

# ISO/IEC JTC 1/SC 32 N 1843

Date: 2009-03-03

REPLACES: --

<p style="text-align: center;"><b>ISO/IEC JTC 1/SC 32</b></p> <p style="text-align: center;"><b>Data Management and Interchange</b></p> <p style="text-align: center;"><b>Secretariat: United States of America (ANSI)</b> <b>Administered by Farance Inc. on behalf of ANSI</b></p>
--

<b>DOCUMENT TYPE</b>	Other document (open)
<b>TITLE</b>	Response to the Questionnaire on Privacy of the TMB Task Force on Privacy (on behalf of JTC1/SC32)
<b>SOURCE</b>	WG1 Convener - Wenfeng Sun
<b>PROJECT NUMBER</b>	
<b>STATUS</b>	Response developed by SC32 WG1 (Data Management and interchange: eBusiness) at meeting in Ottawa, 16-19 February, 2009 in reply to inquiry by TMB Task Force on Privacy.
<b>REFERENCES</b>	
<b>ACTION ID.</b>	FYI
<b>REQUESTED ACTION</b>	
<b>DUE DATE</b>	
<b>Number of Pages</b>	11
<b>LANGUAGE USED</b>	English
<b>DISTRIBUTION</b>	P & L Members SC Chair WG Conveners and Secretaries

Dr. Timothy Schoechle, Secretary, ISO/IEC JTC 1/SC 32  
Farance Inc \*, 3066 Sixth Street, Boulder, CO, United States of America  
Telephone: +1 303-443-5490; E-mail: [Timothy@Schoechle.org](mailto:Timothy@Schoechle.org)  
available from the JTC 1/SC 32 WebSite <http://www.jtc1sc32.org/>  
\*Farance Inc. administers the ISO/IEC JTC 1/SC 32 Secretariat on behalf of ANSI

**TITLE:** JTC1/SC32/WG1 Response to the Questionnaire on Privacy of the TMB Task Force on Privacy (on behalf of JTC1/SC32)

**SOURCE:** JTC1/SC32/WG1 - eBusiness

**STATUS:** Publicly available response to the TMB Questionnaire on Privacy

**ACTION:** For input and use by the ISO TMB Task Force on Privacy

**DUE DATE:** 28 February, 2009

**NO. OF PAGES:** 10

- NOTES:**
1. This response to the TMB Questionnaire was developed by JTC1/SC32/WG1 at its 16-19 February, 2009 meeting. JTC1/SC32/WG1 welcomes this opportunity to inform the TMB on its standards and standards development work related to privacy, and is ready to provide a more detailed response and/or answer any specific questions which the TMB Task Force on Privacy may have.
  2. The key standards referenced in this response, namely, the *ISO/IEC 14662 Open-edi Reference Model* and the existing, and under development, Parts of the multipart *ISO/IEC 15944* eBusiness standards are ISO/IEC JTC1 "publicly available standards". Thus participants in the TMB Task Force on Privacy (and others) are able to access these standards "at no cost".
  3. The ISO/IEC 14662 *Open-edi Reference Model* standard serves as the common foundation and basis for the 2000 (and ongoing) "*ISO, IEC, ISO, ITU, UN/ECE, etc. Memorandum of Understanding (MoU) on e-Business Standards*"
  4. Appendix A to this response contains a small set of key concepts and their definitions taken from existing ISO/IEC JTC1/SC32 standards which may be of use to the work of the TMB Task Force (TF) on Privacy. Here JTC1/SC32/WG1 standards development work on these privacy protection related definitions and associated terms already includes the provision of French, Russian and Chinese language equivalencies for these eBusiness definitions and associated terms.

## Attachment 1

**Questionnaire from the ISO TMB Task Force on Privacy**

ISO/TMB has recently established a Task Force on Privacy ("TF"). The purpose of the TF is to advise the ISO/TMB on ISO technical standards that could support the implementation of public policy initiatives on privacy, with a specific focus on protection of personally identifiable information (PII) and fair information handling. A meeting of the TF recently took place during which it was concluded that, due to the very broad nature of privacy, a questionnaire would be sent to ISO technical committees involved in privacy-related issues and other relevant groups (ITU-T, CEN). The answers to these questions will be compiled and used to help determine what, if any, ISO's future involvement on the topic of privacy should be.

