TECHNICAL SPECIFICATION

ISO/IEC TS 20748-4

First edition
2019-09

Information technology for learning, education and training — Learning analytics interoperability —

Part 4: Privacy and data protection policies

Reference number
ISO/IEC TS 20748-4:2019(E)

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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **3**
5 Privacy and data protection requirements **4**
5.1 General 4
5.2 The concept of privacy and data protection in LET 4
5.3 Privacy and data protection issues related to learning analytics 6
5.4 Privacy framework requirements 7
6 Learning analytics privacy and data protection attributes **8**
7 LA privacy and data protection attribute specifications **11**
7.1 General 11
7.2 Specification of required information on core privacy and data protection characteristics of LA system 11
7.2.1 Core LA privacy and data protection requirements 11
7.2.2 Institutional code of practice for use of LA 12
7.2.3 Information collection principles for LA 13
7.2.4 Information processing principles 13
7.2.5 Information dissemination principles for LA 15
7.3 Principles and data requirements for consent to share data for learning analytics 15
7.3.1 General requirements 15
7.3.2 Timing of consent 16
7.3.3 Consent frameworks and types of consent 17
7.3.4 Minimum data requirements for documentation of consent 17
7.4 Accountability and governance related to privacy and data protection for LA 18
Bibliography **19**

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 36, *Information technology for learning, education and training*.

A list of all parts in the ISO/IEC 20748 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.

Introduction

The ISO/IEC 20748 series clarifies and regularizes the behaviour of components related to learning analytics interoperability. Privacy and data protection are identified as important cross-cutting requirements impacting all sub-processes of learning analytics (LA). Even if privacy and data protection are regulated by law in some jurisdictions, there is a need to specify privacy requirements as part of this series to establish principles that can influence design and operation of learning analytics systems.

The concepts of privacy and data protection are used differently around the world. In this document, which is designed to be used in an educational setting, 'privacy and data protection' are used as one concept to capture both the social and contextual aspects of privacy and the more technical and managerial aspects of data protection for learning, education and teaching (LET). Privacy and data protection requirements for learning analytics can be derived from multiple sources, both written and non-written, including educational policy frameworks, ICT infrastructure principles, international privacy frameworks (e.g., OECD, APEC, European Union), trade agreements, national legal frameworks, ethical principles observed in LET, etc. These requirements are often expressed as high level principles that different constituencies could agree upon. This document develops detailed privacy and data protection attributes pertaining to the learning analytics process cycle (described in ISO/IEC TR 20748-1). This document enables the development of LA privacy and data protection attribute specifications, which detail how information exchange should be performed to fulfil the aims of LA operations without compromising privacy and data protection of the individual.

This document is intended to inform system developers in designing LA systems and processes supporting inclusive privacy and data protection policies. The primary beneficiaries of privacy and data protection policies are the individuals who share their PII, in this case the students (and their parents or guardians), teachers and other actors who take part in learning, education and training. Educational organizations and third party providers are also target user groups.

Information technology for learning, education and training — Learning analytics interoperability —

Part 4: Privacy and data protection policies

1 Scope

This document specifies privacy and data protection requirements and attributes to inform design of learning analytics systems and learning analytics practices in schools, universities, workplace learning and blended learning settings.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
accountability
principle that individuals, organizations, and the community are responsible for their actions and may be required to explain them to others

[SOURCE: ISO/TS 14441:2013, 3.1, modified — Note 1 to entry has been deleted]

3.2
anonymization
process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

[SOURCE: ISO/IEC 29100:2011, 2.2]

3.3
consent
process that provides the data subject (learner, teacher, instructor, or other natural person participating in LET) with explanations that will help that data subject in making educated decisions about whether to begin or continue participating in data collection, use or disclosure of personally identifiable information (PII) (3.9)

Note 1 to entry: Consent is an ongoing, interactive process over the lifetime of the data rather than a one-time information session.

