Date: 2025-04-17

ISO/IEC ~~JTC1/SC 27/WG 5 N9999~~

~~Date: 2024-12-95~~

~~ISO/IEC DIS~~ FDIS 27701~~.2:2024~~:2025(en)

ISO/IEC JTC1/SC 27/WG 5

Secretariat: DIN

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la protection de la vie privée – Exigences et lignes directrices

~~Edited DIS -~~
~~MUST BE USED~~
~~FOR FINAL~~
~~DRAFT~~

~~Document type: International Standard~~
~~Document subtype:~~
~~Document stage: (30) Committee~~
~~Document language: E~~

~~C:\Users\Alan Shipman\Documents\Alan's Documents\ISO\JTC1SC27\27552\SHIPMAN\ISO-IEC_27552_(E) WD2 V5.4.doc STD Version 2.1c2~~

Contents

Page

Foreword viiiviii
Introduction ixix
1 Scope 11
2 Normative references 11
3 Terms, definitions and abbreviations 11
4 Context of the organization 55
4.1 Understanding the organization and its context 55
4.2 Understanding the needs and expectations of interested parties 6
4.3 Determining the scope of the privacy information management system 77
4.4 Privacy information management system 77
5 Leadership 77
5.1 Leadership and commitment 77
5.2 Privacy policy 88
5.3 Roles, responsibilities and authorities 88
6 Planning 88
6.1 Actions to address risks and opportunities 88
6.1.1 General 88
6.1.2 Privacy risk assessment 99
6.1.3 Privacy risk treatment 99
6.2 Privacy objectives and planning to achieve them 11
6.3 Planning of changes 12
7 Support 12
7.1 Resources 12
7.2 Competence 12
7.3 Awareness 12
7.4 Communication 12
7.5 Documented information 13
7.5.1 General 13
7.5.2 Creating and updating documented information 13
7.5.3 Control of documented information 13
8 Operation 14
8.1 Operational planning and control 14
8.2 Privacy risk assessment 14
8.3 Privacy risk treatment 14
9 Performance evaluation 15
9.1 Monitoring, measurement, analysis and evaluation 15
9.2 Internal audit 15
9.2.1 General 15
9.2.2 Internal audit programme 15
9.3 Management review 16
9.3.1 General 16

9.3.2 Management review inputs 16
9.3.3 Management review results 16
10 Improvement 16
10.1 Continual improvement 16
10.2 Nonconformity and corrective action 16
11 Further information on annexes 1717
Annex A (normative) PIMS reference control objectives and controls for PII controllers and PII processors 18
Annex B (normative) Implementation guidance for PII controllers and PII processors 26
B.1 Implementation guidance for PII controllers 26
B.1.1 General 26
B.1.2 Conditions for collection and processing 26
B.1.2.1 Objective 26
B.1.2.2 Identify and document purpose 26
B.1.2.3 Identify lawful basis 26
B.1.2.4 Determine when and how consent is to be obtained 27
B.1.2.5 Obtain and record consent 27
B.1.2.6 Privacy impact assessment 28
B.1.2.7 Contracts with PII processors 28
B.1.2.8 Joint PII controller 29
B.1.2.9 Records related to processing PII 30
B.1.3 Obligations to PII principals 31
B.1.3.1 Objective 31
B.1.3.2 Determining and fulfilling obligations to PII principals 31
B.1.3.3 Determining information for PII principals 31
B.1.3.4 Providing information to PII principals 32
B.1.3.5 Providing mechanism to modify or withdraw consent 32
B.1.3.6 Providing mechanism to object to PII processing 33
B.1.3.7 Access, correction or erasure 33
B.1.3.8 PII controllers' obligations to inform third parties 34
B.1.3.9 Providing copy of PII processed 34
B.1.3.10 Handling requests 35
B.1.3.11 Automated decision making 35
B.1.4 Privacy by design and privacy by default 35
B.1.4.1 Objective 35
B.1.4.2 Limit collection 35