1. *Does your work programme currently include (or do you plan to include) any items that deal with data privacy, PII or fair information handling? If so, what does it (or will it) cover?*

The short answer is "Yes". JTC1/SC32/WG1<sup>1</sup> has been including making provisions for being able to support privacy protection requirements since the late 1990s with the inception of the development of multipart ISO/IEC 15944 eBusiness standard. The 1<sup>st</sup> edition of the ISO/IEC 14662 *Open edi Reference Model* (1997) states that standards required for Open-edi include support for national and international law and regulation. The *Open-edi Reference Model* also includes a Figure A.1 "Relationship of Open-edi standardization areas with other standards and impact of the legal environment".

The *Open-edi Reference Model* also serves as the basis and foundation for the 2000 (and ongoing) ITU, ISO, IEC, UN/ECE, etc., "*Memorandum of Understanding (MoU) concerning standardization in the field of electronic business*".

When the earlier ISO/IEC JTC1 "*Study Group – Privacy Technology*", had its meeting 17-18 June, 2004 (Montreal, Canada), JTC1/SC32 prepared and submitted a presentation in response to questions of the JTC1 SG on Privacy. At that time, i.e., four years ago, JTC1/SC32 already informed JTC1 of the applicability of its Open-edi and e-Business standards to privacy protection requirements. Again, in 2006, JTC1/SC32 at its March, 2006 Plenary established an "Kobe Privacy Ad-Hoc Group" in response to JTC1 Banff, 2005 Plenary Resolution 36 "Privacy Management". The resulting JTC1/SC32 Kobe resolution #9 and response document (JTC1/SC32 N1462). Requested "SC32 Ad Hoc Group on Privacy, Kobe Resolution on "Privacy Management"\* requested "*JTC1 (and SC27) to take into account that many of the requirements arising from laws or regulations pertaining to "privacy" or "data protection" have already been taken into account and are supported in existing JTC1/SC32 standards and those under development.*" The SC32 N1462 document also provided a list of JTC1/SC32 standards work which contains elements or functions that support the implementation of privacy/data protection requirements.

---

<sup>1</sup> JTC1/SC32 = "Data management and interchange"  
SC32/WG1 = "eBusiness"

It is the opinion of JTC1/SC32/WG1 that many of the issues raised with respect to privacy protection requirements have already been addressed in a general sense in the *ISO/IEC 14662 Open-edi Reference Model* and in particular, in Parts 1, 4 and 5 of the multipart ISO/IEC 15944 eBusiness standard. These standards focus on the “*Business Operational View (BOV)*” which includes being able to support legal and regulatory requirements of jurisdictional domains. Requirements of this nature are modelled as external constraints. Here privacy protection requirements represent a particular class of external constraints which apply where an individual is a party to a business transaction.

This statement needs to be qualified by stating that e-Business standards development of JTC1/SC32/WG1 focuses on “business transactions” and the “collaboration space” of and among the Persons (including “individuals”) who are parties to a business transaction.

This statement also needs to be clarified by stating that the “*Business Operational View (BOV)*” aspects of Open-edi standards development work focuses on the “WHATs”, and not the “HOW to” which is the purpose of the “*Functional Services View (FSV)*”, (e.g., the use of ICT technologies to support privacy protection requirements as defined and specified in BOV type standards.)

Another qualification which needs to be made here, and a very important one, is that e-Business standards and the key element of a business transaction is that it focuses on the making of a “commitment”, i.e., “commitment exchange”, among the parties to a business transaction (including where the buyer is an “individual”). This places higher levels of unambiguity (trustworthiness, integrity, accuracy, etc.), on “personal information”. For example, “lower” (or less stringent) levels may exist or be required with respect to (day-to-day) ordinary “information exchange” of personal information.