Note 2 to entry: For the collection, use or disclosure of PII for individuals who are not of legal age or cannot consent for other reasons, depending on the nature of the data, additional consent requirements may apply, e.g., permission from a responsible adult or guardian.

3.4
data controller
natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of PII

[SOURCE: Adapted from GDPR Article 4(7)]

3.5
data protection
technical and social regimen for negotiating, managing, and ensuring informational privacy, confidentiality, and security

[SOURCE: ISO/TS 14265:2011, 2.9]

3.6
learning analytics
LA
measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimizing learning and the environments in which it occurs

[SOURCE: ISO/IEC TR 20748-2:2016, 3.12]

3.7
learning analytics service
system that aggregates and analyses learner data that is collected when learners interact with a platform and software

3.8
personally identifiable information
PII
any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

[SOURCE: ISO/IEC 29100:2011, 2.9, modified — Note 1 to entry has been deleted]

3.9
PII actor
stakeholder involved in the processing of PII

Note 1 to entry: According to ISO/IEC 29100:2011, 4.2 there are four types of actors who can be involved in the processing of PII: PII principals, PII controllers, PII processors and third parties.

3.10
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes

[SOURCE: ISO/IEC 29100:2011, 2.10, modified — Note 1 to entry has been deleted]

3.11
PII principal
natural person to whom the personally identifiable information (PII) relates

[SOURCE: ISO/IEC 29100:2011, 2.11, modified — Note 1 to entry has been deleted]

3.12
PII processor
privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.13
privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual

3.14
privacy policy
overall intention and direction, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting

[SOURCE: ISO/IEC 29100:2011, 2.16]

3.15
privacy and data protection attribute
learning analytics privacy and data protection attribute
LA privacy and data protection attribute
specification of a privacy and data protection requirement related to a learning analytics process

3.16
pseudonymization
de-identification technique that replaces an identifier (or identifiers) for a data principal with a pseudonym in order to hide the identity of that data principal

[SOURCE: ISO/IEC 20889:2018, 3.27]

3.17
sensitive data
data with potentially harmful effects in the event of disclosure or misuse

[SOURCE: ISO 5127:2017, 3.1.10.16]

3.18
sensitive PII
category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal

Note 1 to entry: In some jurisdictions or in specific contexts, sensitive PII is defined in reference to the nature of the PII and can consist of PII revealing the racial origin, political opinions or religious or other beliefs, personal data on health, sex life, or criminal convictions, as well as other PII that might be defined as sensitive.

[SOURCE: ISO/IEC 29100:2011, 2.26]

4 Abbreviated terms

APEC	Asia-Pacific Economic Cooperation
FERPA	Family Educational Rights and Privacy Act (USA)
GDPR	General Data Protection Regulation (of European Union)
LA	learning analytics
LET	learning, education and training
OECD	Organization for Economic Co-operation and Development
PII	personally identifiable information

5 Privacy and data protection requirements

5.1 General

As the field of privacy and data protection for learning analytics is new and evolving, the specifications in this document will only address a subset of all issues an organization needs to handle in setting up a learning analytics service. This document comprises discussion of requirements (Clause 5), a set of privacy and data protection attributes (Clause 6) and a number of attributes selected for further specification (Clause 7).

5.2 The concept of privacy and data protection in LET

What privacy entails is difficult to define restrictively as privacy means different things in different countries around the world. What is seen as an intrusion into the private life or affairs of an individual, and whether gathering of data about the individual is seen as undue or illegal, varies with cultural context.

The approach taken in this document is, therefore, to look at privacy problems in a LET context to be able to specify privacy and data protection principles for LET that address specific problems and support a good learning environment for the individuals involved.

Privacy is the right of an individual to keep oneself and one's information concealed or hidden from unauthorized access and view of others. The composite concept of privacy and data protection used in this document refers to the capacity to control when, how and to what degree information about a person is communicated to others in a particular context or setting. The capacity to control can lie with the individual, with the context, or both.