B.1.4.3 Limit processing 36
B.1.4.4 Accuracy and quality 36
B.1.4.5 PII minimization objectives 36
B.1.4.6 PII de-identification and deletion at the end of processing 37
B.1.4.7 Temporary files 37
B.1.4.8 Retention 38
B.1.4.9 Disposal 38
B.1.4.10 PII transmission controls 38
B.1.5 PII sharing, transfer and disclosure 38
B.1.5.1 Objective 38
B.1.5.2 Identify basis for PII transfer between jurisdictions 38
B.1.5.3 Countries and international organizations to which PII can be transferred 39
B.1.5.4 Records of transfer of PII 39
B.1.5.5 Records of PII disclosure to third parties 39
B.2 Implementation guidance for PII processors 40
B.2.1 General 40
B.2.2 Conditions for collection and processing 40
B.2.2.1 Objective 40
B.2.2.2 Customer agreement 40
B.2.2.3 Organization's purposes 40
B.2.2.4 Marketing and advertising use 41
B.2.2.5 Infringing instruction 41
B.2.2.6 Customer obligations 41
B.2.2.7 Records related to processing PII 42
B.2.3 Obligations to PII principals 42
B.2.3.1 Objective 42
B.2.3.2 Comply with obligations to PII principals 42
B.2.4 Privacy by design and privacy by default 42
B.2.4.1 Objective 42
B.2.4.2 Temporary files 42
B.2.4.3 Return, transfer or disposal of PII 43
B.2.4.4 PII transmission controls 43
B.2.5 PII sharing, transfer and disclosure 44

B.2.5.1 Objective 44
B.2.5.2 Basis for PII transfer between jurisdictions 44
B.2.5.3 Countries and international organizations to which PII can be transferred 44
B.2.5.4 Records of PII disclosures to third parties 45
B.2.5.5 Notification of PII disclosure requests 45
B.2.5.6 Legally binding PII disclosures 45
B.2.5.7 Disclosure of subcontractors used to process PII 45
B.2.5.8 Engagement of a subcontractor to process PII 46
B.2.5.9 Change of subcontractor to process PII 46
B.3 Implementation guidance for PII controllers and PII processors 46
B.3.1 Objective 46
B.3.2 General 47
B.3.3 Policies for information security 47
B.3.4 Information security roles and responsibilities 47
B.3.5 Classification of information 48
B.3.6 Labelling of information 48
B.3.7 Information transfer 48
B.3.8 Identity management 48
B.3.9 Access rights 49
B.3.10 Addressing information security within supplier agreements 49
B.3.11 Information security incident management planning and preparation 50
B.3.12 Response to information security incidents 50
B.3.13 Legal, statutory, regulatory and contractual requirements 52
B.3.14 Protection of records 52
B.3.15 Independent review of information security 52
B.3.16 Compliance with policies, rules and standards for information security 53
B.3.17 Information security awareness, education and training 53
B.3.18 Confidentiality or non-disclosure agreements 53
B.3.19 Clear desk and clear screen 54
B.3.20 Storage media 54
B.3.21 Secure disposal or re-use of equipment 54
B.3.22 User endpoint devices 55
B.3.23 Secure authentication 55
B.3.24 Information backup 55
B.3.25 Logging 56
B.3.26 Use of cryptography 56

B.3.27 Secure development life cycle **57**
B.3.28 Application security requirements **57**
B.3.29 Secure system architecture and engineering principles **58**
B.3.30 Outsourced development **58**
B.3.31 Test information **58**
Annex C (informative) **Mapping to ISO/IEC 29100** **59**
Annex D (informative) **Mapping to the General Data Protection Regulation** **62**
Annex E (informative) **Mapping to ISO/IEC 27018 and ISO/IEC 29151** **66**
Annex F (informative) **Correspondence with ISO/IEC 27701:2019** **69**
Bibliography **7676**