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)

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: 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.

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 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

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.

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.

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.

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.

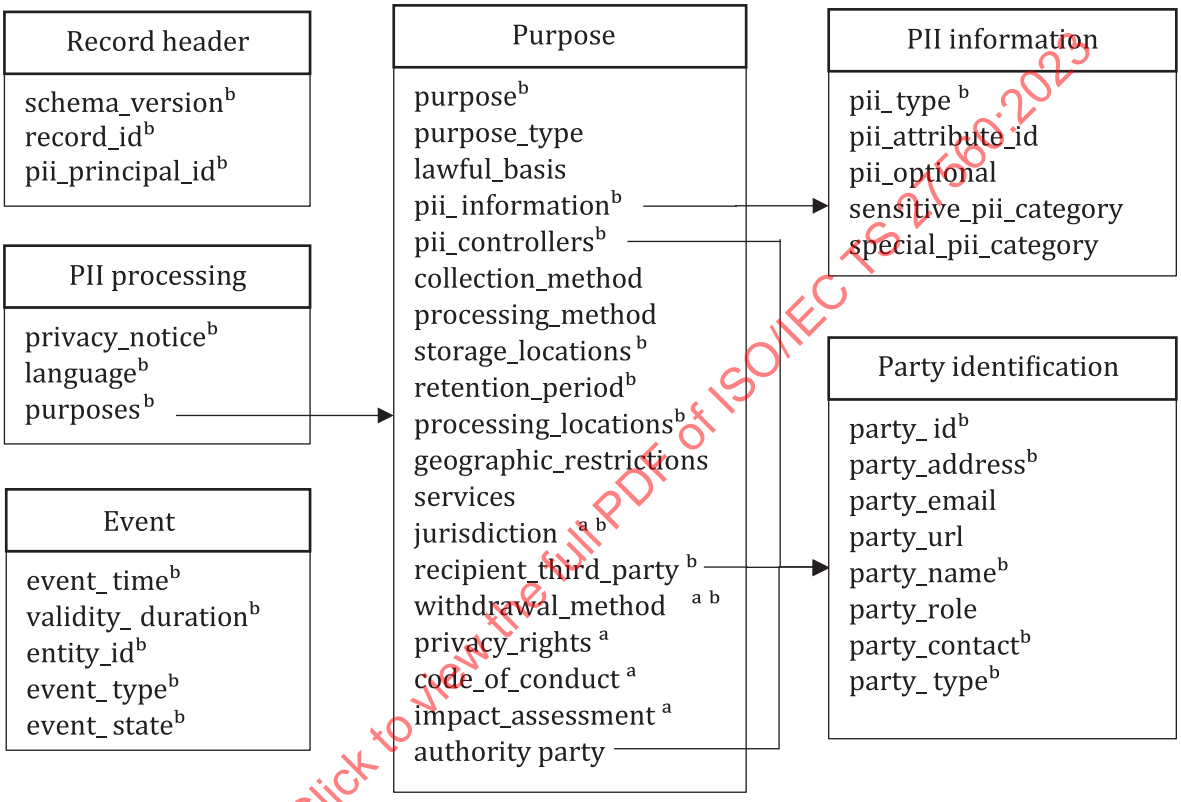
NOTE 1 The structure of the record, consisting of its sections, fields, and their expected formats and values, is collectively referred to as a "schema" so as to permit declaring information about the representation of fields in a record for its correct technical interpretation.

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.

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.

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 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

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.

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.

6.3.4.7 lawful_basis

This refers to the lawful basis used by the PII controller for justifying processing of PII stated in the record. The value of this field shall relate to consent.

The presence of lawful_basis is optional.

Recommended encoding format: string.

See ISO/IEC 29184:2020, 5.4.2.

Requirements and guidance: none.

6.3.4.8 pii_information

This refers to a data structure that contains one or more PII type values where each type represents one attribute. A corresponding PII information structure shall exist in the PII information section for each element.

The presence of pii_information is required.

Recommended encoding format: array of strings.

See ISO/IEC 29184:2020, 5.3.4.

