FINAL
DRAFT

TECHNICAL SPECIFICATION

ISO/IEC DTS 27560

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2023-03-30

Voting terminates on:
2023-05-25

Privacy technologies — Consent record information structure

Reference number
ISO/IEC DTS 27560:2023(E)

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 had 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 27, *Information security, cybersecurity and privacy protection*.

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

This document specifies requirements and guidelines for organizations to record information about:

— consent obtained from individuals prior to collecting and processing personally identifiable information (PII); and

— the means by which individuals keep track of such content.

ISO/IEC 29184 specifies controls which shape the content and the structure of online privacy notices, and the process of asking for consent to collect and process PII from PII principals. ISO/IEC 29184 is focused on the obligations of the PII controller, or entities processing PII on behalf of the PII controller, to inform PII principals of how their PII is processed. ISO/IEC 29184 does not address the needs of PII principals.

This document builds upon ISO/IEC 29184 by addressing the concept of giving the PII principal a record for their own recordkeeping, which includes information about the PII processing agreement and interaction. We call this record the “consent receipt”.

This document specifies a structure that is used by both principals in consent management: an organization that keeps records with good integrity (subject to the defined controls), and an artefact (the “consent receipt”) that is given to the individual whose PII is being processed.

This document does not specify an exchange protocol for consent records or consent receipts, nor structures for such exchanges.

Privacy technologies — Consent record information structure

1 Scope

This document specifies an interoperable, open and extensible information structure for recording PII principals' consent to PII processing. This document provides requirements and recommendations on the use of consent receipts and consent records associated with a PII principal's PII processing consent, aiming to support the:

— provision of a record of the consent to the PII principal;

— exchange of consent information between information systems;

— management of the life cycle of the recorded consent.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes 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 29100:2011, *Information technology — Security techniques — Privacy framework*

ISO/IEC 29184:2020, *Information technology — Online privacy notices and consent*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29100, ISO/IEC 29184 and the following apply.

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

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

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

3.1
consent
personally identifiable information (PII) principal's freely given, specific, and informed agreement to the processing of their PII

Note 1 to entry: Consent is a freely given and unambiguous decision or a clear affirmative action of a PII principal by which the PII principal, after being informed about a set of terms for the processing of their PII, denotes an agreement to this processing.

Note 2 to entry: Processing of PII refers to operations such as its collection, use, disclosure, storage, erasure, or transfer.

[SOURCE: ISO/IEC 29100:2011, 2.4, modified – Notes 1 and 2 to entry have been added]

3.2
consent receipt
information issued or provided as an acknowledgement of consent record(s), which may contain a reference to the records and information within it

Note 1 to entry: The consent receipt is intended to facilitate inquiries or complaints by the personally identifiable information (PII) principal about the processing of PII, and for the PII principal to exercise rights related to their PII.

3.3
consent record
information record describing a personally identifiable information (PII) principal's consent for processing of their PII, and the time and manner of a PII principal's acceptance of PII processing notice

3.4
consent type
description of the way in which consent is expressed by the personally identifiable information (PII) principal

Note 1 to entry: The criteria or conditions associated with consent type can be derived from laws, regulations, standards, and domain-specific guidelines.

Note 2 to entry: Commonly used types for consent are: explicit, explicitly expressed and implied. See ISO/IEC 29184:2020, 3.1 for further details.

4 Abbreviated terms

ASCII American Standard Code for Information Interchange

GDPR general Data Protection Regulation

HMAC hash-based message authentication code

JSON JavaScript object notation

UTF unicode transformation format

UUID universally unique identifier

5 Overview of consent records and consent receipts

5.1 General

PII principals are often asked to provide PII by organizations who want to process information about them. A PII principal can consent to the collection and processing of PII. A standardized record of a consent enhances the ability to maintain and manage permissions for personal data by both the PII principal and the PII controller. This document describes an extensible information structure for recording a PII principal's consent to data processing.

