International Standard
FINAL DRAFT

ISO/IEC FDIS 15944-17

Information technology — Business operational view —

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

ISO/IEC JTC **1**/SC **32**

Secretariat: **ANSI**

Voting begins on:
2024-01-25

Voting terminates on:
2024-03-21

Reference number
ISO/IEC FDIS 15944-17:2024(en)

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

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 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.

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

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.

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

The ISO/IEC 14662 and the 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 5.2 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. “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] 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 the1st edition of 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] 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 parities 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)]

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

1) See further sublause 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 business. See https://www.itu.int//ITU-T/e-business/files/mou.pdf

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). ISO/IEC 14662:2010, Figure 1 illustrates the realm to which PbD aligns with the Open-edi environment.

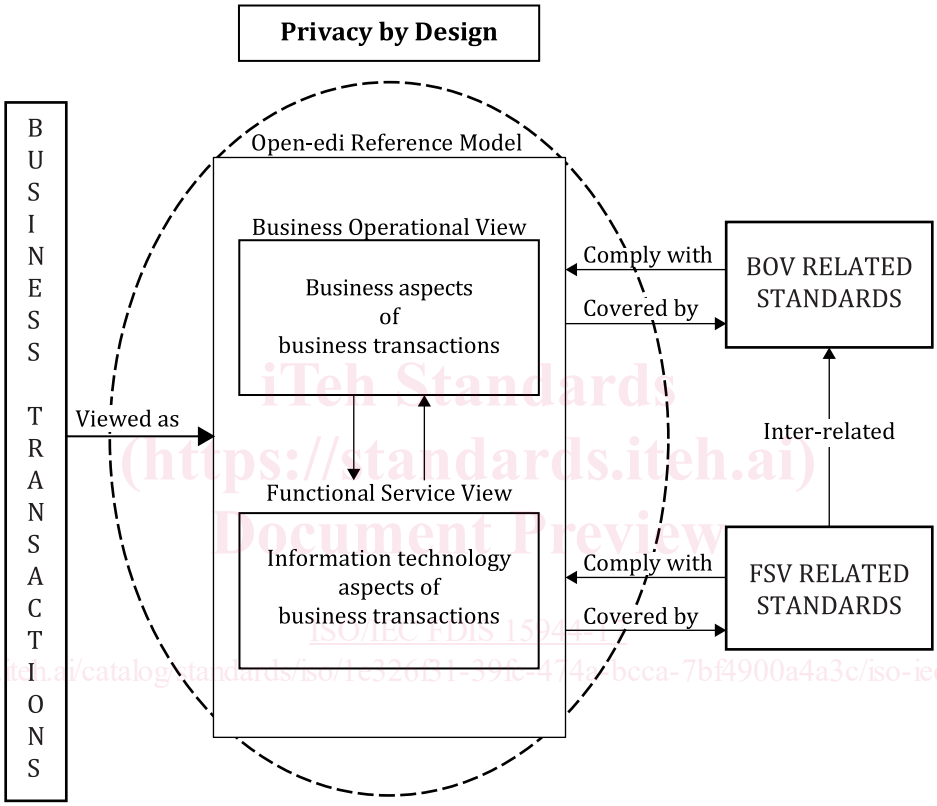

Figure 1 — Privacy by Design and Open-edi reference model environment

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 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 15944-5:2008, 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). 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 shows an integrated view of these business operational requirements. Since the focus of this document on Open-edi and Privacy by Design is that of external constraints for which jurisdictional domains are the primary source, these primary sources have been shaded (see 5.2 for sources of requirements).

