

ISO/IEC 15944-17:2024-04 (E)

Information technology - Business operational view - Part 17: Fundamental principles and rules governing Privacy-by-Design (PbD) requirements in an EDI and collaboration space context

Contents

Page

Foreword..... v

Introduction..... vi

1 Scope..... 1

2 Normative references..... 1

3 Terms and definitions..... 2

4 Abbreviated terms..... 18

5 Fundamental privacy protection principles..... 19

5.1 Overview..... 19

5.2 Primary sources of privacy protection principles..... 20

5.3 Exceptions to the application of the privacy protection principles..... 20

5.4 Key eleven (11) privacy protection principles..... 20

5.5 Link to “consumer protection” and “individual accessibility” requirements..... 21

5.6 Requirements for tagging (or labelling) sets of personal information (SPIs) in support of privacy protection requirements (PPR)..... 22

5.7 Requirements for making all personal information (PI) available to the buyer where the buyer is an individual..... 22

6 Fundamental principles and rules governing Privacy by Design (PbD) requirements..... 22

6.1 Overview..... 22

6.2 Fundamental principles of Privacy by Design..... 23

6.2.1 Privacy by Design Principle 1: Proactive not reactive; preventative not remedial..... 23

6.2.2 Privacy by Design Principle 2: Privacy as the Default Setting..... 23

6.2.3 Privacy by Design Principle 3: Privacy Embedded into Design..... 24

6.2.4 Privacy by Design Principle 4: Full Functionality — Positive-Sum, not Zero-Sum..... 25

6.2.5 Privacy by Design Principle 5: End-to-End Safeguards — Full Information Management Life Cycle (ILCM) Protection..... 25

6.2.6 Privacy by Design Principle 6: Visibility and Transparency — Keep it Open..... 26

6.2.7 Privacy by Design Principle 7: Respect for User Privacy — Keep it User-Centric..... 26

6.3 Exceptions to the application of any of the Privacy by Design principles..... 27

6.4 Mapping the eleven (11) Privacy Protection Principles (PPP) to the seven (7) Privacy by Design principles..... 27

7 Collaboration space and privacy protection..... 27

7.1 Overview..... 27

7.2 Collaboration space: Role of consumer (as individual), vendor and regulator..... 28

8 Ensuring that personal information is ‘under the control of’ the organization throughout its ILCM..... 30

8.1 Overview..... 30

8.2 Rules governing the specification of ILCM aspects of personal information..... 31

8.3 Implementing “under the control of” and accountability..... 31

9 Conformance statement..... 32

9.1 Overview..... 32

9.2 Conformance to the ISO/IEC 14662 Open-edi Reference Model and the multipart ISO/IEC 15944 eBusiness standard..... 33

9.3 Conformance to ISO/IEC 15944-17..... 33

9.4 Conformance by agents and third parties to ISO/IEC 15944-17..... 33

Annex A (normative) Consolidated controlled vocabulary definitions and associated terms, as human interface equivalents (HIEs), with cultural adaptability: English and French language equivalency in an IT standardization context	34
Annex B (normative) Consolidated set of rules in existing Parts of ISO/IEC 15944 of particular relevance to PbD as external constraints on business transactions which apply to personal information (PI) in an EDI and collaboration space context	37
Annex C (informative) Mapping ISO/IEC 15944-8 Privacy Protection Principles (PPP) to the Privacy by Design principles	54
Annex D (informative) Exclusions to the scope of ISO/IEC 15944-17	58
Annex E (informative) Fair Information Principles / Fair Information Practices	60
Annex F (informative) Aspects currently not addressed	61
Bibliography	62