INTERNATIONAL STANDARD

ISO/IEC 15944-12

First edition
2020-05

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)

Reference number
ISO/IEC 15944-12:2020(E)

© ISO/IEC 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

© ISO/IEC 2020 – All rights reserved

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

 © ISO/IEC 2020 – All rights reserved

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.

© ISO/IEC 2020 – All rights reserved

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.

© ISO/IEC 2020 – All rights reserved

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

0.2.1 ISO/IEC 14662: Open-edi reference model[1)]

ISO/IEC 14662[2)] 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.)

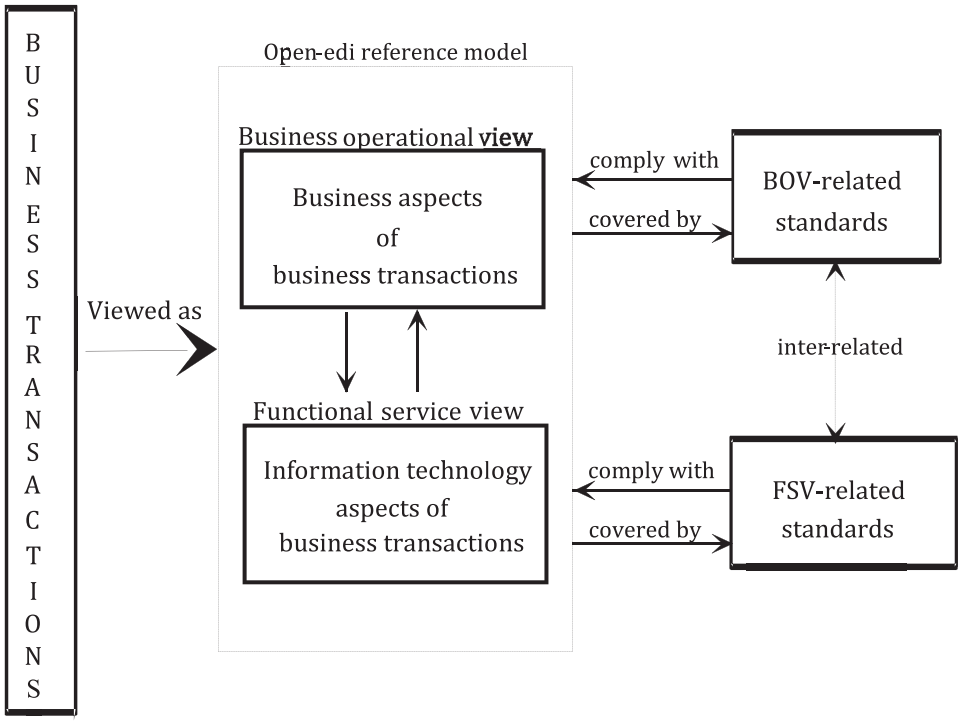

Figure 1 — Open-edi reference model environment

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 protection[3)] 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.

© ISO/IEC 2020 – All rights reserved

This document is based on ISO/IEC 14662 as well as existing parts of the ISO/IEC 15944 series, which serve as its key normative references and overall boundaries for the scope of this document. ISO/IEC 15944-5 and ISO/IEC 15944-8, in particular, serve as the basis for this document as they both focus on external constraints.

0.2.2 ISO/IEC 15944-1: Business operational view (BOV) – 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 are required to be taken into account in the development of business semantic descriptive techniques for modelling e-business transactions and components thereof as re-useable business objects. 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, and accessibility (see ISO/IEC 15944-5:2008, 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). Here 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.

Figure 2, based on ISO/IEC 15944-1:2011, Figure 3, shows an integrated view of these business operational requirements. Since the focus of this document is that of external constraints for which jurisdictional domains are the primary source, these primary sources have been shaded in Figure 2.