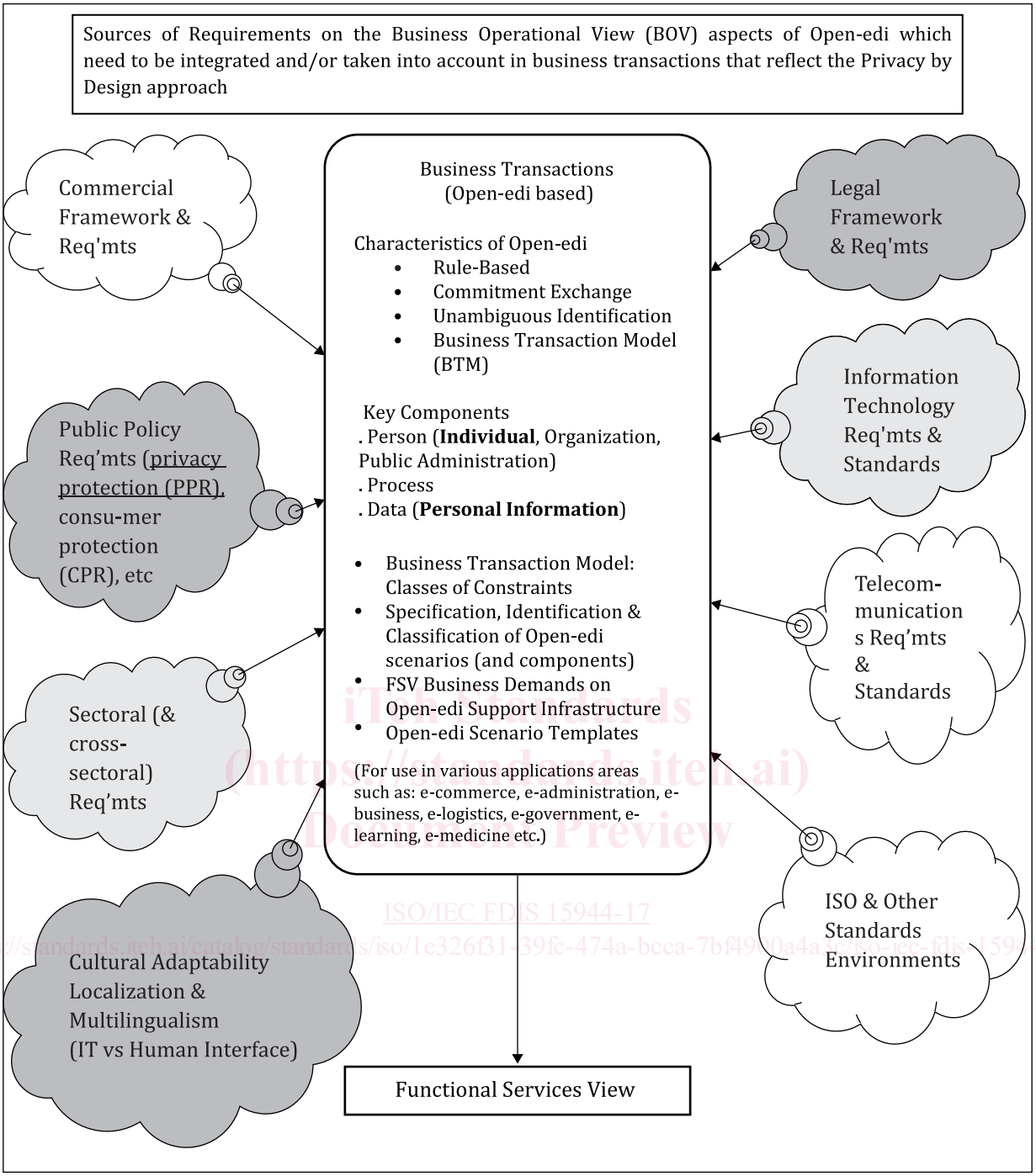

Figure 2 — Integrated view of business operational requirements with a focus on external constraints relevant to Privacy by Design

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[3)].

0.2.3 Links to ISO/IEC 15944-5, ISO/IEC 15944-8, ISO/IEC 15944-4 and ISO/IEC 15944-12

3) The text in this section is based on existing text in Section "0.3" in ISO/IEC 15944-1 and ISO/IEC 14662 (3rd edition). ISO/IEC 15944-7 "… eBusiness vocabulary" standard

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 identifies 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 uses ISO/IEC 15944-8 as the basis for establishing the fundamental privacy protection principles and rules that carry over to Privacy by Design. (Refer to Annex C.)

ISO/IEC 15944-4 helps to define the context in which PPP and PbD rules apply which is to the collaboration space. ISO/IEC 15944-4 provides the independent and the trading partner perspectives in the Open EDI ontology. In ISO/IEC 15944-1:2011, 6.1.3, Rule 1 states: *“Business transactions require both information exchange and commitment exchange.”* REA firmly agrees with and helps give definition to this assertion. Reciprocal commitments are exchanged in REA via economic contracts that govern exchanges, while information exchange is tracked via business events that govern the state transitions of business transaction entities that represent various economic phenomena. (See further 7.2 for REA and collaboration space). It is the requirement for information exchange and more specifically, information exchange with an individual within a business transaction that will trigger privacy protection rules in an Open EDI environment.