Requirements and guidance: none.

6.3.4.9 pii_controllers

This refers to a data structure that contains one or more party_identifier values where each identifier represents one PII controller. A corresponding party identification structure shall exist in the party identification section for each element.

The presence of pii_controllers is required.

Recommended encoding format: array of strings.

See ISO/IEC 29184:2020, 5.3.4.

Requirements and guidance: If there are multiple PII controllers, the array shall list the PII controllers and joint controllers at the time of collecting or granting consent.

6.3.4.10 collection_method

This reference to a description of the PII collection methods that are applicable for the processing of PII described in the consent record.

The presence of collection_method is optional.

Recommended encoding format: array of strings.

See ISO/IEC 29184:2020, 5.3.5, 5.3.6 and 5.3.7.

Requirements and guidance: The collection method can be directly provided by an individual, observed for PII principal's activities, inferred from existing PII, or indirectly collected from a third party or obtained from another source.

6.3.4.11 processing_method

This is how the PII will be used. If the PII principal was informed of the processing operations employed by the PII controller(s) to process the PII, under the auspices of this consent, then that information may be recorded as part of the consent record.

The presence of processing_method is optional.

Recommended encoding format: array of strings.

See ISO/IEC 29184:2020, 5.3.8.

Requirements and guidance: Where the method of use includes creating or utilizing automated decision-making systems or large scale of processing or profiling, it can be necessary to provide information about these depending on legal jurisdictions.

6.3.4.12 storage_locations

This refers to the geo-locations of where the data will be physically stored.

The presence of storage_locations is required.

Recommended encoding format: array of strings.

See ISO/IEC 29184:2020, 5.3.9.

Requirements and guidance: PII may be stored on servers, devices, or in other forms. The PII controller should indicate the applicable locations of storage or their approximations. The location information is relevant for assessing and evaluating jurisdictional obligations regarding data transfers, storage, and dissemination.

6.3.4.13 retention_period

The PII controller shall provide information about the retention period and/or disposal schedule of PII that it is collected and processed.

The presence of retention_period is required.

Recommended encoding format: date and time format and duration format according to the ISO 8601 series.

See ISO/IEC 29184:2020, 5.3.11.

Requirements and guidance: The recommendation is to use either a date and time format in order to indicate a scheduled disposal (e.g. 2023-06-23T14:30) or a duration if PII information is continuously collected and disposed at a regular schedule (e.g. P3Y6M4DT12H30M5S). It is not necessary to include time (T) if the granularity is not required.

The information concerning the retention period and/or disposal schedule may be in the form of a specified period (e.g. 5 years) from the date of collection or processing, or from the occurrence of a specific event, or a specified date (e.g. to be disposed of on 1 January 2025). It may also consist of the criteria used to determine that period or schedule.

NOTE An organization can collect PII for multiple purposes. Depending on the purposes, the retention period can differ. As such, the data retention period can also be specified per purpose.

6.3.4.14 processing_locations

This refers to the locations or geo-locations where the PII will be processed if different from storage_locations.

The presence of processing_locations is optional.

Recommended encoding format: array of strings.

See ISO/IEC 29184:2020, 5.3.9.

Requirements and guidance: PII can be processed on servers. The PII controller should indicate the applicable locations of processing if different from storage_locations. The location information is relevant for assessing and evaluating legal obligations regarding data transfers, storage, and dissemination.

6.3.4.15 geographic_restrictions

This refers to the geographic restrictions for processing of personal data.

The presence of geographic_location is optional.

Recommended encoding format: array of strings.

See ISO/IEC 29184:2020, 5.3.9.

Requirements and guidance: The PII controller should indicate if there are any geographic restrictions in the processing of personal data for example, based on geo-location or jurisdiction restrictions. The restriction also applies to PII processors and third parties.

6.3.4.16 services

This refers to a service or business process within which the purpose of PII processing is applied or interpreted.

The presence of services is optional.

Recommended encoding format: reference to an array.

See ISO/IEC 29184.

