

Date: 2023-12-19

Reference number of document: **ISO/IEC FDIS 15944-17**

Committee identification: ISO/IEC JTC 001 1/SC 32/AWG 01

Secretariat: JTC1/SC32 ANSI

Date: 2024-01-10

Style Definition

Formatted: zzCover large, Space Before: 0 pt, After: 0 pt

Formatted

Formatted: Font: 11 pt, French (Switzerland)

Formatted

Formatted: Font: 11 pt, French (Switzerland)

Formatted: Font: 11 pt

Formatted: Space After: 0 pt

Information technology — Business Operational View — operational view —

Formatted: Font: 16 pt

**Part 17:
Fundamental principles and rules governing Privacy-by-Design (PhDPbD) requirements in an EDI and collaboration space context**

Formatted: Regular, Font: 16 pt, Bold

Formatted: Cover Title_A2, Space After: 0 pt, Tab stops: Not at 10.39 cm

Formatted: Font: 16 pt, Bold

Formatted

Technologies de l'information — Vue opérationnelle d'affaires — Partie 17: JTC1/SC32
<https://standards.iteh.ai/catalog/standards/iso/15944-17>

**Edited DIS -
MUST BE USED
FOR FINAL
DRAFT**

FDIS stage

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

ISO/IEC FDIS 15944-17

<https://standards.iteh.ai/catalog/standards/iso/1e326f31-39fc-474a-bcca-7bf4900a4a3c/iso-iec-fdis-15944-17>

Edited DIS -
MUST BE USED
FOR FINAL
DRAFT

© ISO [year]/IEC 2024

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 - copyright office

CP 401 • Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Phone: + 41 22 749 01 11

Email: copyright@iso.org

E-mail: copyright@iso.org

Website: www.iso.org

Published in Switzerland

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Font color: Auto, English (United Kingdom)

Formatted: zzCopyright address

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Font color: Auto, English (United Kingdom)

Formatted: zzCopyright address

Formatted: Font color: Auto, French (Switzerland)

Formatted: French (Switzerland)

Formatted: Font color: Auto

Formatted: zzCopyright address

Formatted: Font color: Auto

Formatted: Font color: Auto, English (United Kingdom)

Formatted: Font color: Auto, English (United Kingdom)

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

ISO/IEC FDIS 15944-17

<https://standards.itih.ai/catalog/standards/iso/1e326f31-39fc-474a-bcca-7bf4900a4a3c/iso-iec-fdis-15944-17>

~~Edited DIS -~~
~~MUST BE USED~~
~~FOR FINAL~~
~~DRAFT~~

© ISO/IEC 2023 - All rights reserved

Contents—Page

Introduction	xii
0.1 Purpose and overview	xii
0.2 Use of ISO/IEC 14662 and ISO/IEC 15944	xii
0.2.1 ISO/IEC 14662 "Open edi Reference Model"	xii
0.2.2 ISO/IEC 15944-1 Business operational view (BOV) operational aspects of Open edi for implementation	xiv
0.2.3 Links to ISO/IEC 15944-5, ISO/IEC 15944-8, ISO/IEC 15944-4 and ISO/IEC 15944-12	xvii
0.3 Importance and role of terms and definitions	xvii
0.4 Basic rules and guidelines	xviii
0.5 Use of "Person", "organization", "individual" and "party" in the context of business transaction and commitment exchange	xviii
0.6 Use of "identifier" (in a business transaction) and roles of an individual	xviii
0.7 Use of "jurisdictional domain" in the context of privacy protection requirements and Privacy by Design	xviii
0.8 Use of "privacy protection" in the context of business transaction, EDI and any type of commitment exchange	xix
0.9 Use of "set of recorded information" (SRI) and "set of personal information" (SPI) versus record, document, message, data, etc.	xix
0.10 Aspects currently not addressed	xix
0.11 IT-systems environment neutrality	xx
0.12 Organization and description of this document	xx
1 Scope	1
2 Normative references	3
3 Terms and definitions	5
4 Abbreviated terms	25
5 Fundamental privacy protection principles	27
5.1 Overview	28
5.2 Primary sources of privacy protection principles	29
5.3 Exceptions to the application of the privacy protection principles	30
5.4 Key eleven (11) privacy protection principles	30
5.5 Link to "consumer protection" and "individual accessibility" requirements	31
5.6 Requirements for tagging (or labelling) sets of personal information (SPIs) in support of privacy protection requirements (PPR)	32
5.7 Requirements for making all personal information (PI) available to the buyer where the buyer is an individual	32
6 Fundamental principles and rules governing Privacy by Design (PbD) requirements	32
6.1 Overview	32

