

Contents

	Page
Foreword	ii
0 Introduction	1
0.1 General	1
0.2 Data protection principles	1
0.3 Notification	2
1 Scope	3
2 Normative references	3
3 Terms, definitions and abbreviations	3
4 Context of the organization	8
4.1 Understanding the organization and its context	8
4.2 Understanding the needs and expectations of interested parties	8
4.3 Determining the scope of the personal information management system	8
4.4 Personal information management system	8
5 Leadership	9
5.1 Leadership and commitment	9
5.2 Policy	9
5.3 Organizational roles, responsibilities and authorities	10
5.4 Embedding the PIMS in the organization's culture	11
6 Planning	11
6.1 Actions to address risks and opportunities	11
6.2 PIMS objectives and planning to achieve them	15
7 Support	16
7.1 Resources	16
7.2 Competence	16
7.3 Awareness	16
7.4 Communication	16
7.5 Documented information	16
8 Operation	17
8.1 Operational planning and control	17
8.2 Implementing the PIMS	17
9 Performance evaluation	34
9.1 Monitoring, measurement, analysis and evaluation	34
9.2 Internal audit	34
9.3 Management review	35
10 Improvement	35
10.1 Nonconformity and corrective action	35
10.2 Preventive actions	36
10.3 Continual improvement	36
Annex A (informative) ISO standardized management system	37
Annex B (informative) Comparison between the GDPR 2016 and UK practice under the DPA 1998	37
<i>Table B.1 — Comparison between the GDPR 2016 [1] and UK practice under the DPA 1998 [3]</i>	38
Annex C (informative) Codes, seals, certifications and trust marks	39
Bibliography	41

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.