© ISO/IEC 2020 – All rights reserved

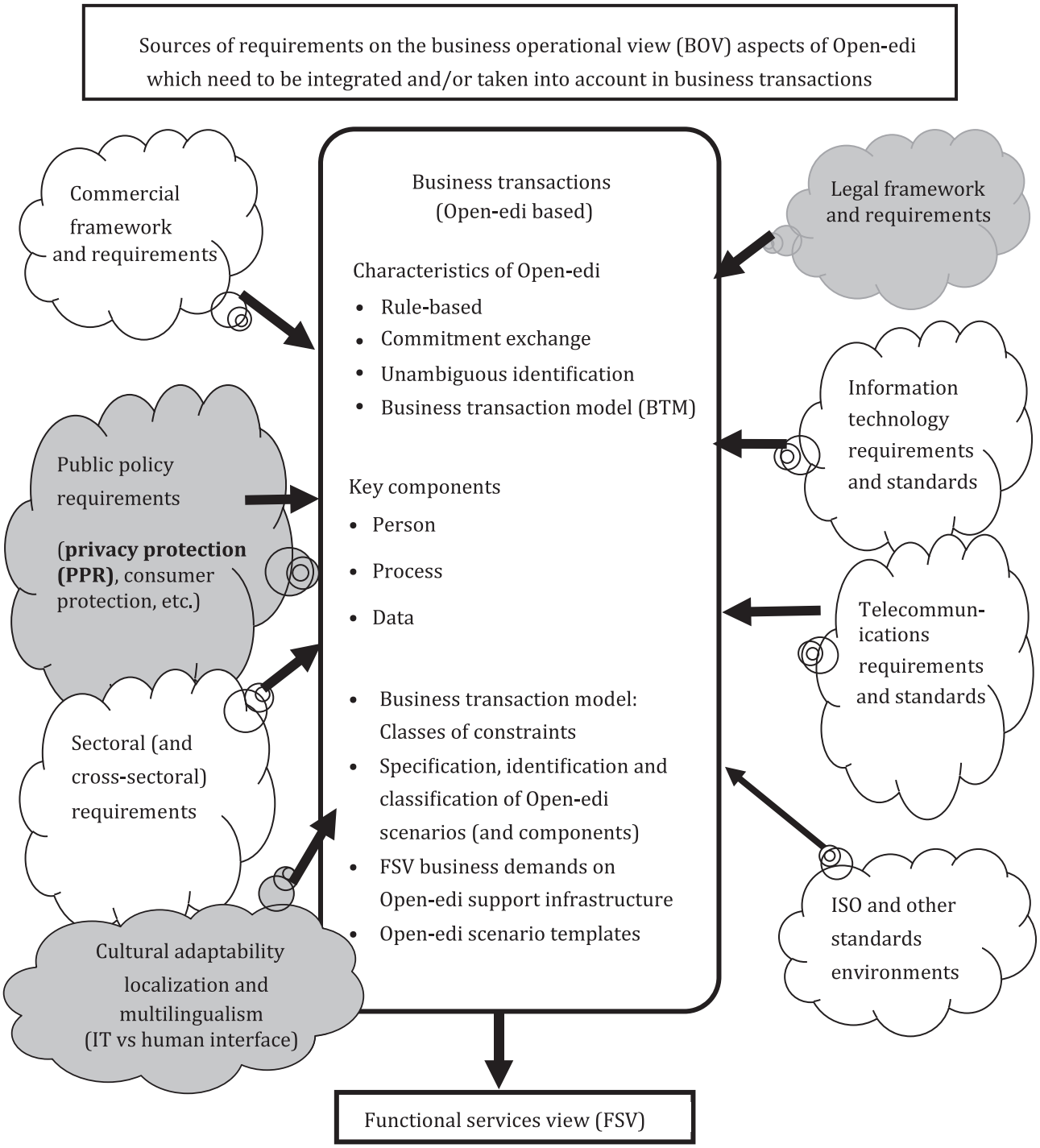

Figure 2 — Integrated view of business operational requirements with an external constraints focus

In electronic business transactions, whether undertaken on a for profit or not-for-profit basis, the key element is commitment exchange among Persons made through their decision-making applications (DMAs) of their information technology systems (IT Systems, see ISO/IEC 14662:2010, 5.2) acting on behalf of "Persons". "Persons" are the only entities able to make commitments.

