

ISO/IEC 15944-12:2020-05 (E)

Information technology - Business operational view - Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	2
4	Abbreviated terms	30
5	Fundamental privacy protection principles	31
5.1	Overview	31
5.2	Primary sources of privacy protection principles	31
5.3	Key eleven (11) privacy protection principles	32
5.4	Link to “consumer protection” and “individual accessibility” requirements (see ISO/IEC 15944-8:2012, 6.3)	33
5.5	Privacy protection principles in the context of ILCM requirements	34
5.6	Requirement for tagging (or labelling) sets of personal information (SPIs) in support of privacy protection requirements (PPR) in accordance with ISO/IEC 15944-8:2012, 5.4	34
5.7	Requirements for making all personal information (PI) available to the buyer where the buyer is an individual	34
5.8	Rules governing ILCM aspects of personal information profiles (PIPs)	35
6	Integrated set of information life cycle management (ILCM) principles in support of information law and privacy protection requirements (PPR)	36
6.1	Primary purpose of Clause 6	36
6.2	Information life cycle management (ILCM) principles that support privacy protection requirements (PPR)	38
6.2.1	Compliance with privacy protection requirements (PPR) and associated information law requirements	38
6.2.2	Direct relevance, informed consent and openness	38
6.2.3	Ensuring that personal information is “under the control of” the organization throughout its ILCM	40
6.2.4	Limiting use, disclosure and retention	41
6.2.5	Timely, accurate, relevant	43
6.2.6	Data integrity and quality	45
6.2.7	Safeguards for non-authorized disclosure requirements	45
6.2.8	Back-up, retention and archiving	46
6.2.9	Disposition and expungement	47
6.2.10	Organizational archiving	47
6.2.11	Historical, statistical and/or research value	47
6.3	Requirement for tagging (or labelling) data elements in support of privacy protection requirements (PPR)	49
7	Rules governing ensuring accountability for and control of personal information (PI)	49
7.1	Purpose	49
7.2	Key aspects of Open-edi requirements	49
7.3	Key aspects of “under the control of”	50
7.4	“under the control of” in support of PPR and in an ILCM context	50
7.5	Implementing “under the control of” and accountability	51

8	Rules governing the specification of ILCM aspects of personal information	56
8.1	Overview	56
8.2	Rules governing establishing ILCM responsibilities for personal information (PI).....	57
8.3	Rules governing establishing specifications for retention of personal information (PI) — applicable “SRI retention triggers”	59
8.4	Rules governing identification and specification of state changes of personal information (PI)	62
8.4.1	General requirements.....	62
8.4.2	Specification of state changes allowed to personal information (PI).....	63
8.4.3	Specification of store change type	65
8.4.4	Rules governing specification of source of state changes	67
8.5	Rules governing disposition of personal information (PI)	68
8.6	Rules governing the establishment and maintenance of record retention and disposal schedules (RRDS) for sets of personal information (SPIs).....	71
9	Data conversion, data migration and data synchronization	73
9.1	Purpose.....	73
9.2	Rules governing data conversion of set(s) of personal information (SPI)	74
9.3	Rules governing requirements for data synchronization of sets of personal information (SPI)	74
10	Rules governing EDI of personal information (PI) between primary ILCM Person, i.e., the seller, and its “agent”, “third party” and/or “regulator”	76
10.1	General requirements	76
10.2	ILCM rules pertaining to use of an “agent”	77
10.3	ILCM rules pertaining to use of a “third party”	78
10.4	ILCM rules pertaining to involvement of a “regulator”	78
11	Conformance statement	79
11.1	Overview	79
11.2	Conformance to the ISO/IEC 14662 Open-edi reference model and the ISO/IEC 15944 series.....	79
11.3	Conformance to ISO/IEC 15944-12	80
11.4	Conformance by agents and third parties to ISO/IEC 15944-12.....	80
Annex A	(normative) Consolidated list of terms and definitions with cultural adaptability: ISO English and ISO French language equivalency	81
Annex B	(normative) Consolidated set of rules in the ISO/IEC 15944 series of particular relevance to privacy protection requirements (PPR) as external constraints on business transactions which apply to personal information (PI) in an ILCM requirements context	96
Annex C	(informative) Business transaction model (BTM): Classes of constraints	112
Annex D	(informative) Linking ILCM to process phases of a business transaction	116
Annex E	(informative) Generic approach to ILCM decisions in a PPR context — ILCM compliance decision tree	118
Annex F	(informative) Generic approach to identification of properties and behaviours of personal information (PI) as transitory records and their disposition/expungement	121
Annex G	(informative) Notes on referential integrity and privacy protection transactional integrity (PPTI) in Open-edi among IT systems	123
Annex H	(informative) Exclusions to the scope of ISO/IEC 15944-12	125
Annex I	(informative) Aspects not currently addressed in this document	127
Annex J	(informative) List of parts of the ISO/IEC 15944 series	130
Annex K	(informative) Abstract of ISO/IEC 15944-12: ISO English, ISO French and ISO Chinese	131
	Bibliography	134