The final qualification which should be stated is that these e-Business standards and their development are “constraints-based” and make a clear distinction between “internal constraints” and “external constraints”. Here the primary source of external constraints are jurisdictional domains. In this context, “privacy protection” requirements represent a set of external constraints which is viewed as a sub-type of a more general set of external constraints of a “public policy” nature which are applicable when an “individual” is the “buyer” in a “business transaction”. In addition to “privacy protection” requirements, “public policy” requirements also include those of “consumer protection” and “Individual accessibility” nature.

To conclude, from its inception, the development of the multipart ISO/IEC 15944 eBusiness standard, whose general title is “Information technology – Business Operational View (BOV)” has been architected and structurally engineered to be able to support privacy protection requirements. These apply in a business transaction where the buyer is an “individual”. The multipart ISO/IEC 15994 eBusiness standard focuses on the “BOV” aspects of the *ISO/IEC 14662 Open-edi Reference Model*. The following existing Parts of ISO/IEC 15944 may be of particular interest to the TMB Task Force on Privacy

- Part 1: Operational Aspects of Open-edi for Implementation
- Part 4: Business transaction scenarios: Accounting and economic ontology
- Part 5: Identification and referencing of requirements of jurisdictional as sources of external constraints.

Finally, JTC1/SC32/WG1 has the following Part of ISO/IEC 15944 under development which is of direct relevance to the TMB Task Force of Privacy and that is:

- Part 8: Identification of privacy protection requirements as external constraints on business transactions.<sup>2</sup>

Here it must be stressed and emphasized that in the development of this Part 8 (as in the other Parts of the multipart ISO/IEC 15944 eBusiness standard), that JTC1/SC32/WG1 maximizes the use of existing ISO, IEC and ITU standards as well as ISO/IEC JTC1 standards. JTC1/SC32/WG1 is particularly conscious of the need to apply this working principle to the development of ISO/IEC15944-8.

2. *If your work programme currently includes (or will include) data privacy, PII or fair information handling related matters, what assistance or guidance from the ISO/TMB would be useful?*

JTC1/SC32 wants to maintain a close working relationship with the ISO/TMB TF on Privacy. JTC1/SC32/WG1 recognizes that the focus and scope of its standards development is that in the context of e-Business standards development requirements only. The degree to which the identification and specification of privacy protection requirements in an Open-edi and e-Business context are of a generic nature or not remains to be determined.

3. *Do you have suggestions for further ISO standards activities to support the implementation of public policy initiatives on data privacy, PII or fair information handling that could complement existing national and international standards?*

Yes.

- 1) The first suggestion here is that the TMB TF on Privacy considers expanding the distribution list for this Questionnaire. For example, there is a direct link between “privacy protection” requirements and “consumer protection” requirements. As such COPOLCO may have useful information on its ISO standards.

---

<sup>2</sup> For the rationale for this project subdivision for a new Part 8 within the development of the ISO/IEC 15944 multipart standard, see document ISO/IEC JTC1 SC32/WG1 N0351 (2007-06-30).

Also there is a direct link between “privacy protection” requirements” and “individual accessibility” requirements as identified in the “*UN Convention of the Rights of Persons with Disabilities*”<sup>3</sup>, i.e., as stated in its Article 22 “*Respect for privacy*”

<http://www.un.org/esa/socdev/enable/rights/convtexte.htm>

In addition, ISO TC46 “Information and Documentation” already has, and is developing, generic standards of an “information handling” nature, i.e. those pertaining to information/record/document management, archiving, evidentiary aspects, etc. The ISO TMB TF on Privacy should also ask for TC46 response and input here with respect to standards of an “information handling” nature.

- 2) In the English language, the phrase “personally identifiable information (PPI)” is grammatically and semantically very confusing. This is because it seems to apply to any information which an individual can identify, i.e., any particular set of recorded information which one, as an individual, can identify, (e.g., any result of a Google or Web-browser based search). This is a quite a different concept from that of “personal information” pertaining to privacy or data protection requirements as found in existing privacy/data protection legislation and regulations of jurisdictional domains. These can be summarized as “personal information” being “any recorded information on or about an identifiable individual that is recorded in any form, including electronically or on paper”.
- 3) The use of the phrase “fair information handling” also is confusing. In the international trade arena, one already has concepts and definitions of “fair trade”, “fair trade goods”, etc. In short, the use of “fair” in an international context is already commonly associated with an approach to trade in goods and services with developing countries. It is also confused with “fair use” in the education and research sectors in relation to copyright issues.