Formatted: Font: Bold, Font color: Auto

Edited DIS
MUST BE USED
FOR FINAL
DRAFT

~~6.2 Fundamental principles of Privacy by Design 33~~

~~6.2.1 Privacy by Design Principle 1: Proactive not reactive; preventative not remedial 33~~

~~6.2.2 Privacy by Design Principle 2: Privacy as the Default Setting 34~~

~~6.2.3 Privacy by Design Principle 3: Privacy Embedded into Design 35~~

~~6.2.4 Privacy by Design Principle 4: Full Functionality – Positive Sum, not Zero Sum 35~~

~~6.2.5 Privacy by Design Principle 5: End-to-End Safeguards – Full Information Management Life Cycle (ILCM) Protection 36~~

~~6.2.6 Privacy by Design Principle 6: Visibility and Transparency – Keep it Open 36~~

~~6.2.7 Privacy by Design Principle 7: Respect for User Privacy – Keep it User-Centric 37~~

~~6.3 Exceptions to the application of any of the Privacy by Design principles 37~~

~~6.4 Mapping the eleven (11) Privacy Protection Principles (PPP) to the seven (7) Privacy by Design principles 38~~

~~7 Collaboration space and privacy protection 38~~

~~7.1 Overview 38~~

~~7.2 Collaboration space: Role of consumer (as individual), vendor and regulator 38~~

~~8 Ensuring that personal information is ‘under the control of’ the organization throughout its ILCM 43~~

~~8.1 Overview 43~~

~~8.2 Rules governing the specification of ILCM aspects of personal information 44~~

~~8.3 Implementing “under the control of” and accountability 44~~

~~9 Conformance statement 45~~

~~9.1 Overview 45~~

~~9.2 Conformance to the ISO/IEC 14662 Open-edi Reference Model and the multipart ISO/IEC 15944 eBusiness standard 46~~

~~9.3 Conformance to ISO/IEC 15944-17 46~~

~~9.4 Conformance by agents and third parties to ISO/IEC 15944-17 46~~

~~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 48~~

~~A.1 Purpose 49~~

~~A.2 Maximizing unambiguity and quality control 49~~

~~A.3 Role and importance of ISO/IEC 15944-7 “Information technology – Business Operational View – Part 7: eBusiness vocabulary in support of facilitating HIE approach 51~~

~~A.4 List of terms and definition with cultural adaptability: English and French language equivalency in the IT standardization context 52~~

~~Annex B (normative) Consolidated controlled vocabulary definitions and associated terms, as human interface equivalents (HIEs), with cultural adaptability: English and French language equivalency in an EDI and collaboration space context 53~~

~~B.1 Overview 53~~

~~B.2 Organization of Annex B Controlled Vocabulary list in table form 53~~

~~Edited DIS~~
~~MUST BE USED~~
~~FOR FINAL~~
~~DRAFT~~

Annex C (informative) Mapping ISO/IEC 15944-8 Privacy Protection Principles (PPP) to the Privacy by Design principles 1

C.1 Purpose 1

C.2 Organization of Annex C 1

Annex D (informative) Exclusions to the scope of ISO/IEC 15944-17 9

D.1 Functional services view (FSV) 9

D.2 Internal behaviour of organizations (and public administration) 9

D.3 Overlap of and/or conflict among jurisdictional domains as sources of privacy protection requirements (PPR) 9

