PD ISO/IEC TS 27560:2023

BSI Standards Publication

Privacy technologies — Consent record information structure

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 27560:2023

National foreword

This Published Document is the UK implementation of ISO/IEC TS 27560:2023.

The UK participation in its preparation was entrusted to Technical Committee IST/33/5, Identity Management and Privacy Technologies.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 28510 9

ICS 35.030

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 September 2023.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 27560:2023

TECHNICAL SPECIFICATION

ISO/IEC TS 27560

First edition
2023-08

Privacy technologies — Consent record information structure

Technologies pour la protection de la vie privée — Structure de l'information d'enregistrement du consentement

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

Documents
Document Sharing Hub
© ISO/IEC 2023

Full document details: PD ISO/IEC TS 27560:2023

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 27560:2023

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **2**
5 Overview of consent records and consent receipts **2**
5.1 General 2
5.2 Consent record 2
5.3 Consent receipt 3
6 Elements of a consent record and consent receipt **3**
6.1 Overall objectives 3
6.2 PII controller recordkeeping 3
6.2.1 General 3
6.2.2 Record keeping for consent records 4
6.2.3 Recordkeeping for consent receipts 5
6.2.4 Relationship between records and receipts — control 6
6.3 Record information structure 6
6.3.1 General 6
6.3.2 Structure of the consent record 6
6.3.3 Record header section contents 7
6.3.4 PII processing section contents 9
6.3.5 PII information 17
6.3.6 Party identification section contents 19
6.3.7 Event section contents 21
6.4 Receipt information structure 23
6.4.1 General 23
6.4.2 Structure of the receipt — control 23
6.4.3 Consent management — control 23
6.4.4 PII principal participation — control 23
6.4.5 Receipt metadata section contents 24
6.4.6 Receipt content — control 24
Annex A (informative) **Examples of consent records and receipts** **25**
Annex B (informative) **Example of consent record life cycle** **29**
Annex C (informative) **Performance and efficiency considerations** **33**
Annex D (informative) **Consent record encoding structure** **38**
Annex E (informative) **Security of consent records and receipts** **39**
Annex F (informative) **Signals as controls communicating PII principal's preferences and decisions** **41**
Annex G (informative) **Guidance on the application of consent receipts in the context of privacy information management systems** **43**
Annex H (informative) **Mapping to ISO/IEC 29184** **50**
Bibliography **52**

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

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.

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

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: namely a specification for data to be held by the organization to allow record-keeping 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.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TS 27560:2023

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]

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

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 their 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

PII personally identifiable information

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

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

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 a 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 information on the consent record encoding structure.

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

6.2 PII controller recordkeeping

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.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

6.2.2 Record keeping for consent records

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 consent records 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 and Annex D for consent record encoding structures.

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.

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

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

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 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, traceable, 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.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

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 If the amount of information replicated between the consent record and consent receipt is minimal, then the PII controller assumes that the PII principal will trust the PII controller to maintain the availability and integrity of the consent records over a given period of time, as indicated by the organization.

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.

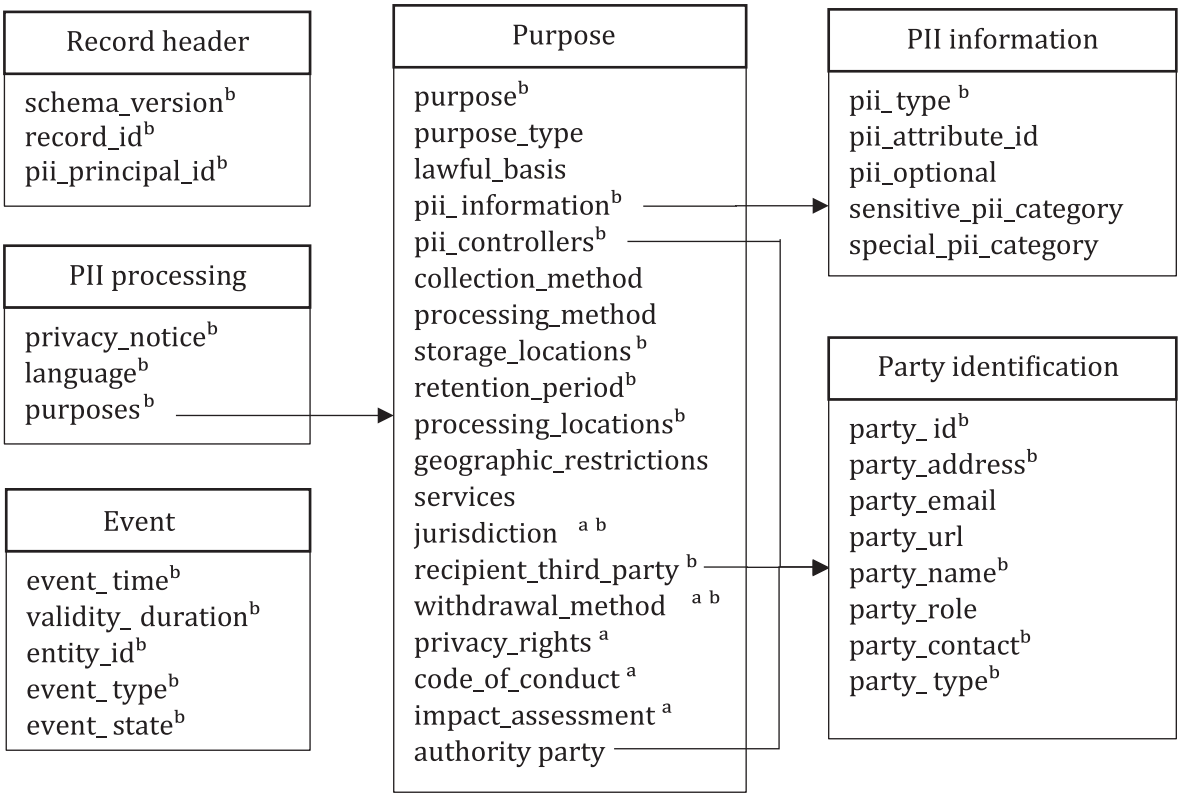
NOTE 2 Implementers can organize the structure of record and receipt fields within their schema according to the implementers' operational needs.

