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This British Standard supersedes BS 10012:2009, which will be withdrawn on 25 May 2018.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

3.1.7 documented information

information required to be controlled and maintained by an *organization* (**3.1.17**) and the medium on which it is contained

NOTE 1 Documented information can be in any format and media, and from any source.

NOTE 2 Documented information can refer to:

- *the* management system *(**3.1.11**), including related* processes *(**3.1.25**);*
- *information created in order for the organization to operate (documentation);*
- *evidence of results achieved (records).*

3.1.8 effectiveness

extent to which planned activities are realized and planned results achieved

3.1.9 genetic information

personal information relating to the inherited or acquired genetic characteristics of a *natural person* (**3.1.14**)

NOTE Genetic information typically includes unique information about the physiology which can indicate the health of the natural person and which results, in particular, from an analysis of a biological sample from the natural person in question.

3.1.10 interested party (preferred term); stakeholder (admitted term)

person or *organization* (**3.1.17**) that can affect, be affected by, or perceive itself to be affected by a decision or activity

NOTE Examples of relevant persons include workers, citizens, patients, consumers and users.

3.1.11 management system

set of interrelated or interacting elements of an *organization* (**3.1.17**) to establish *policies* (**3.1.23**) and *objectives* (**3.1.16**) and *processes* (**3.1.25**) to achieve those objectives

NOTE 1 A management system can address a single discipline or several disciplines.

NOTE 2 The system elements include the organization's structure, roles and responsibilities, planning and operation.

NOTE 3 The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

3.1.12 measurement

process (**3.1.25**) to determine a value

3.1.13 monitoring

determining the status of a system, a *process* (**3.1.25**) or an activity

NOTE To determine the status, there might be a need to check, supervise or critically observe.

3.1.14 natural person (data subject)

living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity

NOTE Extracted from the definition of "personal data" in Article 4(1) of the GDPR [1].

3.1.15 nonconformity

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

3.1.16 objective

result to be achieved

NOTE 1 An objective can be strategic, tactical, or operational.

*NOTE 2 Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process (**3.1.25**)).*

NOTE 3 An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a PIMS objective, or by the use of other words with similar meaning (e.g. aim, goal, or target).

NOTE 4 In the context of PIMS, PIMS objectives are set by the organization, consistent with the PIMS policy, to achieve specific results.

3.1.17 organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its *objectives* (**3.1.16**)

NOTE The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

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

3.1.18 outsource (verb)

make an arrangement where an external *organization* (**3.1.17**) performs part of an organization's function or *process* (**3.1.25**)

*NOTE An external organization is outside the scope of the management system (**3.1.11**), although the outsourced function or process is within the scope.*

3.1.19 performance

measurable result

NOTE 1 Performance can relate either to quantitative or qualitative findings.

*NOTE 2 Performance can relate to the management of activities, processes (**3.1.25**), products (including services), systems or organizations (**3.1.17**).*

3.1.20 personal information

information relating to an identified or identifiable *natural person* (**3.1.14**)

NOTE 1 An identifiable person is one who can be identified directly or indirectly, in particular with reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

NOTE 2 This includes pseudonymized but not fully anonymized data.

NOTE 3 Article 4(1) of the GDPR [1] defines "personal data" in this manner.

3.1.21 personal information management policy

statement of overall intentions and direction of the organization as formally approved by top management for managing compliance with data protection requirements and good practice

NOTE Hereafter referred to as "PIMS policy".

3.1.22 personal information management system (PIMS)

part of the overall management framework that plans, establishes, implements and maintains the management of personal information

NOTE It is recognized that an organizational PIMS addresses the management of personal information that might be held across a wide range of operational units and information technology based applications systems.

3.1.23 policy

intentions and direction of an *organization* (**3.1.17**), as formally expressed by its *top management* (**3.1.33**)

3.1.24 procedure

documented set of actions which is the prescribed or accepted way of doing something

3.1.25 process

set of interrelated or interacting activities which transforms inputs into outputs

3.1.26 processing

operation or set of operations which is performed upon personal information or sets of personal information

NOTE This is irrespective of whether or not by automated means.

EXAMPLE Processing can include collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (from the GDPR [1], Article 4(2)).

3.1.27 profiling

form of automated processing of personal information consisting of the use of personal information to evaluate certain personal aspects relating to a *natural person* (**3.1.14**)

NOTE Profiling is often used to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

3.1.28 requirement

need or expectation that is stated, generally implied or obligatory

NOTE 1 "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied.

NOTE 2 A specified requirement is one that is stated, for example in documented information.

3.1.29 risk

effect of uncertainty

NOTE 1 An effect is a deviation from the expected - positive or negative.

NOTE 2 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

NOTE 3 Risk is often characterized by reference to potential "events" (as defined in PD ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in PD ISO Guide 73:2009, 3.6.1.1) of occurrence.

3.1.30 special categories of personal information

personal information (**3.1.20**) relating to the *natural person's* (**3.1.14**):

a) racial or ethnic origin;

b) political opinions;

c) religious or philosophical beliefs;

d) trade-union membership;

e) the processing of genetic information;

f) biometric information for the purpose of uniquely identifying a *natural person*;

g) information concerning health or information concerning a natural person's sex life or sexual orientation.

NOTE See Article 9 of the GDPR [1] for special conditions under which special category information can be processed.

3.1.31 system

set of interrelated or interacting elements

[SOURCE: BS EN ISO 9000:2015, 3.5.1]

3.1.32 third party

natural or legal person, public authority, agency or body other than the data subject, data controller, data processor and workers who, under the direct authority of the data controller or data processor, are authorized to process personal information

[SOURCE: Adapted from Article 4(10) of the GDPR[1]]

3.1.33 top management

person or group of people who directs and controls an *organization* (3**.1.17**) at the highest level

NOTE 1 Top management has the power to delegate authority and provide resources within the organization.

*NOTE 2 If the scope of the management system (**3.1.11**) covers only part of an organization, then top management refer to those who direct and control that part of the organization.*

3.1.34 workers

people working under the control of the organization

NOTE 1 This includes employees, temporary staff, contractors, volunteers and consultants.

NOTE 2 This also includes top management.

3.2 Abbreviations

BCR	Binding Corporate Rules
DPA	Data Protection Act 1998 [3]
DPO	Data Protection Officer
EEA	European Economic Area
EU	European Union
FCA	Financial Conduct Authority
GDPR	General Data Protection Regulation [1]

ICO	Information Commissioner's Office
PIA	Privacy Impact Assessment
PIMS	Personal Information Management System

4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its personal information management system.

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

- the interested parties that are relevant to the PIMS;
- the relevant requirements of these interested parties.

4.3 Determining the scope of the personal information management system

The organization shall determine the boundaries and applicability of the PIMS to establish its scope.

When determining this scope, the organization shall consider:

- the external and internal issues referred to in **4.1**;
- the requirements referred to in **4.2**;
- organizational objectives and obligations;
- the organization's acceptable level of risk; and
- applicable statutory, regulatory, contractual and/or professional duties.

The scope shall be available as documented information.

4.4 Personal information management system

Objective: To plan for the implementation of a PIMS that can provide direction and support for compliance with data protection requirements and good practice.

The organization shall establish, implement, maintain and continually improve a PIMS, including the processes needed and their interactions, in accordance with the requirements of this British Standard.