This document elaborates on the example presented in ISO/IEC 29184. See Annex H for the mapping between the clauses of this document and those in ISO/IEC 29184.

5.2 Consent record

A consent record documents the PII principal's decision regarding consent to process their PII. Prior to collecting and processing PII, PII controllers typically present a privacy notice describing the proposed processing of PII and relevant information such as relevant privacy rights. The PII principal can decide to provide their PII for processing. The PII controller can then document that decision and its context in

the form of a consent record, to satisfy their regulatory obligations and recordkeeping requirements. The PII controller defines the detailed structure.

See Annex A for an example of a consent record in JSON format.

5.3 Consent receipt

A consent receipt is an authoritative document providing a reference to a consent record, or information contained therein. Receipts are intended for entities to share information regarding consent, such as a PII controller giving the PII principal a receipt regarding their given consent and its associated processing. Receipts enable stakeholders such as PII principals to keep their own records and to ensure that the consent decisions are acknowledged by relevant entities such as the PII controller. Receipts also facilitate inquiries or complaints, such as from a PII principal to a PII controller or an authority regarding consent or rights associated with their PII.

See Annex A for an example of a consent receipt in JSON format.

6 Elements of a consent record and consent receipt

6.1 Overall objectives

The first overall objective of this document is to describe consent record as an information structure for recordkeeping activities related to:

— the PII requested by a PII controller to perform certain activities;

— the provision of notices that indicate which treatments or uses of the PII will be made by the PII controller and possibly other third parties;

— the reception of PII by the PII controller because it is either provided directly by the PII principal, or derived or inferred from existing PII, or obtained from a third party; and

— the dates when: the PII is requested by the PII controller, the PII principal gives consent, and the PII is received by the PII controller.

A second overall objective of the document is to describe consent receipt as an information structure for the optional transmission of PII controller to a PII principal. It either refers to a consent record or contains information from a consent record. This information can be used by the PII principal independent of the PII controller to form the basis for the PII principal's personal recordkeeping activities.

See Annex D for storage and transmission information of consent records.

See Annex G for guidance to implementors of ISO/IEC 27701.

6.2 Recordkeeping for online privacy notices and consent

6.2.1 General

This clause describes requirements for recording details of online privacy notices and consent exchanged by a PII controller and the PII principal prior to commencement of PII processing. This clause also describes requirements for recording sufficient details to enable ongoing reference to the notice provided in accordance with ISO/IEC 29184:2020, 6.2.8 and to enable management of changing conditions with respect to the notice and consent in ISO/IEC 29184:2020, 6.5.

6.2.2 PII controller recordkeeping

6.2.2.1 Presentation of notice — control

The organization shall keep records of the specific version or iterations of a notice as it was presented to the PII principal. Such records shall be kept in a format and manner that provide assurances that the records' integrity is maintained over time and accurately reflects the notice, its contents, and context of use at the time of presentation to the PII principal.

6.2.2.2 Timeliness of notice — control

The organization shall keep records of the time of and the manner in which the notice was presented, and if available, the location.

NOTE The content of notices is described in ISO/IEC 29184:2020, 5.3.

6.2.2.3 Obtaining consent — control

Where consent is the basis for PII processing, the organization shall keep records of the consent obtained from the PII principal in a format and manner that provides assurances that the records' integrity is maintained over time and accurately reflects the activities related to obtaining consent.

6.2.2.4 Time and manner of consent — control

The organization shall keep records of the time of and the manner in which the consent was obtained, and if available, the location.

6.2.2.5 Technical implementation — control

Technical implementation shall include communication, storage, security, serialization, modelling, language selection, and other activities related to maintenance of records and its information described in this document (see 6.3).

See Annex C for information on performance and efficiency considerations.

See Annex E for security of consent records and receipt.

6.2.2.6 Unique reference — control

The organization shall assign, maintain and use unique references to the specific version of information within a consent record where such information is expected to change over time.

NOTE An example of information present within consent records that can change over time includes privacy notices, where the unique reference refers to the specific version applicable at the time of record creation.