© ISO/IEC 2020 – All rights reserved

The **business operational view (BOV)** was defined as:

*"perspective of **business transactions** limited to those aspects regarding the making of **business** decisions and **commitments** among **Persons** which are needed for the description of a **business transaction**".*

[SOURCE: ISO/IEC 14662:2010, 3.3]

There are three categories of Person as a role player in Open-edi, namely: (1) the Person as "individual", (2) the Person as "organization", and (3) the Person as "public administration"[4]. There are also three basic (or primitive) roles of Persons in business transactions, namely: "buyer", "seller", and "regulator". When modelling business transactions, jurisdictional domains prescribe their external constraints in the role of "regulator" and execute them as "public administration".

0.2.3 Link to ISO/IEC 15944-5 and ISO/IEC 15944-8

ISO/IEC 15944-5 focuses on external constraints the primary source of which is jurisdictional domains, at various levels. It also identified a common class of external constraints known as "public policy", which apply where and when the "buyer" in a business transaction is an "individual". It identified three key sub-types, along with applicable rules; of public policy constraints, namely: "consumer protection", "privacy protection" and "individual accessibility" (see ISO/IEC 15944-5:2008, 6.3). In addition, ISO/IEC 15944-5 specifies how and where (common) external constraints of jurisdictional domains impact the "Person", "process", and "data "components of the business transaction model (BTM), as introduced in ISO/IEC 15944-1.

ISO/IEC 15944-8, which is based on ISO/IEC 15944-5, focuses on providing a more detailed identification and specification of the common privacy protection requirements as they apply to any business transaction where the buyer is an individual.

This document:

— is based on both ISO/IEC 15944-5 and ISO/IEC 15944-8;

— integrates applicable concepts and definitions, principles, rules, etc., found in both ISO/IEC 15944-5 and ISO/IEC 15944-8 (as well as applicable elements of the Open-edi reference model and other parts of the ISO/IEC 15944 series); and

— focuses on information life cycle management (ILCM) aspects at a more granular level, i.e., that required to be able to support implementation of the same.

0.3 Link to Privacy-by-Design (PbD) [48] approach

The overall purpose of the Privacy by Design (PbD) approach is to ensure that privacy protection requirements (as stated in applicable legal and/or regulatory requirements) are identified and specified in a systematic and rule-based manner for those developing any IT systems within their organization.

It is noted that although this is the first part in the ISO/IEC 15944 series in which Privacy by Design is formally mentioned, the PbD approach has always been supported and "imbedded" in the development of the ISO/IEC 15944 series. The need to comply with and support privacy protection requirements was already incorporated in ISO/IEC 15944-1:2002, D.1.1.

The development of the ISO/IEC 15944 series fully supports the seven "foundation principles" of the PbD approach[5]. In particular it provides the detailed rules, definitions and related guidelines necessary

4) While "public administration" is one of the three distinct sub-types of Person, most of the rules in this document applicable to "organization" also apply to "public administration". In addition, an unincorporated seller is also deemed to function as an "organization". Consequently, the use of "organization" throughout this document also covers "public administration". Where it is necessary to bring forward specific rules, constraints, properties, etc., which apply specifically to "public administration", this is stated explicitly.

5) 1. Proactive and not reactive; preventative and not reactive; 2. Privacy as the default setting; 3. Privacy embedded in design; 4. Full functionality – positive-sum, not zero-sum; 5. End to end security – full lifecycle protection; 6. Visibility and transparency – keep it open; 7. Respect for user privacy – keep it user-centric. [48]

 © ISO/IEC 2020 – All rights reserved

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 that for any personal information interchanged via EDI among parities to a particular business transaction.

0.4 Importance and role of terms and definitions

The ISO/IEC 15944 series sets out the processes for achieving a common understanding of the business operational view (BOV) from commercial, legal, ICT, public policy and cross-sectoral perspectives. It is therefore important to check and confirm that a “common understanding” in any one of these domains is also unambiguously understood as identical in the others.

