

ISO/IEC 15944-8:2012-04 (E)

Information technology - Business Operational View - Part 8: Identification of privacy protection requirements as external constraints on business transactions

Contents		Page
Foreword		vii
0	Introduction	viii
0.1	Purpose and overview	viii
Operational View (BOV"))		x
0.2	Introducing the use of "Person", "organization" and "party" in the context of business transaction and commitment exchange	xi
0.3	Importance and role of terms and definitions	xiii
0.4	Importance of the two classes of constraints of the Business Transaction Model (BTM) ..	xiii
0.5	Need for a standard based on rules and guidelines	xiv
0.6	Use of "jurisdictional domain", and "jurisdiction" (and "country") in the context of business transaction and commitment exchange	xv
0.7	Use of "identifier" as "identifier (in business transaction)" to prevent ambiguity	xvi
0.8	Use of "privacy protection" in the context of business transaction and commitment exchange	xvi
0.9	Organization and description of this document	xvii
1	Scope	1
1.1	Statement of scope	1
1.2	Exclusions	2
1.2.1	Functional Services View (FSV)	2
1.2.2	Internal behaviour of organizations (and public administration)	2
1.2.3	"organization Person"	2
1.2.4	Overlap of and/or conflict among jurisdictional domains as sources of privacy protection requirements	2
1.2.5	Publicly available personal information	3
1.3	Aspects currently not addressed	4
1.4	IT-systems environment neutrality	7
2	Normative references	9
2.2	Referenced specifications	10
3	Terms and definitions	11
4	Symbols and abbreviations	41
5	Fundamental principles and assumptions governing privacy protection requirements in business transactions involving individuals (external constraints perspective)	43
5.1	Introduction	43
5.2	Exceptions to the application of the privacy protection principles	46
5.3	Fundamental Privacy Protection Principles	46
5.3.1	Privacy Protection Principle 1: Preventing Harm	46
5.3.2	Privacy Protection Principle 2: Accountability	47
5.3.3	Privacy Protection Principle 3: Identifying Purposes	50
5.3.4	Privacy Protection Principle 4: Informed Consent	50
5.3.5	Privacy Protection Principle 5: Limiting Collection	52
5.3.6	Privacy Protection Principle 6: Limiting Use, Disclosure and Retention	54
5.3.7	Privacy Protection Principle 7: Accuracy	57
5.3.8	Privacy Protection Principle 8: Safeguards	58
5.3.9	Privacy Protection Principle 9: Openness	59

5.3.10	Principle Protection Principle 10: Individual Access	60
5.3.11	Privacy Protection Principle 11: Challenging Compliance	62
5.4	Requirement for tagging (or labelling) data elements in support of privacy protection requirements	63
6	Collaboration space and privacy protection	65
6.1	Introduction	65
6.2	Basic Open-edi collaboration space: Buyer and seller	65
6.3	Collaboration space: The role of buyer (as individual), seller and regulator	66
7	Public policy requirements of jurisdictional domains	69
7.1	Introduction	69
7.2	Jurisdictional domains and public policy requirements	69
7.2.1	Privacy protection	70
7.2.2	Person and external constraints: Consumer protection	72
7.2.3	Individual accessibility	73
7.2.4	Human rights	74
7.2.5	Privacy as a right of an "individual" and not the right of an organization or public administration	74
8	Principles and rules governing the establishment, management and use of identities of an individual	77
8.1	Introduction	77
8.2	Rules governing the establishment of personae, identifiers and signatures of an individual	78
8.3	Rules governing the assignment of unique identifiers to an individual by Registration Authorities (RAs)	84
8.4	Rules governing individual identity, authentication, recognition, and use	85
8.5	Legally recognized individual identifies (LRIs)	90
9	Person component - individual sub-type	93
9.1	Introduction	93
9.2	Role qualification of a Person as an individual	93
9.3	Persona and legally recognized names (LRNs) of an individual	94
9.4	Truncation of legally recognized names of individuals	94
9.5	Rules governing anonymization of individuals in a business transaction	95
9.6	Rules governing pseudonymization of personal information in a business transaction	97
10	Process component	99
10.1	Introduction	99
10.2	Planning	99
10.3	Identification	99
10.4	Negotiation	100
10.5	Actualization	100
10.6	Post-Actualization	100
11	Data component	101
11.1	Introduction	101
11.2	Rules governing the role of Business Transaction Identifier (BTI) in support of privacy protection requirements	101
11.3	Rules governing state of change management of business transactions in support of privacy protection requirements	102
11.4	Rules governing records retention of personal information in a business transaction	102
11.5	Rules governing time/date referencing of personal information in a business transaction	103
12	Template for identifying privacy protection requirements on business transactions	105
12.1	Introduction and basic principles	105
12.2	Template structure and contents	105
12.3	Template for specifying the scope of an Open-edi scenario	106
12.4	Consolidated template of attributes of Open-edi scenarios, roles and information bundles	113

