



**International
Standard**

ISO/IEC 15944-8

**Information technology — Business
operational view —**

Part 8:

**Identification of privacy
protection requirements as
external constraints on business
transactions**

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

*Partie 8: Identification des exigences de protection de la vie
privée en tant que contraintes externes sur les transactions
d'affaires*

**Second edition
2026-02**

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

ISO/IEC 15944-8:2026

<https://standards.iteh.ai/catalog/standards/iso/ec028739-f3e7-4e75-805c-c5c72b4e706b/iso-iec-15944-8-2026>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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
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	32
5 Fundamental principles and assumptions governing privacy protection requirements in business transactions involving individuals (external constraints perspective)	34
5.1 General	34
5.2 Exceptions to the application of the privacy protection principles	36
5.3 Fundamental privacy protection principles	36
5.3.1 General	36
5.3.2 Privacy protection principle 1: Preventing harm	36
5.3.3 Privacy protection principle 2: Accountability	37
5.3.4 Privacy protection principle 3: Identifying purposes	40
5.3.5 Privacy protection principle 4: Informed Consent	40
5.3.6 Privacy protection principle 5: Limiting collection	42
5.3.7 Privacy protection principle 6: Limiting use, disclosure and retention	43
5.3.8 Privacy Protection Principle 7: Accuracy	46
5.3.9 Privacy Protection Principle 8: Safeguards	46
5.3.10 Privacy Protection Principle 9: Openness	47
5.3.11 Principle Protection Principle 10: Individual Access	48
5.3.12 Privacy Protection Principle 11: Challenging compliance	50
5.4 Requirement for tagging (or labelling) data elements in support of privacy protection requirements	51
6 Collaboration space and privacy protection	52
6.1 General	52
6.2 Basic Open-edi collaboration space: Buyer and seller	52
6.3 Collaboration space: The role of buyer (as individual), seller and regulator	54
7 Public policy requirements of jurisdictional domains	55
7.1 General	55
7.2 Jurisdictional domains and public policy requirements	55
7.2.1 General	55
7.2.2 Privacy protection	56
7.2.3 Person and external constraints: Consumer protection	58
7.2.4 Individual accessibility	59
7.2.5 Human rights	60
7.2.6 Privacy as a right of an “individual” and not the right of an organization or public administration	60
8 Principles and rules governing the establishment, management and use of identities of an individual	61
8.1 General	61
8.2 Rules governing the establishment of personae, identifiers and signatures of an individual	62
8.3 Rules governing the assignment of unique identifiers to an individual by Registration Authorities (RAs)	67
8.4 Rules governing individual identity, authentication, recognition, and use	68
8.5 Legally recognized individual identifies (LRIIs)	72
9 Person component — Individual sub-type	73
9.1 General	73
9.2 Role qualification of a Person as an individual	73

9.3	Persona and legally recognized names (LRNs) of an individual.....	74
9.4	Truncation of legally recognized names of individuals.....	75
9.5	Rules governing anonymization of individuals in a business transaction.....	75
9.6	Rules governing pseudonymization of personal information in a business transaction.....	76
10	Process component.....	77
10.1	General.....	77
10.2	Planning.....	77
10.3	Identification.....	78
10.4	Negotiation.....	78
10.5	Actualization.....	78
10.6	Post-actualization.....	78
11	Data component.....	79
11.1	General.....	79
11.2	Rules governing the role of Business Transaction Identifier (BTI) in support of privacy protection requirements.....	79
11.3	Rules governing state of change management of business transactions in support of privacy protection requirements.....	80
11.4	Rules governing records retention of personal information in a business transaction.....	80
11.5	Rules governing time/date referencing of personal information in a business transaction.....	81
12	Template for identifying privacy protection requirements on business transactions.....	82
12.1	Introduction and basic principles.....	82
12.2	Template structure and contents.....	82
12.3	Template for specifying the scope of an Open-edi scenario.....	83
12.4	Consolidated template of attributes of Open-edi scenarios, roles and information bundles.....	91
13	Conformance statement.....	94
13.1	General.....	94
13.2	Conformance to the ISO/IEC 14662 Open-edi Reference Model and the multipart ISO/IEC 15944 eBusiness standard.....	95
13.3	Conformance to ISO/IEC 15944-8.....	95
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.....	96
Annex B (normative)	Consolidated set of rules in existing parts of ISO/IEC 15944 of particular relevance to privacy protection requirements as external constraints on business transactions.....	99
Annex C (normative)	Business Transaction Model (BTM): Classes of constraints.....	111
Annex D (normative)	Integrated set of information life cycle management (ILCM) principles in support of information law compliance.....	115
Annex E (normative)	Key existing concepts and definitions applicable to the establishment, management, and use of identities of a single individual.....	118
Annex F (normative)	Coded domains for specifying state change and record retention management in support of privacy protection requirements.....	120
Annex G (informative)	Abstract of ISO/IEC 15944-8.....	128
Annex H (Informative)	Exclusions to the scope of ISO/IEC 15944-8.....	129
Annex I (Informative)	Aspects not currently addressed in this document.....	130
Bibliography.....		132

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Technical Committee ISO/IEC JTC1, *Information technology*, Subcommittee SC 32, *Data management and interchange*.

This second edition cancels and replaces the first edition (ISO/IEC 15944-8:2012), which has been technically revised.

The main changes are as follows:

- [Clause 1](#) (Scope) has been amended to move the detailed description of "Exclusions" and "Aspects currently not addressed" to two separate informative annexes;
- definitions in [Clause 3](#) have been updated to be aligned with other referenced source definitions;
- clauses and annexes have been aligned to changes in ISO/IEC Directives, Part 2;
- minor edits of [Clause 5](#), [Clause 9](#), [Clause 12](#), all annexes and the bibliography.