D.4 Changes in jurisdictional domain of parties to a business transaction 10

D.5 Publicly available personal information (PAPI) 10

Annex E (informative) Fair Information Principles / Fair Information Practices 11

E.1 Purpose 11

E.2 Origin of FIP 11

E.3 Use of FIP in ISO/IEC 15944 standards development 11

E.4 Addition of FIP in ISO/IEC 15944-8 “Preventing Harm” 11

Annex F (informative) Aspects currently not addressed 12

Bibliography 13

Foreword viii

Introduction xii

1 Scope 1

2 Normative references 3

3 Terms and definitions 5

4 Abbreviated terms 25

5 Fundamental privacy protection principles 28

5.1 Overview 28

5.2 Primary sources of privacy protection principles 29

5.3 Exceptions to the application of the privacy protection principles 30

5.4 Key eleven (11) privacy protection principles 30

5.5 Link to “consumer protection” and “individual accessibility” requirements 31

5.6 Requirements for tagging (or labelling) sets of personal information (SPIs) in support of privacy protection requirements (PPR) 32

5.7 Requirements for making all personal information (PI) available to the buyer where the buyer is an individual 32

6 Fundamental principle (and rules) governing Privacy by Design (PbD) requirements 32

6.1 Overview 32

6.2 Fundamental principles of Privacy by Design 33

6.2.1 Privacy by Design Principle 1: Proactive not reactive, Preventative not remedial 33

**FOR FINAL
DRAFT**

**Edited DIS
MUST BE USED**

iTeh Standards

(<https://standards.itel.ai>)

Document Preview

ISO/IEC FDIS 15944-17

<https://standards.itec.ai/en/standards/iso-iec-15944-17/4a-bcca-7b900a4a3c/iso-iec-fdis-15944-17>

6.2.2 Privacy by Design Principle 2: Privacy as the Default Setting 34

6.2.3 Privacy by Design Principle 3: Privacy Embedded into Design..... 35

6.2.4 Privacy by Design Principle 4: Full Functionality — Positive-Sum, not Zero-Sum..... 35

6.2.5 Privacy by Design Principle 5: End-to-End Safeguards — Full Information Management Life Cycle (ILCM) Protection..... 36

6.2.6 Privacy by Design Principle 6: Visibility and Transparency — Keep it Open..... 36

6.2.7 Privacy by Design Principle 7: Respect for User Privacy — Keep it User-Centric 37

6.3 Exceptions to the application of any of the Privacy by Design principles 37

6.4 Mapping the eleven (11) Privacy Protection Principles (PPP) to the seven (7) Privacy by Design principles..... 38

7 Collaboration space and privacy protection 38

7.1 Overview..... 38

7.2 Collaboration space: Role of consumer (as individual), vendor and regulator..... 38

8 Ensuring that personal information is ‘under the control of’ the organization throughout its ILCM 43

8.1 Overview..... 43

8.2 Rules governing the specification of ILCM aspects of personal information 44

8.3 Implementing “under the control of” and accountability 44

9 Conformance statement..... 45

9.1 Overview..... 45

9.2 Conformance to the ISO/IEC 14662 Open-edi Reference Model and the multipart ISO/IEC 15944 eBusiness standard 46

9.3 Conformance to ISO/IEC 15944-17..... 46

9.4 Conformance by agents and third parties to ISO/IEC 15944-17 46

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..... 49

Annex B (normative) Consolidated set of rules in existing Parts of ISO/IEC 15944 of particular relevance to PbD as external constraints on business transactions which apply to personal information (PI) in an EDI and collaboration space context 53

Annex C (informative) Mapping ISO/IEC 15944-8 Privacy Protection Principles (PPP) to the Privacy by Design principles 1