13	Conformance statement	119
13.1	Introduction	119
Annex A (normative) Consolidated list of terms and definitions with cultural adaptability: ISO English and ISO French language equivalency		120
A.1	Introduction	120
A.2	ISO English and ISO French	120
A.3	Cultural adaptability and quality control	120
A.4	Organization of Annex A - Consolidated list in matrix form	121
relevance to privacy protection requirements as external constraints on business transactions		185
B.1	Introduction	185
B.2	Organization of Annex B: Consolidated list in matrix form	185
supporting privacy protection requirements		186
relevance to supporting privacy protection requirements		189
relevance to supporting privacy protection requirements		190
relevance to supporting privacy protection requirements		194
Annex C (normative) Business Transaction Model (BTM): Classes of constraints		200
Annex D (normative) Integrated set of information life cycle management (ILCM) principles in support of information law compliance		205
D.1	Introduction	205
D.2	Purpose	205
D.3	Approach	206
D.4	Integrated set of information life cycle management (ILCM) principles	206
Annex E (normative) Key existing concepts and definitions applicable to the establishment, management, and use of identities of a single individual		209
Annex F (normative) Coded domains for specifying state change and record retention management in support of privacy protection requirements		211
F.1	Introduction	211
F.2	State changes	212
F.2.1	Introduction	212
F.2.2	Specification of state changes allowed to personal information	213
F.2.3	Store change type	214
F.3	Records retention	216
F.4	Records destruction	218
Bibliography		220
Figures Page Figure 1 -- Open-edi environment - Open-edi Reference Model		ix
Figure 2 -- Integrated view - Business operational requirements: External constraints focus		xi
Figure 3 -- Primary sources for privacy protection principles		45
Figure 4 -- Concept of a business collaboration		66
Figure 5 -- Privacy collaboration space (of a business transaction) including the role of a regulator. 68		
Figure 6 -- Common public policy requirements, i.e., external constraints, applying to a business transaction where the "buyer" is an "individual"		70

Figure 7 -- Illustration of relationships of links of a (real world) individual to (its) persona (e) to identification schemas and resulting identifiers to associated Person signatures -- in the context of different business transactions and governing rules	80
Figure 8 -- Illustration of range of links between personae and identifiers of an individual identity(ies) of an individual	86
Figure 9 -- Illustration of two basic options for establishment of a recognized individual identity (rii) 89 Figure C.1 -- Business Transaction Model - Fundamental components (Graphic illustration)	200
Figure C.2 -- UML-based Representation of Figure C.1 -- Business Transaction Model	201
Figure C.3 -- Business Transaction Model: Classes of constraints	204
Tables Page Table 1 -- Template for specifying the scope of an Open-edi scenario	106
Table 2 -- Consolidated template of attributes of Open-edi scenarios, roles and information bundles	113
Information Bundles and Semantic Components	213
Semantic Components	215
Responsibility	216