It is assumed by JTC1/SC32/WG1 that the phrase “fair information handling” embodies and basically pertains to the governance, information management policy, and information management practices of an organization or public administration and the use of their supporting ICT systems., with all these being in compliance with applicable laws and/or regulations, including those of a privacy protection nature. As such it is also assumed, that the phrase “fair information handling” is used to differentiate privacy protection requirements from all the other laws and regulations which pertain to any and all aspects of an organization’s internal information management and

---

<sup>3</sup> At its May, 2008 Sydney Plenary Meeting adopted Resolution WG1/17 Resolution WG 1 / 17: WG1 support to UN convention on the rights of persons with disabilities which reads as follows, “SC32/WG1 resolves that in its current standards development work and any of its new standards development projects, as well as any (post-2008) amendments or new editions of its existing standards, that these shall be able to support and facilitate whenever possible the implementation of the objectives and requirements of the 2006 “UN Convention on the Rights of Persons with Disabilities and Optional Protocols”, both generally and especially in the fields Open-edi and eBusiness. [See document JTC1/SC32 N 1728a]

external information exchange, i.e., “information law” requirements (including those of an EDI nature).

- 4) Finally, it is noted that when first introduced in Europe, almost two decades ago, “data protection” legislation or regulations pertained only to “machine-readable” or “computerized” recorded information. At that time, they did not apply to “paper records”. “Privacy” legislation when introduced (in common law based jurisdictional domains) was from its outset “technology neutral” and applicable to any form of recorded information. To bridge these two distinct and different approaches of jurisdictional domains, JTC1/SC32/WG1 combined these two perspectives into the integrated concept of “privacy protection”. [For its existing ISO/IEC standards definitions relevant to privacy protection, see Appendix A)

Please return your completed questionnaire to Sandy Louis-Gros ([gros-louis@iso.org](mailto:gros-louis@iso.org)) by February 28<sup>th</sup>, 2009.

---

## Appendix A – Set of Concepts and their definitions taken from existing ISO/IEC JTC1/SC32 standards which may be of use to the ISO TF on Privacy

1. Currently, the ISO/IEC 14662 Open-edi Reference Model and the existing Parts 1, 2, 4, 5 and 6 of the multipart ISO/IEC 15944 eBusiness standards, together contain a consolidated set of 271 defined concepts. These include 73 defined concepts drawn from other ISO/IEC, ISO and ITU standards.
2. A few of these key concepts and their definitions are presented in three sets as follows:
  - from the ISO/IEC 14662 Open-edi Reference Model standard (ISO/IEC 14662)
  - those pertaining to “Person” and “individual”; and,
  - those pertaining to “public policy” and “privacy protection”.

Note: The use of **bold** in the definitions below indicates the use of terms for other concepts which are also defined.

### 2.1 From the ISO/IEC 14662 Open-edi Reference Model (2<sup>nd</sup> edition, 2004)

#### **business**

series of **processes**, each having a clearly understood purpose, involving more than one **Person**, realised through the exchange of **recorded information** and directed towards some mutually agreed upon goal, extending over a period of time

[ISO/IEC 14662:2004 (3.1.2)]

#### **Business Operational View (BOV)**

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**

[ISO/IEC 14662:2004 (3.1.3)]

#### **business transaction**

predefined set of activities and/or **processes** of **Persons** which is initiated by a **Person** to accomplish an explicitly shared **business** goal and terminated upon recognition of one of the agreed conclusions by all the involved **Persons** although some of the recognition may be implicit

[ISO/IEC 14662:2004 (3.1.4)]

#### **commitment**

making or accepting of a right, obligation, liability or responsibility by a **Person** that is capable of enforcement in the **jurisdictional domain** in which the **commitment** is made

[ISO/IEC 15944-1:2002 (3.9)]