Annex D (informative) Exclusions to the scope of ISO/IEC 15944-17..... 9

Annex E (informative) Fair Information Principles / Fair Information Practices..... 11

Annex F (informative) Aspects currently not addressed 12

Bibliography..... 13

~~Edited DIS~~

List of Figures

Figure 1 Privacy by Design and Data Privacy by Design Reference Model

**MUST BE USED
FOR FINAL
DRAFT**



~~Figure 2 Integrated view of business operational requirements with a focus on external constraints relevant to Privacy by Design xi~~

~~Figure 3 Primary sources for privacy protection principles 30~~

~~Figure 4 Privacy collaboration space (of a business transaction) including the role of a regulator 41~~

~~Figure 5 Generalized collaboration space 42~~

~~Figure 6 collaboration space involving an individual and personal information 43~~

List of Tables

~~Table A.1 Columns in Table A.2 51~~

~~Table A.2 List of newly introduced terms and definitions with cultural adaptability of ISO English and ISO French language equivalency 52~~

~~Table B.1 Columns in Table B.2 Consolidated Lists of Rules and associated guidelines 53~~

~~Table B.2 Consolidated lists of rules and associated guidelines 53~~

~~Table C.1 Organization of Columns in Table C.2 77~~

~~Table C.2 Mapping of the eleven PPP with the seven PbD principles 78~~

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

[ISO/IEC FDIS 15944-17](https://standards.itih.ai/catalog/standards/iso/1e326f31-39fc-474a-bcca-7bf4900a4a3c/iso-iec-fdis-15944-17)

<https://standards.itih.ai/catalog/standards/iso/1e326f31-39fc-474a-bcca-7bf4900a4a3c/iso-iec-fdis-15944-17>

~~**Edited DIS -**
MUST BE USED
FOR FINAL
DRAFT~~

Formatted: HeaderCentered

Formatted: Font: Bold

Foreword

Formatted: Foreword Title, Space After: 0 pt

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.

Formatted: Left: 1.9 cm, Right: 1.9 cm, Gutter: 0 cm, Section start: New page, Header distance from edge: 1.27 cm, Footer distance from edge: 0.5 cm

Formatted: English (United Kingdom)

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).

Formatted: English (United Kingdom)

Field Code Changed

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 have 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.

Formatted: English (United Kingdom)

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, www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

Formatted: English (United Kingdom)

Field Code Changed

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

Formatted: English (United Kingdom)

This document is intended to be used in conjunction with ISO/IEC 14662, ISO/IEC 15944-1, ISO/IEC 15944-4, ISO/IEC 15944-5, ISO/IEC 15944-8 and ISO/IEC 15944-12.

Formatted: Foreword Text, Space After: 0 pt

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.

Formatted: English (United Kingdom)

Field Code Changed

Formatted: FooterPageRomanNumber

Formatted: HeaderCentered

Formatted: Font: Bold

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

ISO/IEC FDIS 15944-17

<https://standards.itih.ai/catalog/standards/iso/1e326f31-39fc-474a-bcca-7bf4900a4a3c/iso-iec-fdis-15944-17>

Formatted: FooterPageRomanNumber

Formatted: Font: Bold

Formatted: HeaderCentered

Introduction

0.1 — Purpose and overview

The ISO/IEC 14662 and the ~~multipart~~ ISO/IEC 15944 Business Operational View (BOV) ~~series of~~ standards focus on electronic data interchange (EDI) and "collaboration space" among Persons. Modelling business transactions using scenarios and scenario components includes specifying the applicable constraints on the data using explicitly stated rules. The ISO/IEC 14662 Open-edi Reference Model identifies two basic classes of constraints, "internal constraints" and "external constraints".

Jurisdictional domains are the primary source of external constraints on business transactions. Privacy protection is addressed as a common set of external constraint requirements coming from jurisdictional domains. Jurisdictional domains, such as UN member states and/or their administrative sub-divisions (see further ~~5-25.2~~ on sources of requirements), have enacted various "privacy" laws, "data protection" laws, "protection of personal information" laws, etc., (as well as pursuant regulations). Some of these sources of legal requirements focus on the protection of personal information in IT systems only, (e.g. ~~7~~ "data protection"), while others focus on the protection of personal information irrespective of the medium used for the recording of personal information and/or its communication to other Persons.