6.2.2.7 Legal compliance — control

The organization shall determine and document how its activities and processes comply with requirements for processing of PII. Where consent records are used to demonstrate legal compliance, the organization shall keep records of specific legal requirements which can apply and their relationship to the information provided in consent records.

6.2.3 Recordkeeping for consent receipts

6.2.3.1 Provision of consent receipt — control

The organization shall make available information on how the PII controller transmits the consent record or consent receipt to the PII principal.

NOTE 1 This control refers to creation and transmission of the consent receipt from PII controller to PII principal. The PII principal is then able to establish and maintain their own independent records.

NOTE 2 A consent record also serves to demonstrate compliance where consent is used as the legal basis for processing activities in some jurisdictions.

NOTE 3 See Annex F for signals as controls communicating the PII principal's preferences and decisions.

6.2.3.2 Contents of consent receipts — control

The information provided as a consent receipt can include some or all of the information present in the consent record.

NOTE The PII controller decides the contents of the consent receipt, balancing operational requirements and the rights of the PII principal for an independent copy of the consent record.

6.2.3.3 Integrity of consent receipts — control

The information provided as a consent receipt may include information integrity controls to hinder modification.

6.2.3.4 Technical implementation — control

The organization shall determine and document how its implementation of consent receipts conforms to information requirements related to consent records as described in 6.3.

NOTE Technical implementation includes data serialization, data modelling, language selection and other activities.

6.2.3.5 Unique reference — control

The organization shall assign, maintain, and use unique references to the specific version of information within a consent receipt where such information is expected to change over time.

NOTE An example of information present within consent records or consent receipts that can change over time includes privacy notices, where the unique reference refers to the specific version applicable at the time of record creation.

6.2.3.6 Accuracy and verifiability — control

The organization shall ensure information provided in the consent receipt is accurate, accountable, and verifiable.

NOTE The PII principal can utilize the consent receipt in contexts other than communication with the PII controller.

6.2.3.7 Use of receipts by PII principal — control

The organization shall make available information necessary for the PII principal to interpret, comprehend, and use the consent receipt.

Where the consent receipt is provided in a machine-readable format, the receipt interpretation information may be given directly or given by reference.

6.2.4 Relationship between records and receipts — control

The organization shall include sufficient information in the consent receipt such that the PII principal is able to communicate about the related consent record and its context as referenced by the receipt. Based on information in the receipt, the PII principal can inform the PII controller or a regulator of the context of an inquiry, complaint or exercise of rights, even if the original consent record managed by the PII controller is no longer available.

NOTE 1 The amount of information replicated between the consent record and consent receipt is determined by the PII controller. If the replicated information is minimal, then the PII controller assumes that the PII principal trusts the PII controller to maintain the availability and integrity of the records over time.

NOTE 2 The consent receipt is intended to facilitate inquiries or complaints by the PII principal about the processing of PII, and for the PII principal to exercise rights related to their PII.

6.3 Record information structure

6.3.1 General

This clause describes requirements for the consent record information structure.

NOTE Annex A provides examples in JSON and JSON-LD formats of consent record structure and its contents.

6.3.2 Structure of the consent record

6.3.2.1 Consent record schema — control

Where the organization creates its own schema for the implementation of consent records, it shall publish or reference the schema(s) being used and maintain documentation necessary for its correct technical implementation and conformance to the requirements specified in this document.

6.3.2.2 Structure of consent record — control

The consent record should be organized into six sections:

— record header section;

— PII processing;

— event;

— purposes;

— PII information section; and

— party identification section.

The organization should document the expected (or acceptable) syntax, values and forms for each field when creating schemas or utilizing them in technical implementations.