NOTE It is recognized that an organizational PIMS addresses the management of personal information that might be held across a wide range of operational units and information technology based applications 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 (BS ISO 55001), information security management (BS EN ISO/IEC 27001)). Where the organization has such multiple, overlapping management systems consideration should be given to utilizing an approach such as described in PAS 99, Specification of common management system requirements as a framework for integration.

5 Leadership

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the PIMS by:

- ensuring that the PIMS policy and PIMS objectives are established and are compatible with the strategic direction of the organization;
- ensuring the integration of the PIMS requirements into the organization's business processes;
- ensuring that the resources needed for the PIMS are available;
- communicating the importance of effective personal information management and of conforming to the PIMS requirements;
- ensuring that the PIMS achieves its intended outcome(s);
- directing and supporting persons to contribute to the effectiveness of the PIMS;
- promoting continual improvement;
- supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

NOTE Reference to 'business' in this British Standard can be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

5.2 Policy

Top management shall establish a PIMS policy that:

a) is appropriate to the purpose of the organization;

b) provides a framework for setting PIMS objectives;

c) includes a commitment to satisfy applicable requirements;

d) includes a commitment to continual improvement of the PIMS management system.

The PIMS policy shall:

- be available as documented information;
- be communicated within the organization;
- be available to interested parties, as appropriate.

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

1) processing personal information only where this is strictly necessary for legal and regulatory purposes, or for legitimate organizational purposes (see **6.1.3.1**);

2) processing only the minimum personal information required for these purposes (see **6.1.7**);

3) providing clear information to natural persons (including children) about how their personal information can be used and by whom (see **8.2.12.2**);

4) ensuring special safeguards when collecting information directly from children (see **6.1.4**, **8.2.2.2**, **8.2.7.3** and **8.2.7.6**);

5) only processing relevant and adequate personal information (see **8.2.8**);

6) processing personal information fairly and lawfully (see **8.2.6**);

7) maintaining a documented inventory of the categories of personal information processed by the organization (see **8.2.2.1**);

8) keeping personal information accurate and, where necessary, up-to-date (see **8.2.9.1**);

9) retaining personal information only for as long as is necessary for legal or regulatory reasons or for legitimate organizational purposes and ensuring timely and appropriate disposal (see **8.2.10**);

10) respecting natural persons' rights in relation to their personal information (see **8.2.12**);

11) keeping all personal information secure (see **8.2.11**);

12) only transferring personal information outside the UK in circumstances where it can be adequately protected (see **8.2.11.8**);

13) where appropriate, the strategy for dealing with regulators across the EU, where goods and/or services are offered to natural persons who are resident in other EU countries;

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

15) developing and implementing a PIMS to enable the PIMS policy to be implemented (see **6.1**, **6.2** and **7**);

16) where appropriate, identifying internal and external interested parties and the degree to which they are involved in the governance of the organization's PIMS (see **7.4**);

17) the identification of workers with specific responsibility and accountability (see **3.1.34** and **8.2.1**) for the PIMS; and

18) maintain records of processing of personal information (see **8.2.6.1**, **8.2.6.2**, **8.2.7.2**, **8.2.11.7** and **8.2.11.9**).

The PIMS policy shall state that it covers either:

- the whole organization; or
- an identified part of the organization.

5.3 Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

a) ensuring that the PIMS conforms to the requirements of this British Standard;

b) reporting on the performance of the PIMS to top management.

A member of the top management team shall be accountable for the management of personal information within the organization so that compliance with data protection requirements and good practice can be demonstrated (see also **8.2.1.1**). This accountability shall include:

1) approval of the PIMS policy by the top management team;

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

3) security and risk management in relation to compliance with the PIMS policy (see also **8.2.11.1**).

One or more suitably qualified or experienced workers shall be appointed to take responsibility for the organization's compliance with the PIMS policy on a day-to-day basis (see also **8.2.1.3**).

NOTE The senior manager accountable and the worker(s) responsible for day-to-day compliance could be the same person.

Workers shall comply with the PIMS 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.

5.4 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, test and maintain awareness of the PIMS through an ongoing education and awareness programme for workers;

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

c) communicate to workers the importance of:

1) meeting PIMS objectives;

2) complying with the PIMS policy;

3) continual improvement of the PIMS policy;

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

e) retain documented information of training and awareness activities and its effectiveness.

---

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the PIMS, the organization shall consider the issues referred to in **4.1** and the requirements referred to in **4.2** and determine the risks and opportunities that need to be addressed to:

- give assurance that the PIMS can achieve its intended outcome(s);
- prevent, or reduce, undesired effects;
- achieve continual improvement.

The organization shall plan:

a) actions to address these risks and opportunities;

b) how to:

- integrate and implement the actions into its PIMS processes;
- evaluate the effectiveness of these actions.

6.1.2 Data inventory and data flow

The organization shall define a data inventory and data flow analysis process that:

a) establishes and maintains a data inventory and data flow analysis that includes the identification of:

1) key business processes that utilize personal information;

2) sources of the personal information;

3) categories of personal information processed, including the identification of high-risk personal information (see **8.2.2.2**);

4) purposes for which the personal information can be used, including subsequent secondary purposes over and above the initial purpose collected;

5) potential recipients of personal information, including disclosure of personal information to third parties, data processors and transfer to vendors;

6) (within personal information data flows) where an organization is acting as a data controller, a data processor or a joint data controller;

7) key systems and repositories of personal information;

8) (within personal information flows) where personal information is transferred over international boundaries or subject to differing laws, regulations, standards or frameworks;

9) retention and disposal requirements for personal information, and the criteria for these requirements; and

b) ensures that repeated data inventories produce consistent, valid and comparable results.

NOTE 1 Article 30 requires data controllers to maintain a record of processing activities to demonstrate compliance with the GDPR [1]. It specifies the information to be provided in the record.

NOTE 2 The organization should consider the retention of up-to-date documented information regarding the data inventory and data flow identification.

NOTE 3 The organization should consider whether to retain superseded versions of the data inventory in accordance with their information retention policy and retention schedule.

6.1.3 Legal basis

6.1.3.1 Processing

The organization shall identify, define and document the legal basis for the processing of all personal information, which shall be selected from one or more of the following:

- the appropriate natural person's unambiguous consent for specific purposes;
- necessary for the performance of a contract to which the natural person is a party, or to take steps to enter into a contract;
- necessary for compliance with a legal obligation to which the organization is subject;
- necessary for protecting the vital interests of the natural person;
- necessary to perform a task carried out in the public interest or exercise of official authority of the organization;
- necessary for the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the natural person (not applicable to processing carried out by public bodies in the performance of their tasks)

  NOTE 1 For further details of "legitimate interest", see Recital 47 of the GDPR [1].

- additional provisions for processing of a kind introduced by national laws.

NOTE 2 Attention is drawn to Article 7 of the GDPR [1] for giving and withdrawing consent by a natural person.

NOTE 3 Attention is drawn to Article 5 1(b) of the GDPR [1] for the documenting of the legitimate interests of the organization.