ISO/IEC 15944-12 is based on both ISO/IEC 15944-5 and ISO/IEC 15944-8 and integrates applicable concepts and definitions, principles, rules, etc., found in both (as well as applicable elements of the Open-edi reference model and other parts of the ISO/IEC 15944 series). The focus is on information life cycle management (ILCM) aspects at a more granular level, i.e. that are required to be able to support implementation of the same. The focus 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. It describes the added business semantic descriptive techniques needed to support information life cycle management 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. ILCM is an important aspect of privacy protection and PbD.

0.3 Importance and role of terms and definitions[4)]

The ISO/IEC 15944 series sets out the processes for achieving a common understanding of the BOV from commercial, legal, ICT, public policy and cross-sectoral perspectives. It is 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 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 Chinese, French, and Russian.

0.4 Basic rules and guidelines

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

4) All the terms and definitions of the current editions of the ISO/IEC 14662 *Open-edi Reference Model* and the multipart ISO/IEC 15944 eBusiness standard have been consolidated in ISO/IEC 15944-7. A primary reason for having “Terms and definitions” in a standard is because one cannot assume that a common understanding exists, worldwide, for a specific concept. And even if one assumes that such an understanding exists, then having such a common definition in Clause 3 serves to formally and explicitly affirm (re-affirm) such a common understanding, i.e. ensure that all parties concerned share this common understanding as stated through the text of the definitions in Clause 3.

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 for which there is mutual agreement. 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.

0.5 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";

— 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.

0.6 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.

0.7 Use of "jurisdictional domain" in the context of privacy protection requirements and Privacy by Design

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.

0.8 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 can only apply to some proportion of the specific role players in a business transaction (including their personae) and not others.

0.9 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.

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 an 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 PbD the concept and definition of SPI applies:

set of personal information (SPI)

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

This document focuses on PbD in support of PPR and as such "set of personal information (SPI)" is used throughout this document.

0.10 Aspects currently not addressed

The first edition of this document focuses on the essential and basic PbD aspects in an EDI and collaboration space context. Other aspects identified in the development of this document remain to be addressed. For detailed information, see Annex F.

0.11 IT-systems environment neutrality

This document, like all the other parts of ISO/IEC 15944, does not assume or 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.

0.12 Organization and description of this document

The focus of this document is on any kind of recorded personal information concerning individuals as buyers in a business transaction or whose personal information is used in a business transaction or any type of commitment exchange. (Refer to the exclusion of Publicly Available Personal Information (PAPI) in Annex D).

This document applies to any organization which receives, creates, process, maintains, communicates, etc. personal information (PI) of a consumer 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 organizations 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 design management 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.

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 context of PbD requirements.

The purpose and focus of Clause 6 is to apply the seven PbD requirements in Open-edi business transaction context using the ISO/IEC 15944 rule-based approach as they apply to any organization (or public administration) in their interaction with any individual (outside of their organization) in the role of that individual as a buyer, i.e. consumer, in its interaction with the organization.

The importance of the concept of "collaboration space" introduced in ISO/IEC 15944-4 is carried forward and adapted in the privacy protection context in Clause 7, as the "privacy collaboration space (PCS)".

Clause 8 summarizes the Information Lifecycle Management (ILCM) aspects of PbD as part of privacy protection requirements when modelling business transactions using the external constraints of jurisdictional domains defined in detail in ISO/IEC 15944-12:2020.

Clause 9 provided the conformance requirements for this document.

Annex A provides the HIEs for all the terms and definitions newly defined in this document in addition to other parts of ISO/IEC 15944.

Annex B provides a consolidated set of rules defined in ISO/IEC 15944 relevant to this document.

Annex C provides the mapping of Privacy Protection Principles (PPP) to the Privacy by Design principles.

Annex D is a further description to the scope to clarify the exclusions that this document is not specifying.

Annex E introduces the concept of Fair Information Principles/Fair Information Practices in more detail.

Annex F provides additional information to the scope, stating those aspects that are yet addressed by the content of this document.