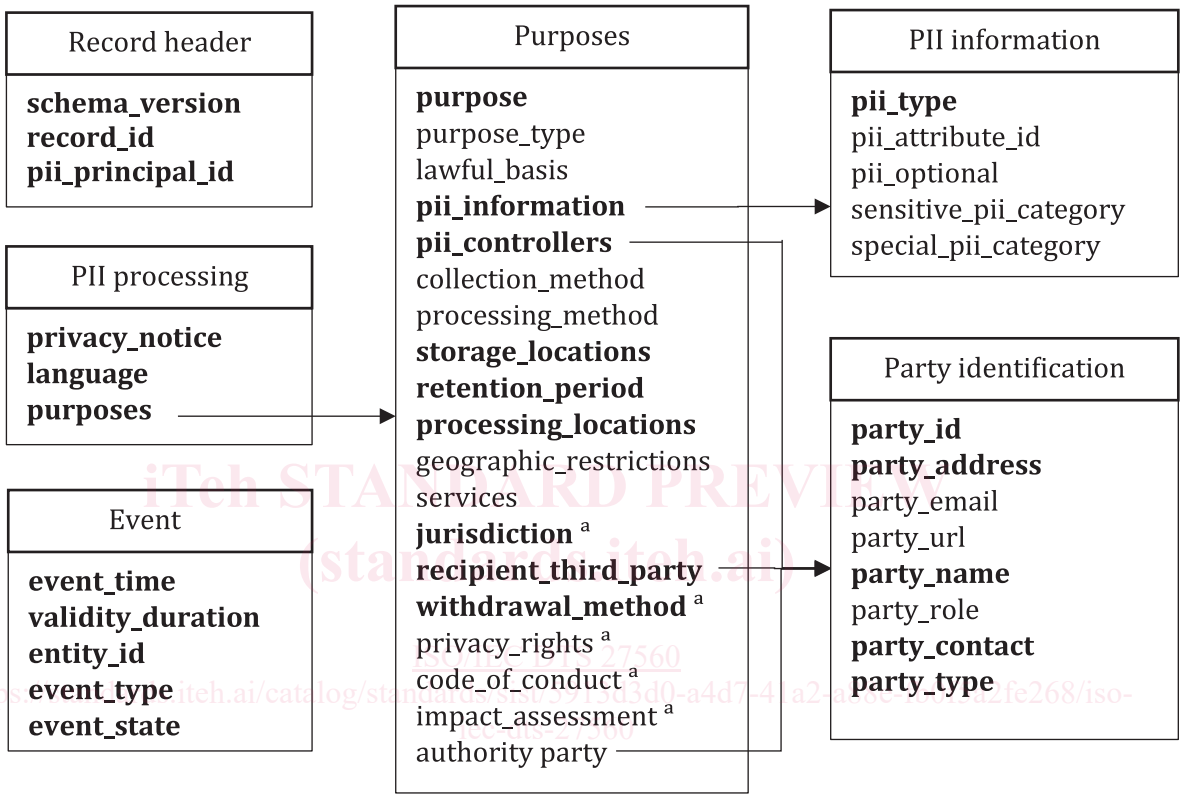
NOTE 1 The structure of the record, consisting of its sections, fields, and their expected formats and values, is collectively referred to as a "schema" so as to permit declaring information about the representation of fields in a record for its correct technical interpretation.

NOTE 2 Implementers can organize the structure of record and receipt fields within their schema according to the implementers' operational needs.

Figure 1 shows one representation of fields in a technical implementation. The "purposes" section in Figure 1 represents the fields which are directly related to the purposes.

The PII controller may have one or more services each with its own list of purposes. Separate records may be created with a single service and one purpose, or they may be combined all within one record. If the record contains multiple purposes the recorded event applies to all the purposes.

This document makes no recommendation to combine or have separate records. Implementers shall organize record contents for the most optimal management of the life cycle of the record and receipt (see Annex B). In addition, implementors may choose to make optimizations. For example, avoiding duplication of information by reorganizing or restructuring the storage and utilization of records by using common references.



Key

[a] These fields can be included under the PII controller party's identification section instead of under the purpose section, but this document does not prescribe which option is used and which is left for implementation. Refer to requirements and recommendations associated with the field.