This subclause is included in each part of the ISO/IEC 15944 series to emphasize that harmonized concepts and definitions (and assigned terms) are essential to the continuity of the overall series.

In order to minimize ambiguity in the definitions and their associated terms, each definition and its associated term has been made available in at least one language other than English in the document in which it is introduced. In this context, it is noted that ISO/IEC 15944-7 already also contains human interface equivalents (HIEs) in ISO Chinese, ISO French, and ISO Russian[6)].

0.5 Based on rules and guidelines

This document is intended to be used by diverse sets of users having different perspectives and needs (see Figure 2).

The ISO/IEC 15944 series focuses on "other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose".

Open-edi is based on rules which are predefined and mutually agreed to. They are precise criteria and agreed-upon requirements of business transactions representing common business operational practices and functional requirements.

These rules also serve as a common understanding bridging the varied perspectives of the commercial framework, the legal framework, the information technology framework, standardisers, consumers, etc.[7)]

0.6 Use of “Person”, “organization”, “individual” and “party” in the context of business transaction and commitment exchange

Throughout this document:

— the use of Person with a capital "P" represents Person as a defined term, i.e., as the entity within an Open-edi Party that carries the legal responsibility for making commitment(s);

— "individual", "organization", and "public administration" are defined terms representing the three common sub-types of "Person"; and

— the use of the words “person(s)” and “party (ies)” without a capital “P” indicates their use in a generic context independent of “Person”, as a defined concept in ISO/IEC 14662 and the ISO/IEC 15944 series.

NOTE A "party" to a business transaction has the properties and behaviours of a "Person”.

6) The designation ISO before a natural language refers to the use of that natural language in ISO standards.

7) The working principle is that of "coordinated autonomy", i.e., all parties are autonomous. Therefore, the extent to which they cooperate, agree on common needs, business rules constraints, practices, etc., and reach agreement on the same in form of precise rules, terms and definitions, etc., is a key influence on the creation of necessary standards as well as common scenarios, scenario attributes and scenario components.

© ISO/IEC 2020 – All rights reserved

0.7 Use of "identifier" (in a business transaction) and roles of an individual

ISO/IEC 15944-1:2011, 6.1.4 focuses on the requirement for the unambiguous identification of entities in business transactions (see also ISO/IEC 15944-1:2011, Annex C). "Unambiguous" is a key issue in business transactions because states of ambiguity and uncertainty are an anathema from commercial, legal, consumer and information technology perspectives. Issues of unambiguousness apply to all aspects of a business transaction and even more so to those which are EDI-based. Open-edi transactions anticipate that all entities are fully and clearly identified prior to the instantiation of a business transaction.

0.8 Use of "jurisdictional domain" in the context of privacy protection and related ILCM requirements

The term "jurisdiction" has many possible definitions. Some definitions of "jurisdiction" have accepted international legal status while others do not. It is also common practice to equate "jurisdiction" with "country", although the two are by no means synonymous. It is also common practice to refer to states, provinces, länder, cantons, territories, municipalities, etc., as "jurisdictions", and in contract law it is customary to specify a particular court of law as having jurisdiction or a defined national body, or an international body as having jurisdiction (even if that is not legally enforceable), and so on. Finally, there are differing "legal" definitions of "jurisdiction". Readers should understand that in this document:

— the use of the term "jurisdictional domain" represents its use as a defined term; and

— the use of the terms "jurisdiction(s)" and/or "country (ies)" represents their use in their generic contexts and do not imply any legal effect per se.

0.9 Use of "privacy protection" in the context of business transaction, EDI and any type of commitment exchange

Jurisdictional domains, such as UN member states (and/or their administrative sub-divisions), 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., "data protection"), while others focus on the protection of personal information irrespective of the medium (see ISO/IEC 15944-1:2011, 6.4.1) used for the recording of personal information and/or its communication to other Persons.