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 for PII processing.

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

The PII controller may have one or more services each with its own list of purposes for the PII processing. 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 consent record and consent 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. This document does not prescribe which option is used, leaving that as an implementation decision. Refer to requirements and recommendations associated with the field.

b These fields are mandatory.

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.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

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.

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

Organizations should consider using measures to prevent identification of the PII principal through using mechanisms such as pseudonyms.

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.

An account identifier, where available, may be used as a pii_principal_id, and where relevant pseudonymised.

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 collected and processed.	Required

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

Table 2 *(continued)*

Data element identifier	Description	Presence
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
geographic_restrictions (see 6.3.4.15)	Geographic restrictions for processing of personal data.	Optional
services (see 6.3.4.16)	A service or business process within which the purpose of PII processing is applied or interpreted.	Optional
jurisdiction (see 6.3.4.17)	The legal jurisdictions governing the processing of PII.	Required
recipient_third_parties (see 6.3.4.18)	A data structure where each entry describes a third party in terms of identity, geo-location of data transfer, and whether it constitutes a jurisdictional change.	Required
withdrawal_method (see 6.3.4.19)	Indicates information or link on how and where the PII principal can withdraw this consent.	Required
privacy_rights (see 6.3.4.20)	Indicates information or location on how and where the PII principal can exercise their privacy rights.	Optional
codes_of_conduct (see 6.3.4.21)	The PII controller may follow a code of conduct which sets the proper application of privacy regulation taking into account specific features within a sector.	Optional
impact_assessment (see 6.3.4.22)	The PII controller may perform a privacy assessment in order to determine privacy risks and potential impacts of non-compliance on the PII principals.	Optional
authority_party (see 6.3.4.23)	Information about the authority or authorities to whom the PII principal can issue an inquiry or complaint with regards to the processing of their data and exercising of rights.	Optional

6.3.4.2 privacy_notice

This refers to an identifier or reference to the PII controller's privacy notice in effect when the consent was obtained, and the record was created. If a privacy notice changes, the reference specified within the record should continue to point to the version in effect when the record was created.

The presence of privacy_notice is required.

Recommended encoding format: URL.

See ISO/IEC 29184:2020, 5.2.8.

Requirements and guidance: The specific version of privacy notice provides context for the consent obtained. The URL identifier may reflect an identifier for the notice.

6.3.4.3 language

This refers to the language of notice and interface related to consent.

The presence of language is required.

© ISO/IEC 2023 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023

Recommended encoding format: ISO 639-1.

See ISO/IEC 29184:2020, 5.2.4.

Requirements and guidance: none.

6.3.4.4 purposes

PII can be associated with multiple purposes that do not share the same lawful basis. Where such PII is specified in a consent record, the organization shall ensure the PII principal is aware of the other purposes and lawful basis.

The presence of purposes is required.

Recommended encoding format: array.

See ISO/IEC 29184:2020, 5.3.2 and 5.3.3.

Requirements and guidance: There can be multiple purposes for processing PII information, legal, business requirements, subscriptions, contractual and many more. For example, a covid-19 vaccination test centre, as the PII controller, can have two purposes for processing personal data: 1) a lawful basis for processing which is carried out in the public interest and 2) processing a special category of personal data to assess working capacity. These should be separate purposes.

NOTE 1 Based on the applicable jurisdiction(s), the specificity and scope of consent can require that consent be expressed for all purposes expressed in the record collectively or individually, with implications on utilization and possible revocation.

NOTE 2 For example, a medical centre can utilize phone numbers for the separate purposes to "send emergency health advice" with a lawful basis for the public interest and to "communicate appointment information" with the consent of the PII principal.

6.3.4.5 purpose

This refers to the purpose for which PII be processed.

The presence of purpose is required.

Recommended encoding format: string.

See ISO/IEC 29184:2020, 5.3.2 and 5.3.3.

Requirements and guidance: The description of the purpose should be sufficiently detailed and should not be ambiguous so as to enable the PII principal to obtain an overview of the intended processing of their PII.

6.3.4.6 purpose_type

This refers to a broad type providing further description and context to the specified purpose for PII processing.

The presence of purpose_type is optional.

Recommended encoding format: string.

See ISO/IEC 29184:2020, 5.3.2 and 5.3.3.

Requirements and guidance: For example, if the purpose, which should be as specific as possible, is “sending newsletters for new products and services”, this purpose is then accompanied with the type “marketing”. This is an abstraction and generalized description of the purpose and further clarifies that the purpose is a specific form of marketing.

© ISO/IEC 2023 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TS 27560:2023