#### **Open-edi**

**electronic data interchange** among multiple autonomous **Persons** to accomplish an explicit shared **business** goal according to Open-edi standards

[ISO/IEC 14662:2004 (3.1.9)]

#### **Functional Service View (FSV)**

perspective of **business transactions** limited to those information technology interoperability aspects of **IT Systems** needed to support the execution of **Open-edi transactions**

## 2.2 Those pertaining to “Person”, “individual”, organization”, and “public administration”

### **Person**

**entity**, i.e. a natural or legal person, recognized by law as having legal rights and duties, able to make **commitment(s)**, assume and fulfil resulting obligation(s), and able to be held accountable for its action(s)

NOTE 1 Synonyms for “legal person” include “artificial person”, “body corporate”, etc., depending on the terminology used in competent jurisdictions.

NOTE 2 Person is capitalized to indicate that it is being utilized as formally defined in the standards and to differentiate it from its day-to-day use.

NOTE 3 Minimum and common external constraints applicable to a business transaction often require one to differentiate among three common subtypes of Person, namely “individual”, “organization”, and “public administration”.

[ISO/IEC 14662:2004 (3.1.14)]

### **individual**

**Person** who is a human being, i.e. a natural person, who acts as a distinct indivisible **entity** or is considered as such

[ISO/IEC 15944-1:2002 (3.28)]

### **organization**

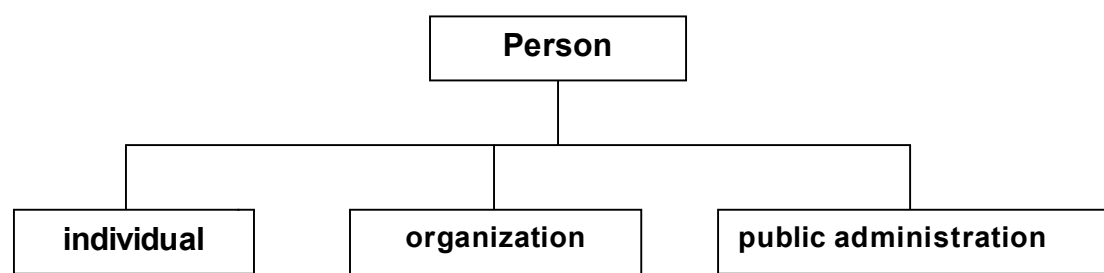
unique framework of authority within which a person or persons act, or are designated to act, towards some purpose

NOTE The kinds of organizations covered by ISO/IEC 15944 include the following:

- a) an organization incorporated under law;
- b) an unincorporated organization or activity providing goods and/or services including:
  - 1) partnerships,
  - 2) social or other non-profit organizations or similar bodies in which ownership or control is vested in a group of individuals,
  - 3) sole proprietorships,
  - 4) governmental bodies;
- c) groupings of the above types of organizations where there is a need to identify these in information interchange.

[ISO/IEC 6523-1:1998 (3.1)]

The relationship of “Person” and its three sub-types “individual”, “organization” and “public administration” is illustrated as follows:



### 2.3. Those pertaining “public policy” and “privacy protection”

#### **consumer protection**

set of **external constraints** of a **jurisdictional domain** as rights of a **consumer** and thus as obligations (and possible liabilities) of a **vendor** in a **business** transaction which apply to the good, service and/or right forming the goal of the **business** transaction (including associated information management and interchange requirements including applicable (**sets of**) **recorded information**)

NOTE 1 Jurisdictional domains may restrict the application of their consumer protection requirements as applicable only to individuals engaged in a business transaction of a commercial activity undertaken for personal, family or household purposes, i.e., they do not apply to natural persons in their role as “organization” or “organization Person”.

NOTE 2 Jurisdictional domains may have particular consumer protection requirements which apply specifically to individuals who are considered to be a “child” or a “minor”, (e.g., those individuals who have not reached their thirteenth birthday).

NOTE 3 Some jurisdictional domains may have consumer protection requirements which are particular to the nature of the good, service and/or right being part of the goal of a business transaction.