The overall purpose of the PbD ~~[2][2]~~ approach is two folds: (1) to ensure that privacy protection requirements (as stated in applicable legal and/or regulatory requirements) are identified as early as possible in the business operational process; (2) are specified in a systematic and rule-based manner for those developing any IT systems within their organization.

The PbD approach has always been supported and embedded in ISO/IEC 15944 development work. The need for the multipart ISO/IEC series of standards to comply with and support privacy protection requirements was already incorporated in the 1st edition of ~~Part 1 titled "Operational aspects of Open-edi for implementation."~~ ISO/IEC 15944-1. The development of the multipart series of ISO/IEC 15944 eBusiness standards and relevant parts of the multipart ISO/IEC standard that focus on privacy protection requirements fully supports the seven (7) foundational principles of the PbD approach ~~[2], [2]~~. In particular, it provides the detailed rules, definitions and related guidelines necessary to ensure that privacy protection requirements are identified and implemented not only throughout the entire life cycle of the recorded information involved, i.e. "cradle-to-grave" information life cycle management (ILCM) but especially for any personal information interchanged via EDI among parties to a particular business transaction.

This document highlights the requirements of ISO/IEC 14662 and ISO/IEC 15944 that focus on addressing commonly definable aspects of external constraints that relate to Privacy by Design in a privacy protection requirements (PPR) context when the source is a jurisdictional domain.¹ 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.

This document also extends the requirements of ISO/IEC 14662 and ISO/IEC 15944 where relevant and describes the added business semantic descriptive techniques needed to support PbD aspects beyond privacy protection requirements (PPR) when modelling business transactions. PbD aspects are central to ensuring that PPR are embedded early on in the design, passed on and supported throughout the lifecycle of the personal information, among all the parties to a business transaction using EDI.

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

0.2.1 — ISO/IEC 14662 "Open-edi Reference Model"²

¹ See further ~~Clause subclause~~ 0.2 below which identifies and summarizes the relevance of ISO/IEC 14662 and specific parts of the multipart ISO/IEC 15944 standard to this document.

² The ISO/IEC 14462 *Open-edi Reference Model* serves as the basis of the 2000 Memorandum of Understanding (MOU) among ISO, IEC, ITU and the UN/ECE concerning [harmonization of standardization in the field of electronic

Formatted: Font: 11 pt

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: FooterPageRomanNumber

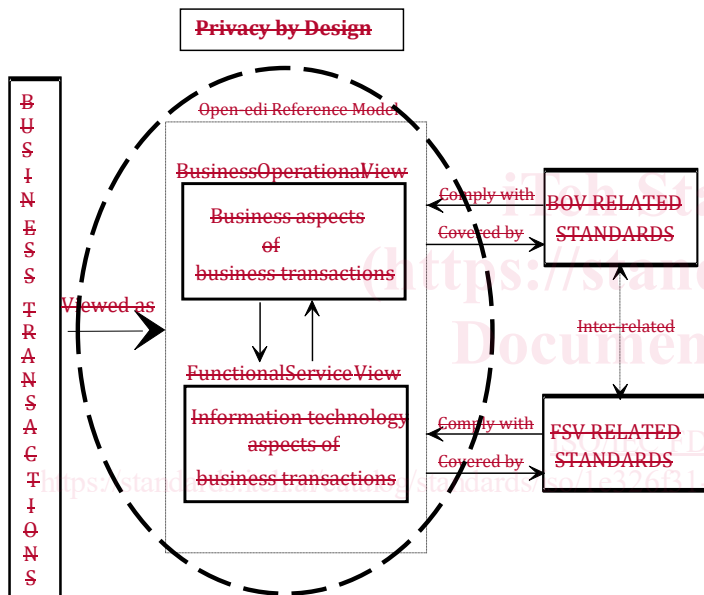
Formatted: HeaderCentered

Formatted: Font: Bold

ISO/IEC 14662 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. 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.