In the case of personal information, this is currently defined by most jurisdictional domains to be a specific sub-set of recorded information relating to the Person as an "individual" — where the qualities of such type of Person are that they are required to be an identifiable, living individual. As a consequence, this may only apply to some proportion of the specific role players in a business transaction (including their personae) and not others.

The delivery of "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 could 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 applied so as 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.

0.10 Use of "set of recorded information" (SRI) and "set of personal information" (SPI) versus record, document, message, data, etc.

The concepts of "record", "document", "data", "message", etc., are defined and used in ISO standards and in different levels of jurisdictional domains. However, multiple differing definitions exist for each of these terms. To address this polysemy issue, the unifying concept and definition of "set of recorded information" was introduced and defined in ISO/IEC 15944-5.

 © ISO/IEC 2020 – All rights reserved

In Open-edi, SRIs are modelled as information bundles (IBs) and semantic components (SCs) when they are interchanged among participating parties in a business transaction. Within the IT systems of an organization, and especially within its decision-making applications (DMAs), the recorded information pertaining to a business transaction is usually maintained as one or more (linked) SRIs.

In order to maximize linkages between Open-edi (external behaviour) aspects and data management (internal behaviour) aspects of an organization (as well as associated record management and EDIFACT standards), SRI is used as a common higher level concept, which incorporates essential attributes of the concepts of "record", "document", "message", etc. as defined in various ways in existing ISO standards.

Where and when a SRI is of the nature of personal information or contains personal information, privacy protection requirements (PPR) apply. Within the context of PPR and with the focus of ILCM the concept and definition of "*set of personal information (SPI)*" is as follows:

— ***set of personal information (SPI)***;

— ***set of recorded information (SRI)*** *which is of the nature of or contains* ***personal information***.

This document focuses on ILCM of personal information in support of PPR and as such *"set of personal information (SPI)"* is used throughout this document while *"set of recorded information* (SRI) when referring to the more generic ILCM aspects.

0.11 Aspects currently not addressed

This first edition of this document focuses on the essential and basic ILCM aspects of privacy protection requirements.

Many other aspects identified in the development of this document remain to be addressed. For detailed information on these see Annex I.

0.12 IT-systems environment neutrality

This document, like all the other parts of ISO/IEC 15944, does not assume nor endorse any specific system environment, database management system, database design paradigm, system development methodology, data definition language, command language, system interface, user interface, syntax, computing platform, or any technology required for implementation, i.e., it is information technology neutral. At the same time, this document maximizes an IT-enabled approach to its implementation and maximizes semantic interoperability.

0.13 Organization and description of this document

This document identifies basic common requirements of information life cycle management (LCM) requirements in a privacy protection context, as external constraints of jurisdictional domains, on the modelling of a business transaction through scenarios and scenario components.

Following Clauses 0, 1, 2, 3 and 4, which have a common approach and similar content in the ISO/IEC 15944 series, Clause 5 summarizes the 11 "Fundamental privacy protection principles" introduced and defined in detail in ISO/IEC 15944-8:2012, Clause 5 along with its associated rules and guidelines. Clause 5 also provides a link to related "consumer protection" and "individual accessibility" requirements. A key purpose of Clause 5 is to place privacy protection principles in the content of ILCM requirements. A related purpose is to bring forward the requirement that any and all sets of personal information (SPIs) are identified, i.e., tagged or labelled, as such in support of privacy protection requirements.

Clause 6 identifies an integrated (minimum) set of ILCM principles along with associated rules and guidelines required to support both general information law requirements and in particular those required to be implemented in support of privacy protection requirements.

Clause 7 focuses on the need to ensure accountability for and control of personal information by any organization (or public administration). Clause 8 expands on this by providing the rules governing specification of ILCM aspects of personal information, i.e., from an implementation perspective.

© ISO/IEC 2020 – All rights reserved

The fact that in their "normal" operations organizations need to undertake data conversions and data migration in the decision-making applications (DMAs) of their IT systems is recognized in Clause 9. However, it is also important that applicable privacy protection requirements remain being supported, i.e., within and among, organizations including data synchronization among their IT systems.