6.1.3.2 Special categories

When special categories of personal information are being processed, the organization shall, in addition to the list detailed in **6.1.3.1**, identify, define and document the additional legal basis for the processing of personal information, which shall be selected from one or more of the following:

- natural person's explicit consent for specific purposes;
- necessary for employment rights or obligations;
- necessary for protecting the vital interests of the natural person;
- necessary for legitimate activities of a foundation, association, or any other non-profit making body for a political, philosophical, religious or trade union aim, with appropriate safeguards;
- information deliberately made public by the natural person;
- necessary for the establishment, exercise or defence of legal claims;
- necessary for reasons of substantial public interest;
- necessary for preventive or occupational medicine, assessment of the working capacity of an employee, medical diagnosis, provision of health or social care systems and services;
- necessary for reasons of public health or professional secrecy;
- additional provisions for processing of a kind introduced by national laws with regard to the processing of genetic, biometric or health data.

6.1.4 Privacy impact assessment (PIA)

NOTE 1 PIAs are sometimes referred to as Data Protection Impact Assessments (DPIAs)

The organization shall define the PIA processes relating to the processing of personal information that:

a) establish and maintain privacy risk criteria, including:
   - risk acceptance criteria;
   - criteria for performing privacy risk assessments (including where externally mandated); and
   - application of the data protection principles (see **0.2**) to the data flows (see **6.1.2**) in order to identify privacy risks (see **6.1.5**).

b) ensure that repeated privacy risk assessment processes are consistent, valid and comparable;

c) identify the data protection risks associated with the privacy risk assessment process to identify risks associated with:
   - relevant privacy laws, standards and frameworks;
   - the impact on the rights and freedoms of natural persons;
   - any physical, material or non-material damage to natural persons; and
   - the impact on the organization (including, but not limited to reputation, regulatory action, financial loss, etc.);

d) identify high-risk personal information (see **8.2.2.2**) and related processes that are high risk;

e) identify the risk owners;

f) analyses the privacy risks that:
   1) assess the potential consequences that would result if the risks identified in the privacy risk assessment were to materialize;

2) assess the realistic likelihood of the occurrence of the risks identified in the privacy risk assessment; and

3) determines the levels of risk.

g) evaluate the privacy risks, including:

1) comparison of the results of risk analysis with the risk criteria; and

2) prioritizing the analysed risks for risk treatment.

The organization shall retain documented information about the privacy impact and risk assessment process.

NOTE 2 Physical, material or non-material damage means, in particular:

- *where the processing might give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal information protected by professional secrecy, unauthorized reversal of de-identification, or any other significant economic or social disadvantage;*
- *where natural persons might be deprived of their rights and freedoms or prevented from exercising control over their personal information;*
- *where special categories of personal information or information relating to criminal convictions and offences or related security measures are processed;*
- *where personal aspects are evaluated, such as profiling;*
- *where personal information of vulnerable natural persons, in particular of children, is processed; or*
- *where processing involves a large amount of personal information and affects a large number of data subjects.*

NOTE 3 Vulnerable natural persons are those who, due to their personal circumstances, are especially susceptible to detriment, particularly when a data controller is not acting with appropriate levels of care.

NOTE 4 An example of a risk assessment process (as applied to records) is included in PD ISO/TR 18128:2014 Information and documentation – Risk assessment for records processes and systems.

6.1.5 Privacy risk treatment

The organization shall define privacy risk treatment processes (see also **8.2.11**) to:

a) select appropriate privacy risk treatment options, taking into account the risk assessment results;

b) determine all controls that are necessary to implement the privacy risk treatment option(s) chosen;

NOTE 1 Organizations are required to implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is carried out in accordance with the law, hence they need to design their controls as appropriate, or identify them from any source, including codes of conduct issued by appropriate regulators and supervisory authorities.

c) formulate a privacy risk treatment plan; and

d) obtain risk owners' approval of the privacy risk treatment plan and acceptance of the residual privacy risks.

The organization shall retain documented information about the privacy risk treatment process.

NOTE 2 The privacy risk assessment and treatment process in this British Standard align with the principles and generic guidelines provided in BS ISO 31000.

NOTE 3 Controls could include, for example, de-identification, pseudonymization, data minimization, reducing the extent and purposes of processing, period of storage, accessibility or technical and organizational information security measures, such as those identified in BS EN ISO/IEC 27001.

6.1.6 Prior consultation and authorization

Where risks to the natural person from personal information processing are identified by the PIA to be of a high level, and the risks are unable to be mitigated, prior consultation and authorization by the supervisory authority shall be sought.

The organization shall retain documented information on the criteria and processes for interacting with appropriate supervisory bodies on prior consultation and authorization.

NOTE 1 High-risk processing includes extensive profiling activities, or the absence of controls taken by the organization to mitigate risks to the natural person.

NOTE 2 See Article (36)3 of the GDPR [1].

6.1.7 Privacy by design and by default

NOTE See Article 25 of the GDPR [1].

When designing or making significant changes to:

a) systems for use within the organization or by data processors; or

b) products and services for the use of individuals or other organizations,

the organization shall ensure that the processing of personal information by such systems, products or services:

1) is minimized by default;

2) uses de-identified information where possible; and

3) is transparent with regards to the functions and processing of personal information.

This shall be achieved by taking the appropriate organizational and technical actions:

i) that are appropriate to the risks identified (see **6.1.4**);

ii) that ensure privacy controls identified (see **6.1.5**) are implemented as appropriate personal information protections; and

iii) that retain appropriate documented information of privacy by design activities and results.

6.2 PIMS objectives and planning to achieve them

The organization shall establish PIMS objectives at relevant functions and levels.

The PIMS objectives shall:

a) be consistent with the PIMS policy;

b) be measurable (if practicable);

c) take into account applicable privacy requirements, and results from risk assessments and risk treatments;

d) be monitored;

e) be communicated;

f) be updated as appropriate.

The organization shall retain documented information on the PIMS objectives.

When planning how to achieve its PIMS objectives, the organization shall determine:

- what will be done;
- what resources will be required;
- who will be responsible;

- when it will be completed;
- how the results will be evaluated.

7 Support

7.1 Resources

The organization shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the PIMS (see also **8.2.1**).

7.2 Competence

The organization shall:

- determine the necessary competence of person(s) doing work under its control that affects its PIMS performance;
- ensure that these persons are competent on the basis of appropriate education, training, or experience;
- where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken;
- retain appropriate documented information as evidence of competence.

NOTE Applicable actions can include, for example, the provision of training to, the mentoring of, or the reassignment of currently employed persons; or the hiring or contracting of competent persons.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

- the PIMS policy;
- their contribution to the effectiveness of the PIMS, including the benefits of improved PIMS performance;
- the implications of not conforming with the PIMS requirements.

For further information on training and awareness, see **8.2.4**.

7.4 Communication

The organization shall determine the internal and external communications relevant to the PIMS, including:

- on what it will communicate;
- when to communicate;
- with whom to communicate;
- how to communicate.

7.5 Documented information

7.5.1 General

The organization's PIMS shall include:

a) documented information required by this British Standard;

b) documented information determined by the organization as being necessary for the effectiveness of the PIMS.

NOTE The extent of documented information for a PIMS can differ from one organization to another due to:

- *the size of organization and its type of activities, processes, products and services;*
- *the complexity of processes and their interactions;*
- *the competence of persons.*

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

- identification and description (e.g. a title, date, author, or reference number);
- format (e.g. language, software version, graphics) and media (e.g. paper, electronic);
- review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the PIMS and by this British Standard shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

- distribution, access, retrieval and use;
- storage and preservation, including preservation of legibility;
- control of changes (e.g. version control);
- retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the PIMS shall be identified, as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

---

8 Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in **6.1**, by:

- establishing criteria for the processes;
- implementing control of the processes in accordance with the criteria;
- keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are controlled.