NOTE Fields in bold are required fields.

Figure 1 — Record schema overview

6.3.3 Record header section contents

6.3.3.1 General

Table 1 summarizes the structure and contents of the record header section.

Table 1 — Record header section

Data element identifier	Description	Presence
schema_version (see 6.3.3.2)	A unique reference for the implementation documentation describing interpretation of the record structure and contents in conformance with this document.	Required
record_id (see 6.3.3.3)	A unique reference for a record.	Required
pii_principal_id (see 6.3.3.4)	The identifier or reference to the PII principal whose PII will be processed.	Required

6.3.3.2 schema_version

This refers to a unique reference for the implementation documentation describing interpretation of the record structure and contents in conformance with this document.

NOTE The interpretation of record structure and contents is based on the use of unique schema_version for each updated record structure.

The presence of schema_version is required.

Recommended encoding format: string

See ISO/IEC 29184.

Requirements and guidance: The schema_version shall refer to the specific version of PII controller implementation documentation in effect at the time the record is created.

6.3.3.3 record_id

This refers to a unique reference for a record.

The presence of record_id is required.

Recommended encoding format: UUID-4[9]

See ISO/IEC 29184.

Requirements and guidance: The record_id is used by parties to the notice and consent interaction, to identify and refer to the record. Record IDs shall be unique within the relevant context to enable identifying records explicitly. While utilizing suggested formats such as UUID-4, which have a low probability of collisions between identifiers, the entity creating the consent record should ensure identifier uniqueness.

6.3.3.4 pii_principal_id

This refers to the identifier or reference to the PII principal whose PII will be processed.

The presence of pii_principal_id is required.

Recommended encoding format: string

See ISO/IEC 29184.

Requirements and guidance: A consent record shall contain an identifier through which the consent (and its record) is associated with a PII principal. Where such identifiers are not created or provided by the PII principal or PII controller, one shall be created for the sole purpose of uniquely specifying the PII principal within the record.

Organizations should consider using measures to protect the identity of the PII principal through using mechanisms such as pseudonyms or decentralized identifiers (DID).

In cases where consent is granted by a PII principal without identifying themselves and where no other means are available to associate the consent to the PII principal, the value of pii_principal_id should be a newly generated identifier specific to that consent record, so as to uniquely associate the consent to a PII principal.

6.3.4 PII processing section contents

6.3.4.1 General

Table 2 summarizes the structure and contents of the PII processing section.

Table 2 — PII processing section contents

Data element identifier	Description	Presence
privacy_notice (See 6.3.4.2)	Identifier or reference to the PII controller's privacy notice and applicable terms of use in effect when the consent was obtained, and the record was created.	Required
language (See 6.3.4.3)	Language of notice and interface related to consent.	Required
purposes (See 6.3.4.4)	PII can be associated with multiple purposes that do not share the same lawful basis.	Required
purpose (See 6.3.4.5)	The purpose for which PII is processed.	Required
purpose_type (see 6.3.4.6)	A broad type providing further description and context to the specified purpose for PII processing.	Optional
lawful_basis (See 6.3.4.7)	The lawful basis for processing personal data associated with the purpose.	Optional
pii_information (See 6.3.4.8)	A data structure that contains one or more PII type values where each type represents one attribute.	Required
pii_controllers (See 6.3.4.9)	A data structure that contains one or more party_identifier values where each identifier represents one PII controller.	Required
collection_method (See 6.3.4.10)	A description of the PII collection methods that will be used.	Optional
processing_method (See 6.3.4.11)	How the PII will be used.	Optional
storage_locations (See 6.3.4.12)	The geo-locations of where the data will be physically stored.	Required
retention_period (See 6.3.4.13)	The PII controller shall provide information about the retention period and/or disposal schedule of PII that it is collecting and processed.	Required
processing_locations (see 6.3.4.14	The locations or geo-locations of where the PII will be processed if different from storage_location.	Optional