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

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 and www.iec.ch/national-committees.

Introduction

0.1 Purpose and overview

0.1.1 General

Modelling business transactions using scenarios and scenario components is done by specifying the applicable constraints on the data content using explicitly stated rules. The *Open-edī Reference Model* identified two basic classes of constraints, "internal constraints" and "external constraints". External constraints apply to most business transactions. (See Clause 0.4 and [Annex C](#).)

Jurisdictional domains are the primary source of external constraints on business transactions. 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.

This document is a BOV-related standard which addresses basic (or primitive) requirements of a privacy protection environment, as legal requirements represented through jurisdictional domains, on business transactions, and also integrates the requirements of the information technology and telecommunications environments.

This document contains a methodology and tool for specifying common classes of external constraints through the construct of "jurisdictional domains". It meets the requirements set in ISO/IEC 15944-1 and ISO/IEC 15944-2 through the use of explicitly stated rules, templates, and Formal Description Techniques (FDTs).

In addition to the existing strategic directions of "portability" and "interoperability", the added strategic direction of ISO/IEC JTC 1 of "cultural adaptability" is also supported in this document. The external constraints of jurisdictional domains as a primary factor in choice and use of language and application of public policy are also addressed.

0.1.2 ISO/IEC 14662

ISO/IEC 14662¹⁾ states the conceptual architecture and framework 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). ISO/IEC 14662:2010, Figure 1 illustrates the Open-edī environment. (For definitions of the terms used in [Figure 1](#), please see [Clause 3](#).)

1) The ISO/IEC 14462 *Open-edī Reference Model* serves as the basis of the 2000 Memorandum of Understanding (MOU) among ISO, IEC, ITU and the UN/ECE concerning standardization in the field of electronic business. {See <https://www.itu.int/ITU-T/e-business/files/mou.pdf>}

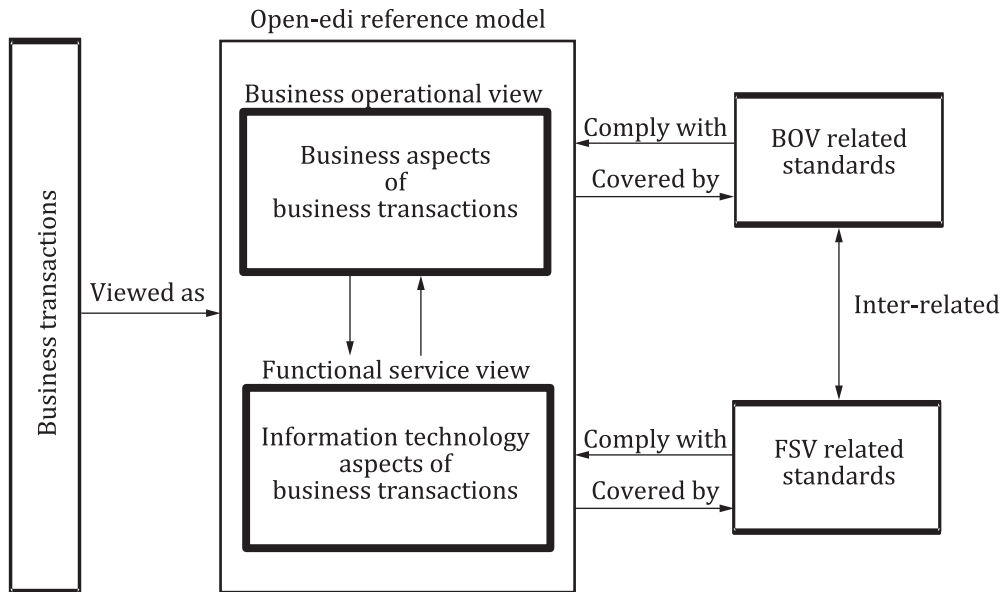


Figure 1 — Open-edi environment — Open-edi Reference Model

ISO/IEC 14662:2010, Clause 5 states:

"The intention is that the sending, by an Open-edi Party, of information from a scenario, conforming to Open-edi standards, shall allow the acceptance and processing of that information in the context of that scenario by one or more Open-edi Parties by reference to the scenario and without the need for agreement.

However, the legal requirements and/or liabilities resulting from the engagement of an organization in any Open-edi transaction may be conditioned by the competent legal environment(s) of the formation of a legal interchange agreement between the participating organizations. Open-edi Parties need to observe rule-based behaviour and possess the ability to make commitments in Open-edi, (e.g. business, operational, technical, legal, and/or audit perspectives)".

In addition, ISO/IEC 14662:2010, Figure A.1 illustrates the Relationships of Open-edi standardization areas with other standards and importance of the legal environment. This document is a BOV standard which focuses on the legal environment for the application of privacy protection from an Open-edi perspective, and, as required follow-up standards development in support of the "Open-edi Reference Model".

ISO/IEC 15944-5 is used to identify the means by which laws and regulations impacting scenarios and scenario components, as external constraints, may be modelled and represented. The primary source of these external constraints is jurisdictional domains.

ISO/IEC 15944-1 creates rules for creating the specification of external constraints when modelling business transactions through scenarios, scenario attributes and scenario components. Several parts of the ISO/IEC 15944 series are used as input to this document. The rules are consolidated in this document in [Annex B](#).

ISO/IEC 15944-1:2025, 7.1 states:

"The approach taken is that of identifying the most primitive common components of a business transaction and then moving from the general to the more detailed, the simplest aspects to the more complex, from no external constraints on a business transaction to those which incorporate external constraints, from no special requirements on functional services to specific requirements, and so on".

This document focuses on addressing commonly definable aspects of external constraints that relate to privacy protection 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.