8.2 Implementing the PIMS

8.2.1 Key appointments

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

8.2.1.1 Top management

A member of the top management team shall be designated as accountable for the management of personal information within the organization so that compliance with data protection requirements and good practice can be demonstrated (also see **5.3**).

8.2.1.2 Data protection officer (DPO)

NOTE See Article 37 of the GDPR [1].

Where the organization is required to appoint a DPO by legislation, a supervisory authority requirement or a business need, a suitably qualified worker shall be appointed to fulfil this role. Contact details for the DPO shall be reported to the relevant supervisory authority.

The DPO or a suitably qualified worker shall ensure that the PIMS policy conforms to applicable laws, regulations and business requirements.

The DPO or a suitably qualified worker shall ensure that the appropriate privacy impact assessments and risk assessments are carried out where necessary.

The DPO or a suitably qualified worker shall ensure that any notifications to the supervisory authority are carried out where necessary.

The organization shall involve the DPO or the suitably qualified worker in a timely manner in all issues relating to the processing of personal information.

8.2.1.3 Day-to-day responsibility for compliance with the PIMS policy

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

Where appropriate, the appointed worker(s) shall report to the DPO or other qualified worker as necessary to fulfil their responsibilities.

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

a) overall responsibility for monitoring compliance with the PIMS policy;

b) development and review of the PIMS policy;

c) ensuring implementation of the PIMS policy;

d) management reviews of the PIMS policy (see **9.3**);

e) training and ongoing awareness as required by the PIMS policy;

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

   1) the management and communication of privacy information (see **8.2.6.1**);

   2) the handling of requests from natural persons (see **8.2.12.2**);

   3) the collection and handling of personal information (see **8.2.6.1**);

   4) complaints handling (see **8.2.12.9**);

   5) the management of security breaches (see **8.2.11.7**); and

6) outsourcing and off-shoring (see **8.2.11.10**).

g) liaison with those responsible for risk management, security issues and audit functions within the organization (see **8.2.11**);

h) provision of expert information, advice and guidance on data protection matters;

i) the interpretation and application of the various exemptions applicable to the processing of personal information (see Introduction and **8.2.7**);

NOTE In addition to the requirements of BS 10012, the organization might wish to consider other approved codes of conduct or good practice or to demonstrate that they are independently accredited against schemes that result in their ability to show a certificate, seal or trust mark issued by an approved third-party organization.

j) the provision of advice in relation to data sharing projects (including security issues when data are off site) (see **8.2.7.4**);

k) ensuring the organization has access to legislative updates and appropriate guidance related to data protection requirements (see **6.1.3**) and that the PIMS policy is continually reviewed to conform to the legislative updates; and

l) 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.

8.2.1.4 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 **8.2.2.2** for examples of personal information in high-risk categories); and

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

8.2.2 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.

8.2.2.1 Inventory

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.

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

*NOTE See **6.1.2**.*

8.2.2.2 High-risk personal information

The inventory (see **8.2.2.1**) shall allow for the explicit identification and documentation of the high-risk categories of personal information processed by the organization.

NOTE 1 High-risk categories of personal information can include:

*a) special category personal information (see **3.1.30**);*

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 natural persons (including children); and

f) sensitive negotiations which could adversely affect natural persons.

NOTE 2 The level of risk can increase where high volumes of personal information are processed.

8.2.3 Risk assessment and treatment

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 natural persons associated with the processing of their personal information, by the implementation of the PIA (see **6.1.4**). Such assessments shall include processing undertaken by other organizations. The organization shall implement a risk treatment plan to manage any risks which are identified by the risk assessment in order to reduce the likelihood of a nonconformity with the PIMS policy.

The risk assessment process shall include procedures whereby any processing of personal information that could cause damage and/or distress to the natural persons can be escalated for review to those responsible and accountable (see **5.3**) 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[4].

8.2.4 Training and awareness

Objective: To ensure that 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 requirements and good practice (see **8.2.1.3**):

- is able to demonstrate competence in their understanding of data protection requirements and good practice and how this should be implemented within the organization, and,
- 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 workers (see also **7.3**) 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.

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. In particular, the requirement of workers to adhere to applicable information security procedures shall be emphasised.

8.2.5 Keeping PIMS up to date

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

The worker(s) with day-to-day responsibility for compliance with the PIMS policy (see **8.2.1**) shall assess at planned intervals whether the PIMS enables and will continue to enable demonstration of compliance with the data protection requirements 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 See https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/ [Last accessed on 28 March 2017.]

8.2.6 Fair, lawful and transparent processing

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

8.2.6.1 Collection and processing of personal information

The PIMS shall ensure, based on the legal basis for processing (see **6.1.3**), that:

a) the organization processes personal information fairly and lawfully;

b) the organization processes personal information only where this is justified, in line with requirements;

NOTE 1 Article 6 of the GDPR [1] defines "Lawfulness of processing".

c) the organization processes high-risk personal information (see **8.2.2.2**) only where this is necessary for the organization's purposes, in line with requirements;

d) the organization provides natural persons with information in an appropriate format, which clearly communicates:

1) the identity of the organization and its representatives where applicable;

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

3) the legitimate interests of the organization or the processing where this is the legal basis used;

4) the types of personal information collected (only where information is collected from a source other than the natural person);

5) the source of the personal information and, where applicable, whether it came from publicly accessible sources (only when information is collected from a source other than the natural person);

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

7) whether personal information is transferred outside the EEA and an explanation of the safeguards in place, and how to get a copy of these safeguards;

8) where the organization is based outside the EU (which will be the case if the UK is no longer be a member of the EU) and the natural person is in the EU, the identity of the EU based representative, where this is required;

NOTE 2 Articles 3(2) and 27 of the GDPR [1] specify when there is a requirement for an EU-based representative. Does not affect, for example, public authorities - see Article 27(2).details of how to contact the organization with queries related to the processing of personal information, including contact details for the DPO (where such an officer has been appointed);

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

10) other information to make the processing fair and transparent:

i) the retention period(s) or the criteria used to set retention;

ii) information regarding the natural person's rights of access to, and correction, deletion and restriction of personal information, as well as the right to data portability;

iii) the right to lodge a complaint with the supervisory authority;

iv) where the processing is based on consent, the right to withdraw consent;

v) where the provision of information is a statutory or contractual requirement, informing the natural person why it is necessary and what the consequences are of failing to provide the information; and

vi) information about any automated decision making and/or profiling that the information might be used for, including the logic involved and the consequences for the natural person.

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

Where profiling by automated means is used for marketing purposes, the PIMS shall ensure that the right to object and the mechanism by which a natural person can object to such processes is clearly explained to that natural person.

The PIMS shall ensure that, where processing has been based upon consent, records of the consent are retained. Further, where consent is withdrawn, processing based on that consent is ceased, and records of the withdrawal of consent are retained.

Where other sectoral requirements or legislation require explicit consent for marketing, the PIMS shall ensure that details of this consent are collected.