The delivery of Privacy by Design and privacy protection requires action both at the business operational level (BOV) and functional services view (FSV) (or technology levels). Where human beings interact with recorded information once it has passed through an Open-edi transaction, they have the potential to compromise technical controls (FSV) that have been applied. It is essential that business models take into account the need to establish overarching business processes that address issues that have not been, and/or cannot be resolved by the technical FSV controls. This is to provide the overall privacy protection demands of regulation that are required to be applied to personal data, their use, prescribed dissemination and so on. In this regard, the interplay of the BOV and FSV views of all organizations is important.

The first is the Business Operational View (BOV). The second is the Functional Service View (FSV). Figure 1 from ISO/IEC 14662:2010, Figure 1 illustrates the realm to which PbD aligns with the Open-edi environment.



business. (See <http://www.itu.int/ITU-T/e-business/files/mou.pdf>) See <https://www.itu.int/ITU-T/e-business/files/mou.pdf>

Formatted: Font: 11 pt

Formatted: FooterPageRomanNumber

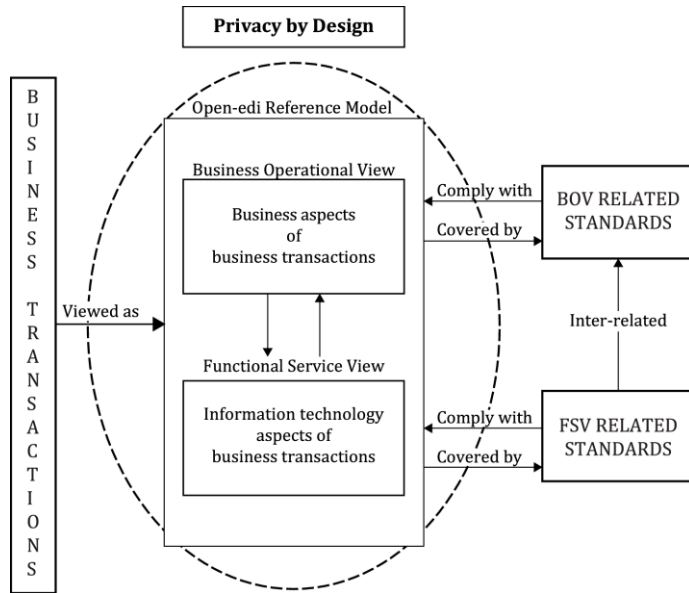


Figure 1 — Privacy by Design and Open-edi reference model environment

0.2.2 — ISO/IEC 15944-1 Business operational view (BOV) — ~~operational~~ — **Operational** aspects of Open-edi for implementation

ISO/IEC 15944-1 states the requirements of the BOV aspects of Open-edi in support of electronic business transactions. They include:

- commercial frameworks and associated requirements;
- legal frameworks and associated requirements;
- public policy requirements particularly which apply to individuals, i.e., are rights of individuals, which are of a generic nature such as consumer protection, privacy protection, accessibility and human rights (see ISO/IEC 15944-5:20172008, 6.3);
- requirements arising from the need to support cultural adaptability. This includes meeting localization and multilingual requirements, (e.g., as can be required by a particular jurisdictional domain or desired to provide a good, service and/or right in a particular market). One needs the ability to distinguish, the specification of scenarios, scenario components, and their semantics, in the context of making commitments, between:

a) — the use of unique, unambiguous and linguistically neutral identifiers (often as composite identifiers) at the information technology interface level among the IT systems of participation parties on the one hand; and, on the other,

b) — their multiple human interface equivalent (HIE) expressions in a presentation form appropriate to the Persons involved in the making of the resulting commitments.