[ISO/IEC 15944-5:2008 (3.33)]

#### **external constraint**

**constraint** which takes precedence over **internal constraints** in a **business** transaction, i.e., is external to those agreed upon by the parties to a **business transaction**

NOTE 1 Normally external constraints are created by law, regulation, orders, treaties, conventions or similar instruments.

NOTE 2 Other sources of external constraints are those of a sectoral nature, those which pertain to a particular jurisdiction or a mutually agreed to common business conventions, (e.g., INCOTERMS, exchanges, etc.).

NOTE 3 External constraints can apply to the nature of the good, service and/or right provided in a business transaction.

NOTE 4 External constraints can demand that a party to a business transaction meet specific requirements of a particular role.

EXAMPLE 1 Only a qualified medical doctor may issue a prescription for a controlled drug.

EXAMPLE 2 Only an accredited share dealer may place transactions on the New York Stock Exchange.

EXAMPLE 3 Hazardous wastes may only be conveyed by a licensed enterprise.

NOTE 5 Where the information bundles (IBs), including their Semantic Components (SCs) of a business transaction are also to form the whole of a business transaction (e.g., for legal or audit purposes), all constraints must be recorded.

EXAMPLE There may be a legal or audit requirement to maintain the complete set of recorded information pertaining to a business transaction, i.e., as the information bundles exchanged, as a “record”.

NOTE 6 A minimum external constraint applicable to a business transaction often requires one to differentiate whether the Person, i.e. a party to a business transaction, is an “individual”, “organization”, or “public administration”. For example, privacy rights apply only to a Person as an “individual”.

[ISO/IEC 15944-1:2002 (3.50)]

#### **personal information**

information on or about an identifiable **individual** that is recorded in any form, including electronically or on paper

NOTE Some examples would be information about a person's religion, age, financial transactions, medical history, address or blood type.

[ISO/IEC 15944-5:2008 (103)]

**privacy protection**

set of **external constraints** of a **jurisdictional domain** pertaining to **recorded information** on or about an identifiable **individual**, i.e. **personal information**, with respect to the creation, collection, management, retention, access and use and/or distribution of such **recorded information** about that **individual** including its accuracy, timeliness and relevancy

NOTE 1 Recorded information collected or created for a specific purpose on an identifiable individual, i.e. the explicitly shared goal of the business transaction involving an individual, must not be utilized for another purpose without the explicit and informed consent of the individual to whom the recorded information pertains.

NOTE 2 Privacy requirements include the right of an individual to be able to view the recorded information about him/her and to request corrections to the same in order to ensure that such recorded information is accurate and up-to-date.

NOTE 3 Where jurisdictional domains have legal requirements which override privacy protection requirements these must be specified, (e.g. national security, investigations by law enforcement agencies, etc.).

[ISO/IEC 15944-5:2008 (3.109)]

**public policy**

category of **external constraints** of a **jurisdictional domain** specified in the form of a right of an **individual** or a requirement of an **organization** and/or **public administration** with respect to an **individual** pertaining to any exchange of **commitments** among the parties concerned involving a good, service and/or right including information management and interchange requirements

NOTE 1 Public policy requirements may apply to any one, all or combinations of the fundamental activities comprising a business transaction, i.e. planning, identification, negotiation, actualization and post-actualization. {See further Clause 6.3 "Rules governing the process component" in ISO/IEC 15944-1:2002}.

NOTE 2 It is up to each jurisdictional domain to determine whether or not the age of an individual qualifies a public policy requirement [e.g. those which specifically apply to an individual under the age of thirteen as a "child", those which require an individual to have attained the age of adulthood (e.g. 18 years or 21 years of age)] of an individual to be able to make commitments of a certain nature.

NOTE 3 Jurisdictional domains may have consumer protection or privacy requirements which apply specifically to individuals who are considered to be "children", "minors", etc. (e.g. those who have not reached their 18th or 21st birthday according to the rules of the applicable jurisdictional domain).

[ISO/IEC 15944-5:2008 (3.113)]

The relationship of the "public policy" standards (development) component of the legal environment to some of its key sub-types is illustrated as:

