparently processed (see 8.2.6);

Principle (b) Obtained only for specific legitimate purposes (see 8.2.7);

Principle (c) Adequate, relevant, limited in line with data limitation principles (see 8.2.8);

Principle (d) Accurate and up to date, with every effort to erase or rectify without delay (see 8.2.9);

Principle (e) Stored in a form that permits identification no longer than necessary (see 8.2.10);

Principle (f) Ensure appropriate security, integrity and confidentiality of personal information using technological and organizational measures (see 8.2.11).

General Accountability for the above

A number of exemptions or derogations from these data protection principles are permitted by the GDPR and can be introduced in national legislation. Examples of such exemptions are the processing for journalistic, academic, artistic and/or literary expression purposes.

NOTE See Recital 153 of the GDPR [1].

Reference can be made to the GDPR, national legislation, guidance from the supervisory authority and to other guidance and sector-specific advice for further details.

0.3 Notification

General notification obligations are not required under the GDPR. However, supervisory authorities might require data controllers and data processors to notify of processing activities that are likely to result in a high risk to the rights and freedoms of natural persons. At the time of the publication of this British Standard, guidance from the supervisory authority is awaited. A plan for the publication of this guidance can be found here: https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/[3].

3 Last accessed on 28 March 2017.

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 requirements 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 planning, establishing, implementing and maintaining a PIMS within an organization. It is intended to provide a common ground for the responsible management of personal information, for providing confidence in its management, and for enabling an effective assessment of compliance with data protection requirements and good practice by both internal and external assessors.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1 audit

systematic, independent and documented *process* (**3.1.25**) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

NOTE 1 An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

NOTE 2 An internal audit is conducted by the organization itself, or by an external party on its behalf.

NOTE 3 "Audit evidence" and "audit criteria" are defined in BS EN ISO 19011.

3.1.2 biometric information

personal information resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a *natural person* (**3.1.14**)

NOTE Biometric information typically allows or confirms the unique identification of the natural person, using information such as facial images or dactyloscopic data (such as finger prints).

3.1.3 competence

ability to apply knowledge and skills to achieve intended results

3.1.4 conformity

fulfilment of a *requirement* (**3.1.28**)

3.1.5 continual improvement

recurring activity to enhance *performance* (**3.1.19**)

3.1.6 corrective action

action to eliminate the cause of a *nonconformity* (**3.1.15**) and to prevent recurrence