Some information is, however, of a more sensitive nature and is, in many jurisdictions, subject to special protections. Such *sensitive data* may include racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic or biometric data, health data, or data concerning sex life or sexual orientation.

NOTE ISO/IEC 29100:2011, Table 2 gives a list of examples of attributes that can be used to identify natural persons, some of them being sensitive personally identifiable information.

Use of sensitive data in LET implies a greater risk against privacy and data protection; therefore, in LA, sensitive data should play a limited role and be used only after explicit consent is given by the individual.

Often in learning, education and training, long-term, deep relationships are built between the student and teachers, fellow students, etc. where PII is exchanged. These relationships are potentially of great benefit for the individual; however, in some cases, the release of PII could also be of great harm. Therefore, handling of PII by the educational institution must be justified by clearly stated principles.

In LET, we find a variety of justifications for processing data about a person (e.g., consent, contract, legal obligations, vital interests, public interests, and legitimate interests of the organization). Lack of clarity of justification for collection of data about a person can threaten privacy and data protection; as can other issues that are typical for LET:

Justification of collecting data: The data processor or data controller (e.g., institution, teacher, researcher) could have a legitimate interest (and their own justification) to process data about a person; however, the limits to the resulting permission to process data (by enrolment to school, a course, etc.) might not be clear.

Purpose of processing data: If collection of student data is limited to support for learning, using the data to sell things to students is excluded. However, the scope of learning is unlimited, which makes further purpose limitation difficult.

When to ask for consent: Learning consists of an infinite number of small steps, often interacting with others over time. Some of these steps involve acting on the analysis of data that the individual should

have consented to being collected and processed. However, sometimes data processing is the right of the organization as part of a contract. To offer consent to an individual when the institution already has the right to process such data is wrong. To act on processed data when the individual should have the opportunity to consent to be involved is also wrong. In long-term and close relationships, as in LET, it is not always easy to draw the line between these two scenarios.

Notification: Age of the students, the educational setting, matters of authority, and other reasons could influence how notification of data collection and processing will be conceived. The educational context is, however, an opportunity to clarify privacy and data protection issues related to use of LA.

In LET, privacy and data protection is accomplished by the application of a set of fair information principles which seek to ensure that:

— only accurate, relevant and timely information (personal and otherwise) is collected and/or exchanged among the actors involved in LET;

— all uses of information are known and appropriate;

— personally identifiable information (PII) is protected.

There are some aspects of LET that will impact on how privacy and data protection will be dealt with in this setting:

— Attending school might be mandatory. In that case, the school is authorized by law or by the context to collect and process data about the student.

— In many cases, education is based on a long-term relationship, to institutions, teachers, fellow students, and others. This might impact on how long data can be kept.

— In most LET settings we find persons with the role to protect students and to know more about potential threats to the individual.

— For underage students, parents have the right to be involved in many questions that concern privacy and data protection for students.

— Learning and knowledge-seeking are without boundaries, the unplanned and unexpected will impact the student journey. Therefore, it is difficult to limit in advance the purpose of collecting data from learning activities.

— Experimentation, play and identity testing is part of education. Therefore, PII is more likely to be shared in educational settings than in settings with a more defined set of roles, e.g., the workplace.

— Openness and trust play an important role in LET. Therefore, in a good learning environment one finds more information about persons than in settings where there is less openness and trust.

These requirements should be further developed, keeping sound pedagogical principles in mind, based on the emergence and evolution of proper practice in the field of learning analytics. It should also be noted that even if students are the primary stakeholders of LET, data will also be collected about teachers and others supporting learning. The privacy and data protection interests of all parties should also be appropriately addressed.

In general, these challenges to privacy and data protection in LET settings present the following high level requirements to ICT systems:

— Support for transparency giving the actors in LET insights into how PII is handled in different systems.

— A processing regimen that allows the individual, where appropriate, to actively manage PII considering age, educational context and legal requirements.

— Data protection policies and systems ensuring privacy, confidentiality and security.