Where high-risk personal information (see **8.2.2.2**) is being collected for a particular purpose(s), the PIMS shall ensure that the privacy information provided explicitly states the purpose(s) for which high-risk personal information is or might be used.

The PIMS shall ensure that new collection methods are reviewed and signed off by an appropriately qualified or experienced worker (see **8.2.1.2**) to ensure that such methods can be demonstrated as compliant with data protection requirements and good practice.

8.2.6.2 Records of privacy information (such as notices and statements)

The PIMS shall maintain records of privacy information provided to individuals (such as 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. Information relating to when a particular privacy notice (or version of a privacy notice) was in effect shall be retained.

NOTE This ensures that there is a record of the terms under which particular personal information was collected.

8.2.6.3 Timing of privacy information

The PIMS shall ensure that, where the organization collects personal information directly from a natural person, any information required to be given to the natural person is provided or made available to the natural person prior to any personal information being obtained.

Where information is not directly obtained from the natural person, the information shall be provided after obtaining the information or:

a) at the latest within one month, having regard to the specific circumstances in which the information is processed, or;

b) if the information is used to communicate with the natural person, then at the time of first communication; or

c) if the information is intended to be disclosed to another recipient, then at least when the information is first disclosed.

8.2.6.4 Accessibility of privacy information

The PIMS shall ensure that any information presented to natural persons is presented in a way which allows it to be easily accessible and understood by the intended audience.

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

8.2.6.5 Collection from third parties

The PIMS shall ensure that, where personal information is collected from third parties, it is collected fairly and lawfully.

Where personal information is collected from third parties, the PIMS shall ensure that, where necessary, the identified natural persons are provided with information as specified in **8.2.6.1**d) within one month of collection, unless the natural person already has the information and/or doing so would involve disproportionate effort.

NOTE 1 "Disproportionate effort" in this context does not merely mean "considerable effort", as the organization could be required to go to considerable lengths to provide information where the processing is likely to have a prejudicial effect on the natural person. Attention is drawn to Article 14 5(b) of the GDPR [1].

NOTE 2 There is no obligation to provide information where the personal information has been obtained or disclosed as expressly permitted by law or there is an obligation of confidentiality laid down by law.

8.2.7 Processing for specific legitimate 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 those purposes.

8.2.7.1 Grounds for processing

The PIMS shall 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.

The PIMS shall ensure that the 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 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 natural persons whose personal information is to be processed for the new purpose have consented to the processing for this new purpose.

The PIMS shall ensure that, where high-risk personal information (see **8.2.2.2**) is to be used for an incompatible new purpose, the natural person's explicit consent is obtained for this prior to processing, unless a relevant exemption applies.

8.2.7.2 Consent for incompatible purposes

Any processing shall be compatible with the original purpose. If personal information is used for any purpose additional to, or different, from the originally specified purpose, the new use shall not be unexpected and shall be fair.

The PIMS shall ensure that any consent for any incompatible purpose is freely given and informed.

The PIMS shall ensure that:

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

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

8.2.7.3 Processing children's information

Where personal information related to children is being processed, particularly with the intention of creating a profile and/or for marketing, the PIMS shall include a mechanism for obtaining the consent of the holder of parental responsibility, except in those instances where the service relates to counselling or preventative services.

NOTE There is no defined age limit for "children". Article 8 of the GDPR [1] states that "natural persons are no longer children once they have reached the age of 16". Where the child is under 16, then processing in relation to information society services is lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. Member states might provide a law for a lower age than 16, but this cannot be lower than 13.

8.2.7.4 Data sharing

The PIMS shall 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 ensure that, where the other organization is 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 does not contravene data protection legislation.

The PIMS shall ensure that, wherever possible, any new processing which involves the sharing of personal information with third parties is compatible with the terms of the information (see **8.2.6.1**) provided to the natural person.

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

1) a legal basis for the data sharing;

2) provided appropriate notice of sharing to the natural person, as appropriate;

3) assessed compliance with the purpose limitation principle; and

4) if required, the natural person's consent to the data sharing.

Where data sharing with third parties is allowed without the consent of the natural person, the PIMS shall 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 ensure that the protocols and controls for the data sharing are documented.

8.2.7.5 Open data

Where personal information is being published as part of an "open data" initiative, the personal information shall be de-identified so that natural persons are not identifiable, unless there are grounds for making the personal information public.

Where de-identification is being used, account shall be taken of all the reasonable means likely to be used to re-identify a natural person.

8.2.7.6 Data matching

Where personal information is matched with other personal information to create, for example, an enhanced profile of an identifiable natural person, the PIMS shall ensure that the matched personal information is only used:

- for notified and compatible purposes;
- as required by law; or
- where consent has been obtained.

Where data matching relates to personal information about children, specific protection measures shall be included within the PIMS. These measures shall take into account:

- the potential risks and consequences;
- requirements for safeguards; and
- the specific rights of children.

8.2.8 Adequate, relevant and in line with data minimization principles

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

8.2.8.1 Adequacy

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

The PIMS shall ensure that regular reviews (e.g. annually) of technology and processes involving the processing of personal information are carried out to ensure that the personal information continues to be adequate for those purposes.

8.2.8.2 Relevant and not excessive

The PIMS shall 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 natural person;

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.

NOTE The organization needs to consider whether it is appropriate to use anonymization or other de-identification of personal information prior to processing to further safeguard the data and document the results of the considerations.

8.2.9 Accuracy

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

8.2.9.1 Accurate and up to date

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

The PIMS shall ensure that natural persons are able 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 document the reported inaccuracy and, where appropriate, the accurate personal information.

The PIMS shall have an approved and documented process to check whether alleged inaccuracies are truly inaccurate. In the event that this checking process concludes that the alleged inaccuracy is erroneous and the data is, in fact, accurate the PIMS shall retain the appropriate evidence.

The PIMS shall 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 natural persons.

The PIMS shall:

a) inform any third party with whom the organization has shared 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 natural persons concerned; and

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

The PIMS shall review 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.

8.2.10 Retention and disposal

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

8.2.10.1 Retention schedules

The PIMS shall reference retention schedules for the identification of retention periods for personal information. Such schedules shall:

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

b) make clear and document the justification and basis for the retention periods.

At the end of the retention period, the PIMS shall ensure that all copies of personal information no longer required by the organization are disposed of, by reference to 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 1 Disposal procedures should include copies held on backup systems/media.

Where personal information is to be transferred for long-term preservation (for example where it is of value for archiving purposes in the public interest, scientific or historical research purposes or

statistical purposes), then it shall be subject to appropriate technical and organizational measures in order to safeguard the rights and freedoms of the natural person.

NOTE 2 See Article 5(1e) of the GDPR [1].

The PIMS shall ensure the implementation of the retention schedules and the communication of the schedules to all relevant workers.

8.2.11 Security issues

Objective: To ensure that personal information is protected against unauthorized or unlawful processing and against external loss, destruction or damage, using appropriate technical and organizational measures and controls.

8.2.11.1 Security measures

The PIMS shall specify appropriate security measures, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes for the processing of personal information.

NOTE Such security measures can include:

a) the pseudonymization and/or encryption of personal information;

b) the ability to ensure on going confidentiality, integrity, availability and resilience of systems;

c) the ability to restore access to personal information in the event of a physical and/or technical incident; and

d) the testing and evaluation of the effectiveness of the identified security measures.

8.2.11.2 Security controls

The PIMS shall implement the appropriate security measures by the specification and implementation of security controls as appropriate:

a) to the type of personal information being processed;

b) to the risk of damage or distress to the natural persons if the information is compromised (see **8.2.3**); and

c) to the risk of operational and reputational damage to the organization.

*NOTE 1 The risk assessment (**8.2.3**) establishes an appropriate level of control. Over-specifying security requirements can be as damaging as under-specifying.*

Where high-risk personal information (see **8.2.2.2**) is processed, the PIMS shall ensure that the security controls specified and implemented are appropriate to the assessed risks, and that they remain so.

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

8.2.11.3 Storage and handling

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

The PIMS shall ensure that specific attention is paid to the storage of personal information on removable media, portable devices (especially if the portable device is used under a "bring your own device" policy) and third-party storage systems (e.g. cloud storage).

8.2.11.4 Transfer

The PIMS shall 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 transmission.

NOTE Where electronic transfers are undertaken, encryption should be used.

8.2.11.5 Access controls

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

Where high-risk personal information is processed (see **8.2.2.2**), the PIMS shall ensure that access controls reflect the sensitivity of this information.

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

8.2.11.6 Security assessments

The PIMS shall 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 natural persons in the event of a security breach.

8.2.11.7 Managing security breaches

The PIMS shall:

a) assess, manage and document security breaches involving personal information, including procedures to mitigate the damage caused by any security breach;

b) notify the supervisory authority (with the required information within 72 hours of becoming aware of the breach) of any security breaches that constitute a breach that is likely to cause a risk to the rights and freedoms of any natural persons. Such notifications shall include:

   1) a description of the personal information involved;

   2) details of categories of the personal information and the approximate number of records involved;

   3) contact details for the DPO or other contact point within the organization;

   4) a description of likely consequences of the breach;

   5) a description of the measures taken or proposed to address the breach and to mitigate any possible adverse effects;

   NOTE 1 Attention is drawn to Article 33(3) of the GDPR [1].

c) where the breach is likely to result in a high risk to the rights and freedoms of natural persons, notify the concerned natural persons without undue delay of:

   1) the security breach;

   2) the nature of the breach; and

3) any recommendations for their actions regarding the mitigation of any adverse risks;

d) document each security breach, including an assessment of how the breach occurred, what corrective action was taken, and what can be learned from the breach;

e) make decisions as to whether or not a security breach is referred to any relevant regulator (for example the FCA); and

f) keep records of any such notifications issued.

NOTE 2 If an organization does not handle/process/store personal information appropriately it might be at risk of sanctions, including fines. The GDPR [1] defines potential sanctions (which apply to any organization (globally) processing the personal information within the scope of the GDPR). These sanctions include:

- *a written warning for the first non-intentional non-compliance case;*
- *regular periodic data protection audits; and*
- *a fine of up to EUR 20 000 000 or up to 4% of annual worldwide turnover of the preceding financial year, whichever is greater.*

NOTE 3 In the event of the organization not complying with the legal requirements of the GDPR [1], organizational adherence to approved codes of conduct or approved certification, seals or marks might be taken into consideration when deciding whether or not to impose a fine and, in the event of a fine being imposed, the amount of that fine. Attention is drawn to Articles 40, 42 and 83 of the GDPR.

NOTE 4 Annex C gives further information on codes, seals and certification.

8.2.11.8 Transfer of personal information outside the UK

NOTE While the UK remains within the EU, the organization may transfer personal information to other parts of the EEA as the rights of natural persons are protected by compliance with the GDPR [1] of that member of the EEA.

Where the organization transfers personal information outside the UK[5], the PIMS shall ensure that the rights of the natural persons are protected:

a) in the event of the UK not being a member of the EU or EEA at the time of transfer:

1) for transfer to a country or territory that is a member of the EEA by establishing whether the EEA has been assessed by the UK as providing adequate protection;

2) for transfer to other countries or territories, by establishing whether the destination country or territory has been assessed by the UK as providing adequate protection;

b) in the event of the UK being a member of the EU or EEA at the time of transfer, by establishing whether the country or territory has been assessed by the European Commission as providing adequate protection;

c) by including within contracts specific conditions which ensure the protection of the personal information and the processing, e.g. using, based on or mirroring established standard clauses or model contracts;

d) by putting in place internal binding corporate rules (BCR) where the transfer is to another entity within the same organization;

e) by complying with an approved code of conduct or approved certification mechanism along with binding and enforceable commitments on the destination organization;

f) for public bodies by complying with a legally binding and enforceable instrument or administrative arrangement;

g) by transferring in line with an applicable derogation.

5 Information on data transfers outside the EU can be found at http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm [last accessed 28 March 2017].

The PIMS shall ensure that the top management and worker(s) responsible and accountable for compliance with data protection requirements and good practice (see **8.2.1.3**) reviews all new initiatives involving:

i) the transfer of personal information between the UK and the EEA; and

ii) the transfer of personal information outside the UK.

This review shall establish whether adequate protection can be provided for such transfers.

The PIMS shall ensure that data processors and any sub-processors based outside the UK who process personal information on behalf of the organization operate according to appropriate contractual terms (e.g. standard clauses or model contracts, such as those approved by the European Commission for ensuring adequate protection for personal information), unless other adequate procedures have been agreed to protect the personal information.

8.2.11.9 Disclosure to third parties requests

The PIMS shall ensure that third parties provide evidence of:

a) their right to request a copy of the specified personal information; and

b) where necessary, their identity.

The PIMS shall 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 maintain 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 [4], verification of identity and minimization of the information disclosed might not be necessary.

8.2.11.10 Subcontracted information processing

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

a) only organizations acting as data processors are selected that can provide technical, physical and organization security which meet the requirements of the organization for all the personal information they process on behalf of the organization;

b) an assessment of appropriate security is undertaken as part of due diligence before an organization acting as data processor 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 security arrangements of the organization acting as the data processor is conducted before entering into the contract;

c) by carrying out due diligence on the organization acting as data processor;

d) once the organization acting as the data processor has been selected, the organization puts in place a binding written agreement or contract that:

   1) sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal information and the categories of natural persons, and the obligations and rights of the organization;

   2) sets out that the organization acting as the data processor shall process personal information only under documented instructions;

3) sets out that, with regard to transfers of personal information to a third country or an international organization, unless required to do so by European Union or Member State law to which the organization acting as data processor is subject, that the organization acting as data processor shall inform the organization of any legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

4) ensures that workers authorized to process the personal information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

5) requires the organization acting as the data processer to assist the organization in complying with natural persons' rights;

6) specifies compliance with the legal requirements to notify the organization of any security breaches without any undue delay;

7) requires the organization acting as the data processor to provide appropriate security for the personal information which it will process;

8) enables regular audits of the security arrangements of the organization acting as the data processor during the period in which the organization acting as the data processor has access to the personal information;

9) requires the organization acting as the data processor to obtain the organization's permission to use further subcontractors to process the personal information;

10) requires that contracts with subcontractors of the organization acting as the data processor require the subcontractors to comply with at least the same security and other provisions as the organization acting as the data processor;

11) requires that contracts with the organization acting as the data processor(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 acting as a data processor as specified by the organization; and

12) requires that the organization acting as the data processor makes available to the organization evidence of compliance with the agreement/contract.

8.2.12 Rights of natural persons

Objective: To ensure that the rights of natural persons are taken into consideration and adhered to where appropriate.

8.2.12.1 Responding to rights

The PIMS shall include procedures which ensure that natural persons' rights in relation to their personal information are respected and that requests to exercise such rights are addressed without undue delay and in any event within one month of receipt of the request from the natural person.

The PIMS shall ensure that natural persons are informed in the event of any extension to the one month time period for complying with requests and for supplying the information in an electronic or hard copy format as requested by the natural person. The PIMS shall ensure that any extension to the one month period for complying with a request from a natural person is no longer than a further two months.

NOTE Such rights include access to information, objection to processing, rectification of inaccurate information, erasure and/or restriction on the use of information, data portability and the right not to be subject to automated processing where such processing relates to profiling or that significantly affects the natural person.

The PIMS shall ensure that the procedures include consideration of whether any derogations or exemptions may apply.

8.2.12.2 Access to information

The PIMS shall ensure that the natural person is able, upon request, to have confirmation as to whether or not personal information concerning them is being processed and, where that is the case, to have access to the personal information, to receive a copy of the personal information and the following information, unless a specific derogation applies:

a) the purposes of the processing;

b) the categories of personal information concerned;

c) the recipients or categories of recipient to whom the information has been disclosed, in particular recipients in third countries or international organizations;

d) where possible, the envisaged period for which the personal information will be stored, or if not possible, the criteria used to determine that period;

e) the existence of the right to request rectification or erasure of personal information or restriction of processing of personal information concerning the natural person or to object to such processing.

f) the existence of the right to lodge a complaint with the supervisory authority;

g) where the personal information has not been collected from the data subject, any available information as to the source of the information;

h) the existence of automated decision-making, including profiling (see **8.2.12.8**) and meaningful information about the logic involved, as well as the significance and consequences of such processing for the natural person; and

i) where the personal information is transferred to a third country or international organization, what the appropriate safeguards are that have been put in place.

8.2.12.3 Rectification

The PIMS shall ensure that the natural person is able, without undue delay, to obtain the rectification of inaccurate personal information concerning him or her in accordance with **8.2.9**. These procedures shall also ensure that the natural person is able to have incomplete personal information completed.

8.2.12.4 Erasure

The PIMS shall ensure that requests from natural persons under the "right to erasure" principle are appropriately handled.

The PIMS shall ensure that a natural person has the right to obtain the erasure of personal information about them without undue delay where:

a) the personal information is no longer necessary in relation to the purposes for which it was originally collected or otherwise processed;

b) where the processing was based on consent, the natural person withdraws their consent, and there is no other legal ground for continuing to process the information;

c) the natural person has objected to the processing in question (see **8.2.12.7**) and there are no overriding legitimate grounds for the processing, or the natural person has objected to marketing;

d) the personal information has been unlawfully processed;

e) the personal information needs to be erased to conform to a legal obligation; or

f) the personal information has been collected to offer information society services.

The PIMS shall ensure that, where the information has been made public, appropriate measures are taken to inform other organizations that might be processing the personal information that the natural person has requested the erasure of the information.

8.2.12.5 Restriction of processing

The PIMS shall ensure that the natural person has the right to obtain restriction of processing personal information where:

a) the accuracy of the personal information has been contested by the natural person, for a period enabling the organization to verify the accuracy of personal information;

b) the processing is unlawful and the natural person objects to the erasure of personal information and requests the restriction of its use instead;

c) the organization no longer needs the personal information for the purposes of the processing, but it is required by the natural person for the establishment, exercise or defence of legal claims; or

d) the natural person has objected to processing and the restriction stays in place pending the verification as to whether the legitimate grounds of the organization override those of the natural person.

The PIMS shall ensure that when a restriction is going to be lifted, the natural person is informed before this takes place.

8.2.12.6 Data portability

The PIMS shall ensure that, where the natural person has the right to data portability and the information is being processed by automated means, the natural person is able to have that information transmitted to them, or to another organization they nominate, free of charge and in a structured, commonly used and machine-readable format.

NOTE See Article 20 of the GDPR [1].

8.2.12.7 Objection

The PIMS shall ensure that procedures are in place to consider and respond to requests from a natural person who objects to processing of personal information.

Where a natural person objects to the processing of personal information for the purposes of direct marketing, the PIMS shall ensure that the processing is ceased for that natural person.

8.2.12.8 Automated decision-making, including profiling

The PIMS shall ensure that there are procedures for the identification of processing of personal information that results from automated decision making, including profiling, that might significantly affect a natural person.

The PIMS shall at least ensure that any automated decision can involve human intervention when this is requested by the natural person.

8.2.12.9 Complaints and appeals

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

8.2.13 Maintenance

Objective: To ensure that technology systems are maintained as appropriate.

The PIMS shall 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.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

- what needs to be monitored and measured;
- the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
- when the monitoring and measuring shall be performed;
- when the results from monitoring and measurement shall be analysed and evaluated.

The organization shall retain appropriate documented information as evidence of the results.

The organization shall evaluate the PIMS performance and the effectiveness of the PIMS.

9.2 Internal audit

The organization shall conduct internal audits at planned intervals, and when major changes take place, to provide information on whether the PIMS:

a) conforms to:
   - the organization's own requirements for its PIMS;
   - the requirements of this British Standard;

b) is effectively implemented and maintained.

The organization shall:

1) plan, establish, implement and maintain an audit programme(s) including the frequency, methods, responsibilities, planning requirements and reporting, which shall take into consideration the importance of the processes concerned and the results of previous audits;
2) define the audit criteria and scope for each audit;
3) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

   *NOTE Regular audits by external parties should be considered by larger organizations and those processing high-risk personal information (see **8.2.2.2**).*

4) ensure that the results of the audits are reported to relevant management;
5) retain documented information as evidence of the implementation of the audit programme and the audit results.

The audit programme shall explicitly include any processing of high-risk personal information (see **8.2.2.2**) and shall include any processing of personal information by subcontractors (data processors) (see **8.2.11.10**).

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

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

9.3 Management review

Top management shall review the organization's PIMS, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the PIMS;

c) information on the PIMS performance, including trends in:

- nonconformities and corrective actions;
- monitoring and measurement results;
- audit results;

d) opportunities for continual improvement;

e) feedback from users of the PIMS;

f) risks identified and escalated by workers;

g) records of procedural reviews;

h) results of technology upgrades and/or replacements;

i) formal requests for assessment by regulatory bodies;

j) complaints handling; and

k) security breaches/security incidents that have occurred.

The outputs of the management review shall include decisions related to continual improvement opportunities and any need for changes to the PIMS, for example, identifying modifications to PIMS policy, procedures and/or technology that might affect compliance.

The organization shall retain documented information as evidence of the results of management reviews.

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

10 Improvement

10.1 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity and, as applicable:

- take action to control and correct it;
- deal with the consequences;

b) evaluate the need for action to eliminate the causes of the nonconformity, in order that it does not recur or occur elsewhere, by:

- reviewing the nonconformity;
- determining the causes of the nonconformity;

- determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

e) make changes to the PIMS, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The risk assessment shall be conducted at regular intervals to determine whether the position has changed and any nonconformities need to be rectified (see **8.2.3**).

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 PIAs (see **6.1.4**).

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

Changes that could affect the ability to demonstrate compliance with data protection requirements 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.

The organization shall retain documented information as evidence of:

- the nature of the nonconformities and any subsequent actions taken;
- the results of any corrective action.

10.2 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 any 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.

10.3 Continual improvement

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

Complaints, security breaches, subject access requests, technological advances and other issues shall be used as an aid to improve the effectiveness of the PIMS.

Annex A (informative)
ISO standardized management system

ISO has published many management system standards for topics ranging from quality and environment to information security and business continuity management. Despite sharing common elements, these standards previously had different structures, which sometimes resulted in some confusion or even conflict for users implementing multiple management systems.

In 2012 ISO introduced a mandatory common structure and core text for all international management system standards (Annex SL[6]). Since that date, all new or revised ISO management system standards have been required to use the same high level structure, core text, and common terms and definitions.

This high level structure is intended to assist users and to ensure consistency and compatibility.

It also means that management system auditors can now use a core set of generic requirements across disciplines and industry sectors.

Whilst the high level structure cannot be changed, subclauses and discipline-specific text can be added.

The structure of ISO management system standards now conform to the following:

Clause 1: Scope

Clause 2: Normative references

Clause 3: Terms and definitions

Clause 4: Context of the organization

Clause 5: Leadership

Clause 6: Planning

Clause 7: Support

Clause 8: Operation

Clause 9: Performance evaluation

Clause 10: Improvement

Annex B (informative)
Comparison between the GDPR 2016 and UK practice under the DPA 1998

The GDPR 2016 updates the principles given in the 1995 Data Protection Directive, from which the 1998 Data Protection Act was derived. Some of the areas it updates are

- natural person's rights;
- the EU internal market;
- enforcement of rule;

6 See ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2016 - Annex SL

- international transfers or personal information; and
- global data protection standards.

The significant changes between practice under the 1998 Data Protection Act and the GDPR 2016 are listed in Table B.1.

NOTE The list given in Table B.1 is not exhaustive and highlights some of the more significant changes.

Table B.1 — *Comparison between the GDPR 2016 [1] and UK practice under the DPA 1998 [3]*

	2016 GDPR regulations	**UK practice DPA 1998**
Application	Regulations apply to all EU member states	UK has the DPA 1998 which was derived from the 1995 EU Directive
The same rules for all companies, regardless of where they are established	Companies based outside of Europe have to apply the same rules when they offer goods or services into the EU market	Non-EU based companies are not required to conform to UK DP laws
Fines	Fines of up to 4% of global turnover or EUR 20 000 000, whichever is the greater, can be imposed by the relevant supervisory authority	Fines of up to GBP 500 000 can be imposed by the ICO
Sanctions	Supervisory authorities can issue a definitive or temporary ban on any processing of personal information	The ICO can issue an enforcement notice
Obligations on processors	Processors have direct obligations and liability, and can be enforced against directly	Processors are only subject to the contract terms of the controllers
Data protection by design and default	Data protection safeguards have to be built into products and services from the earliest stage of development, and privacy-friendly default settings are the norm. Privacy impact assessments are mandatory in some circumstances	No existing specific law/ regulation in the DPA, although good practice guidance exists
Documentation requirements	Companies have to record and maintain details of their data and processing activities	A high-level description is notified to the ICO
Data protection officer	Large companies have to employ a specific DPO	There is no equivalent requirement in the DPA
Right to erasure (sometimes known as the "right to be forgotten")	Requests are considered on a case-by-case basis. When a legitimate request is received by a holder of personal information they are to delete the personal information (subject to there not being any legal reason requiring the personal information to be retained)	Requests are considered on a case-by-case basis. This is a right that is usually exercised through the courts

Table B.1 *(continued)*

	2016 GDPR regulations	UK practice DPA 1998
More information about how data is used	Organizations are to provide natural persons with more information about how their personal information is processed, both when they are collected and when they reply to an access request	Organizations are to provide individuals with information on the data collected, purposes of processing, recipients and sources
A right to data portability	Natural persons have the right to have personal information transported between service providers	There is no right to data portability in the DPA
The right to know when one's data has been compromised	Organizations are to notify the national supervisory authority of data breaches which put natural persons at risk. Where appropriate, organizations are to communicate to the individual all breaches of high-risk personal information so that the individual can take appropriate measures	Material data breaches are required to be reported to the ICO for some public sector organizations Other organizations report voluntarily as best practice
Data breach reporting timescales	Data breaches are reported to the supervisory authority within 72 hours and to individuals as soon as possible	Material data breaches are reported within a reasonable period of time

Annex C (informative)
Codes, seals, certifications and trust marks

If an organization decides to adopt a code of conduct or good practice, certificate, seal or trust mark, the organization should check that the scheme is approved and monitored by a competent supervisory authority and that their accreditation is valid and has not been revoked.

NOTE 1 Attention is drawn to articles 40 and 42 of the GDPR [1].

If a code of conduct or good practice is used by the organization, it should be listed as approved and monitored by a competent supervisory authority.

NOTE 2 Attention is drawn to Article 40 (5) of the GDPR [1].

The organization should ensure that processes and procedures used during assessment for issuance of an approved certificate, seal or mark by an approved third party organization, are followed consistently.

NOTE 3 It should be noted that issuance of any certificate, seal or mark is normally based on a "point in time" assessment and the processes and procedures adopted by the organization might, in practice, differ from those assessed for issuing the demonstration of compliance.

In the event of transfer of personal information to an overseas country, conformance to approved codes, certificates, seals or marks might be an appropriate safeguard that can be provided without requiring any specific authorization from the competent supervisory authority.

NOTE 4 Attention is drawn to Article 42 of the GDPR [1]

Bibliography

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

Standards publications

BS EN ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

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

BS EN ISO 14001, *Environmental management systems — Requirements with guidance for use*

BS EN ISO 19011, *Guidelines for auditing management systems*

BS ISO 31000, *Risk management — Principles and guidelines*

BS ISO 55001, *Asset management — Management systems — Requirements*

BS ISO/IEC 20000-1:2011, *Information technology — Service management — Part 1: Service management system requirements*

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

BS ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

PAS 99, *Specification of common management system requirements as a framework for integration*

PD ISO/TR 18128:2014, *Information and documentation — Risk assessment for records processes and systems*

PD ISO Guide 73:2009, *Risk management — Vocabulary*

Other publications

[1] PARLIAMENT AND COUNCIL OF THE EUROPEAN UNION, Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data. OJ L 119, 4.5.2016 p. 1-88.

[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*.

[3] GREAT BRITAIN. *The Data Protection Act 1998*. *The Stationery Office*, *London*, *1998*

[4] GREAT BRITAIN. *The Freedom of Information Act 2000*. *The Stationery Office*, *London*, *2000*

[5] INFORMATION COMMISSIONER'S OFFICE (ICO). The Guide to Data Protection, ICO, February 2016.[7]

Further reading

INFORMATION COMMISSIONER'S OFFICE (ICO). Auditing data protection: A guide to ICO data protection audits (version 3.5), ICO, June 2015.

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

7 The Information Commissioner's Office (ICO) documents, 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: https://ico.org.uk/ [last accessed 28 March 2017]

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)*.

THIS PAGE DELIBERATELY LEFT BLANK

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.