
**Information technology — Business
operational view —**

Part 12:

**Privacy protection requirements
(PPR) on information life cycle
management (ILCM) and EDI of
personal information (PI)**

Technologies de l'information — Vue opérationnelle d'affaires —

*Partie 12: Exigences en matière de protection de la vie privée (PPR)
relatives à la gestion du cycle de vie de l'information (ILCM) et de
l'EDI des renseignements personnels (PI)*

ISO/IEC 15944-12:2020

<https://standards.iteh.ai/catalog/standards/iso/82aa03bb-58f4-4b17-9d7e-f81c29e8d1da/iso-iec-15944-12-2020>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/IEC 15944-12:2020](https://standards.iteh.ai/catalog/standards/iso/82aa03bb-58f4-4b17-9d7e-f81c29e8d1da/iso-iec-15944-12-2020)

<https://standards.iteh.ai/catalog/standards/iso/82aa03bb-58f4-4b17-9d7e-f81c29e8d1da/iso-iec-15944-12-2020>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see <http://patents.iec.ch>).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 32, *Data management and interchange*.

A list of all parts in the ISO/IEC 15944 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

NOTE This document is intended to be used in conjunction with ISO/IEC 14662, ISO/IEC 15944-1, ISO/IEC 15944-5 and ISO/IEC 15944-8.

0.1 Purpose and overview

Modelling business transactions using scenarios and scenario components includes specifying the applicable constraints on the data content using explicitly stated rules. ISO/IEC 14662 identifies two basic classes of constraints, "internal constraints" and "external constraints". External constraints apply to most business transactions. External constraints have governance over any processing of personal information including that exchanged among parties to a business transaction and doing so from an information life cycle management (ILCM) requirements perspective.

Jurisdictional domains are the primary source of external constraints on business transactions (see [Annex C](#)). Privacy protection requirements in turn are a common requirement of most jurisdictional domains, although they may also result from explicit scenario demands from or on the parties involved in a business transaction. (Requirements for secrecy or confidentiality are not addressed in this document, unless they are implicitly needed to apply privacy protection requirements to data).

The focus of this document is on any kind of recorded information concerning identifiable living individuals as buyers in a business transaction or whose personal information is used in a business transaction or any type of commitment exchange.

This document describes the added business semantic descriptive techniques needed to support information life cycle management (ILCM) aspects as part of privacy protection requirements when modelling business transactions using the external constraints of jurisdictional domains. ILCM aspects are central to the ability to ensure that privacy protection requirements (PPR) are passed on and supported among all the parties to a business transaction using EDI.

This document applies to any organization which receives, creates, process, maintains, communicates, etc. personal information (PI) and, in particular, to those who receive, create, capture, maintain, use, store or dispose of sets of recorded information (SRIs) electronically. This document applies to private and public sector activities of Persons irrespective of whether such activities are undertaken on a for-profit or not-for-profit basis.

This document is intended for use by those organizations to which privacy protection requirements apply and who therefore need to ensure that the recorded information (electronic records and transactions) in their IT Systems is trustworthy, reliable and recognized as authentic. Typical users of this document include

- a) managers of private and public sector organizations;
- b) IT systems and records/information management system professionals;
- c) privacy protection officers (PPOs) and other personnel in organizations, including those responsible for risk management; and
- d) legal professionals and others within an organization responsible for information law compliance by the organization.

0.2 Use of ISO/IEC 14662 and ISO/IEC 15944

0.2.1 ISO/IEC 14662: Open-edi reference model¹⁾

ISO/IEC 14662²⁾ states the conceptual architecture necessary for carrying out electronic business transactions among autonomous parties. That architecture identifies and describes the need to have two separate and related views of the business transaction.

The first is the business operational view (BOV). The second is the functional service view (FSV). [Figure 1](#), taken from ISO/IEC 14662:2010, Figure 1, illustrates the Open-edi environment. (For definitions of the terms used, see [Clause 3](#).)

