ISO 31700-1:2023-01 (E)

Consumer protection - Privacy by design for consumer goods and services - Part 1: High-level requirements

Contents

Page

Foreword ... **vi**

Introduction ... **vii**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 General ... **8**

4.1 Overview ... 8

4.2 Designing capabilities to enable consumers to enforce their privacy rights ... 9

4.2.1 Requirement ... 9

4.2.2 Explanation ... 9

4.2.3 Guidance ... 10

4.3 Developing capability to determine consumer privacy preferences ... 10

4.3.1 Requirement ... 10

4.3.2 Explanation ... 11

4.3.3 Guidance ... 11

4.4 Designing human computer interface (HCI) for privacy ... 11

4.4.1 Requirement ... 11

4.4.2 Explanation ... 12

4.4.3 Guidance ... 12

4.5 Assigning relevant roles and authorities ... 12

4.5.1 Requirement ... 12

4.5.2 Explanation ... 12

4.5.3 Guidance ... 12

4.6 Establishing multi-functional responsibilities ... 13

4.6.1 Requirement ... 13

4.6.2 Explanation ... 13

4.6.3 Guidance ... 13

4.7 Developing privacy knowledge, skill and ability ... 13

4.7.1 Requirement ... 13

4.7.2 Explanation ... 14

4.7.3 Guidance ... 14

4.8 Ensuring knowledge of privacy controls ... 14

4.8.1 Requirement ... 14

4.8.2 Explanation ... 14

4.8.3 Guidance ... 15

4.9 Documentation and information management ... 15

4.9.1 Requirement ... 15

4.9.2 Explanation ... 15

4.9.3 Guidance ... 16

5 Consumer communication requirements ... **16**

5.1 Overview ... 16

5.2 Provision of privacy information ... 17

5.2.1 Requirement ... 17

5.2.2 Explanation ... 17

5.2.3 Guidance ... 17

5.3 Accountability for providing privacy information ... 18

5.3.1 Requirement 18
5.3.2 Explanation 19
5.3.3 Guidance 19
5.4 Responding to consumer inquiries and complaints 19
5.4.1 Requirement 19
5.4.2 Explanation 19
5.4.3 Guidance 19
5.5 Communicating to diverse consumer population 19
5.5.1 Requirement 19
5.5.2 Explanation 19
5.5.3 Guidance 20
5.6 Prepare data breach communications 20
5.6.1 Requirement 20
5.6.2 Explanation 20
5.6.3 Guidance 20
6 Risk management requirements 21
6.1 Overview 21
6.2 Conducting a privacy risk assessment 21
6.2.1 Requirement 21
6.2.2 Explanation 21
6.2.3 Guidance 22
6.3 Assessing privacy capabilities of third parties 22
6.3.1 Requirement 22
6.3.2 Explanation 23
6.3.3 Guidance 23
6.4 Establishing and documenting requirements for privacy controls 23
6.4.1 Requirement: 23
6.4.2 Explanation 23
6.4.3 Guidance 24
6.5 Monitoring and updating risk assessment 24
6.5.1 Requirement 24
6.5.2 Explanation 24
6.5.3 Guidance 24
6.6 Including privacy risks in cybersecurity resilience design 25
6.6.1 Requirement 25
6.6.2 Explanation 25
6.6.3 Guidance 25
7 Developing, deploying and operating designed privacy controls 25
7.1 Overview 25
7.2 Integrating the design and operation of privacy controls into the product development and management lifecycles 26
7.2.1 Requirement 26
7.2.2 Explanation 26
7.2.3 Guidance 26
7.3 Designing privacy controls 27
7.3.1 Requirement 27
7.3.2 Explanation 27
7.3.3 Guidance 27
7.4 Implementing privacy controls 27
7.4.1 Requirement 27
7.4.2 Explanation 27
7.4.3 Guidance 27
7.5 Designing privacy control testing 28
7.5.1 Requirement 28
7.5.2 Explanation 28
7.5.3 Guidance 28
7.6 Managing the transition of privacy controls 29
7.6.1 Requirement 29
7.6.2 Explanation 29
7.6.3 Guidance 29
7.7 Managing the operation of privacy controls 30
7.7.1 Requirement 30
7.7.2 Explanation 30

7.7.3 Guidance 30
7.8 Preparing for and managing a privacy breach 30
7.8.1 Requirement 30
7.8.2 Explanation 31
7.8.3 Guidance 31
7.9 Operating privacy controls for the processes and products upon which the product in scope depends throughout the PII lifecycle 31
7.9.1 Requirement 31
7.9.2 Explanation 31
7.9.3 Guidance 31
8 End of PII lifecycle requirements 32
8.1 Overview 32
8.2 Designing privacy controls for retirement and end of use 32
8.2.1 Requirement 32
8.2.2 Explanation 32
8.2.3 Guidance 32
Bibliography 34