Clause 10 summarizes key rules and requirements found in ISO/IEC 15944-1, ISO/IEC 15944-5 and ISO/IEC 15944-8 which govern EDI of personal information between the primary ILCM Person, i.e., seller, and its use of agents and/or third parties. The clause concludes with a conformance statement.

Finally, annexes are provided for elaboration of points raised in the main body. Of these Annexes A and B are normative, and the remaining annexes are informative.

Annex A is a consolidated list of the definitions and their associated terms introduced in this document in ISO English and ISO French. (For the complete set of ISO French (and ISO Russian and ISO Chinese) equivalents of the entries in Clause 3, see ISO/IEC 15944-7.) As stated in the main body of this document, the issue of semantics and their importance of identifying the correct interpretation across official aspects is critical.

Annex B identifies rules stated in the other parts of ISO/IEC 15944 that are applicable to this document.

Annex C is common to ISO/IEC 15944-2, ISO/IEC 15944-4, ISO/IEC 15944-5 and ISO/IEC 15944-8. It summarizes the business transaction model (BTM).

The focus of Annex D is to link the ILCM process to the process phases of a business transaction. Annex E provides a generic approach to ILCM decisions in a privacy protection requirements context along with an ILCM compliance decision tree template.

The purpose of Annex F is to provide a generic approach to the identification of properties and behaviours of PI as SRI transitory records and their disposition/expungement. In Annex G some notes on referential integrity in Open-edi are presented.

Annex H provides details on a number of exclusions to the scope of this document while Annex I identifies aspects of the scope of this document which have not yet been addressed in this current edition.

Annex J provides the list of all parts in the ISO/IEC 15944 series. Annex K contains abstracts in ISO English, French and Chinese.

© ISO/IEC 2020 – All rights reserved

Information technology — Business operational view —

Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)

1 Scope

This document:

— provides method(s) for identifying, in Open-edi modelling technologies and development of scenarios, the additional requirements in business operational view (BOV) specifications for identifying the additional external constraints to be applied to recorded information in business transactions relating to personal information of an individual, as required by legal and regulatory requirements of applicable jurisdictional domains;

— integrates existing normative elements in support of privacy and data protection requirements as are already identified in ISO/IEC 14662 and ISO/IEC 15944-1, ISO/IEC 15944-2, ISO/IEC 15944-4, ISO/IEC 15944-5, ISO/IEC 15944-8, ISO/IEC 15944-9, and ISO/IEC 15944-10;

— provides overarching, operational 'best practice' statements for associated (and not necessarily automated) processes, procedures, practices and governance requirements that act in support of implementing and enforcing technical mechanisms which support the privacy/data protection requirements necessary for implementation in Open-edi transaction environments;

— focuses on the life cycle management of personal information i.e., the contents of SPIs (and their SRIs) related to the business transaction interchanged via EDI as information bundles and their associated semantic components among the parties to a business transaction.

NOTE Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information as stated in this document serve as a minimum set of ILCM policy and operational requirements for all recorded information pertaining to a business transaction in particular, as well as ILCM implementation in any organization in general.

This document does not specify the technical mechanisms, i.e., functional support services (FSV) which are required to support BOV-identified requirements. Detailed exclusions to the scope of this document are provided in Annex H.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitute requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 14662:2010, *Information technology — Open-edi reference model*

ISO/IEC 15944-1:—,[8] *Information technology — Business operational view — Part 1: Operational aspects of Open-edi for implementation*

ISO/IEC 15944-5:2008, *Information technology — Business operational view — Part 5: Identification and referencing of requirements of jurisdictional domains as sources external constraints*

8) Third edition under preparation. Stage at time of publication: ISO/IEC DIS 15944-1.

© ISO/IEC 2020 – All rights reserved

ISO/IEC 15944-8:2012, *Information technology — Business operational view — Part 8: Identification of privacy protection requirements as external constraints on business transactions*

© ISO/IEC 2020 – All rights reserved