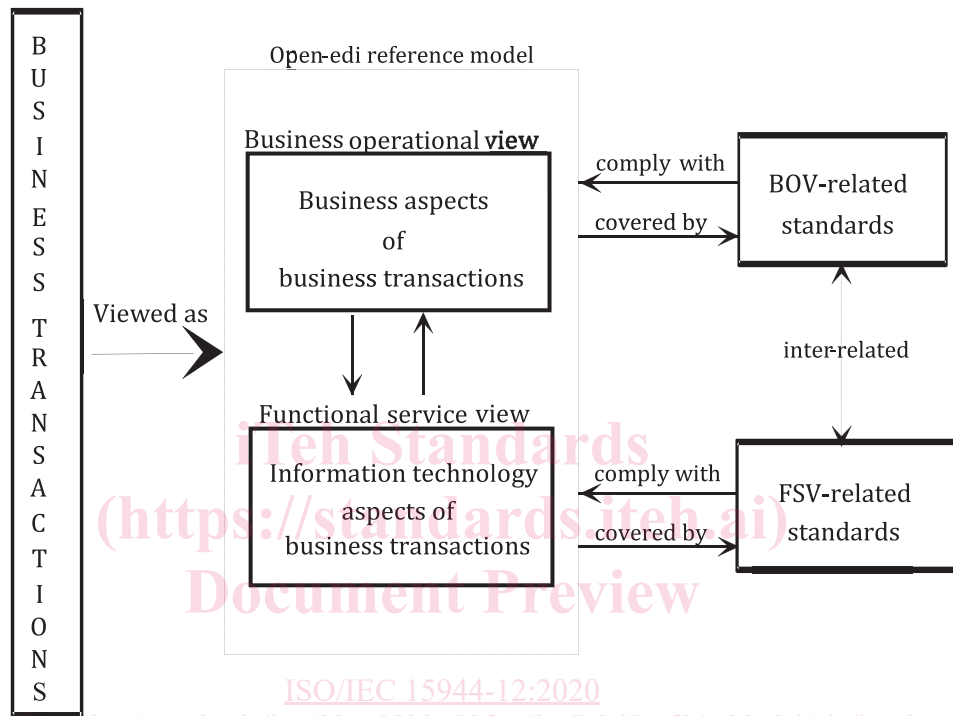


Figure 1 — Open-edi reference model environment

ISO/IEC 15944 is a multipart eBusiness standard which is based on and focuses on the BOV perspective of the ISO/IEC 14662 Open-edi reference model. This document focuses on addressing commonly definable aspects of external constraints that relate to information life cycle management (ILCM) in a privacy and data protection³⁾ context when the source is a jurisdictional domain. A useful characteristic of external constraints is that, at the sectoral level, national and international levels, etc., focal points and recognized authorities often already exist. The rules and common business practices in many sectoral areas are already known. Use of this document (and related standards) addresses the transformation of these external constraints (business rules) into specified, registered, and re-useable scenarios and scenario components.

1) The Memorandum of Understanding between ISO, IEC, ITU and UN/ECE (2000) concerning standardization in the field of electronic business is based on this *Model*. See https://www.unece.org/fileadmin/DAM/oes/MOU/2000/24March2000_IEC_ISO_ITU.pdf.

2) ISO/IEC 14662 is freely-available at <https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>.

3) "Privacy protection" is the common set of worldwide requirements. In the European Union, "data protection" is the equivalent concept (used mainly due to historical reasons). In many other non-European countries, (Australia, Canada, New Zealand, USA, etc., "privacy" is the legal term used in applicable legislation and pursuant regulations. This is because "privacy" applies to not just "data" but any form of recorded information containing "personal information". Thus from an international standards perspective "privacy protection" integrates "privacy" and "data protection" requirements. In many other countries, "privacy" is the legal term used in applicable legislation and pursuant regulations.