Requirements and guidance: The services may be broken down into independent services offered by a PII controller. An example is an automotive business with a sales activity and rental business of their fleet of cars. To understand the use of service and its relation to purpose, consider the example where an organization provides an online video streaming service, within which it uses the user's location to personalise language and content. In this, the "online video streaming service" would be a service and the "personalisation of language and content" would be the purpose. While separation of service can aid in better management of records, both service and purpose can also be described within the description of a purpose, such as "personalisation of language and content for online video streaming service". Organizations shall determine the appropriate method for service and purpose description based on relevant factors such as their use-case, sufficient clarity of information, and any applicable requirements.

6.3.4.17 jurisdiction

This refers to the legal jurisdictions governing the processing of PII.

The presence of jurisdiction is required.

Recommended encoding format: string.

See ISO/IEC 29184:2020, 5.3.9.

Requirements and guidance: The scope and granularity of jurisdiction to be specified shall be determined by the PII controller based on requirements outlined in ISO/IEC 29100:2011, 4.5. The specification of a jurisdiction indicates the specific laws and regulations the PII controller acknowledges as being applicable and indicates what rights and mechanisms the PII principal may avail themselves of.

NOTE Examples of jurisdictions are countries specified using ISO 3166-1 and abbreviated terms such as those for European Union membership e.g. EU.

Requirements and guidance: This field may be included as part of PII controller party's identification (see 6.3.6) instead of under purpose (see 6.3.4.5). This document does not prescribe which option is used, leaving that as an implementation decision.

6.3.4.18 recipient_third_parties

This refers to 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. A corresponding third-party structure shall exist in the party identification section for each array element. If no PII information is shared, the array is empty.

The presence of recipient_third_parties is required.

Recommended encoding format: array of strings.

See ISO/IEC 29184:2020, 5.3.10.

Requirements and guidance: This field may be a group of third parties where information about the group's membership has been provided or made available to the PII principal.

6.3.4.19 withdrawal_method

This field indicates information or a link on how and where the PII principal can withdraw this consent.

The presence of withdrawal_method is required.

Recommended encoding format: string.

See ISO/IEC 29184.

Requirements and guidance: Depending on the jurisdiction of the PII controller and/or the PII principal, legal requirements can apply with regard to providing information on how the (given) consent is withdrawn by the PII principal. Therefore, the information or link specified within the withdrawal field can be connected to conformity with obligations and rights.

Requirements and guidance: The withdrawal of a record may produce an event with state terminated.

Requirements and guidance: This field may be included as part of PII controller party's identification (see 6.3.6) instead of under purpose (see 6.3.4.5). This document does not prescribe which option is used, leaving that as an implementation decision.

6.3.4.20 privacy_rights

This refers to instructions or location on how and where the PII principal may exercise their privacy rights.

The presence of privacy_rights is optional.

Recommended encoding format: array of strings.

See ISO/IEC 29184:2020, 5.3.13.

Requirements and guidance: Instructions on how to exercise privacy rights shall be provided in the link.

Requirements and guidance: The organization shall ensure the PII principal has been provided or is aware of information regarding the existence, applicability, and exercise of applicable rights. Organizations may provide the ability to update conditions of the consent (for example, modify the PII retention period) along with the ability to withdraw the consent. According to the jurisdiction of the PII controller and/or the PII principal, legal requirements can apply with regard to providing information on how the PII principal exercises their privacy rights. For example, when a PII principal withdraws

their consent or terminates a service, the record enters a withdrawn state, refer to event_state field. For consents that offer additional choices to users giving consent, the information or link specified within this field should allow additional choices to be changed.

Requirements and guidance: This field may be included as part of 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.

6.3.4.21 codes_of_conduct

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. The code of conduct shall refer to the name of the code of conduct and a publicly accessible reference to the code of conduct.

The presence of codes_of_conduct is optional.

Recommended encoding format: string.

See ISO/IEC 29184.

Requirements and guidance: The code of conduct does not require an assessment to ensure compliance but it may be conducted if available for the sector.

Requirements and guidance: This field may be included as part of 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.

6.3.4.22 impact_assessment

The PII controller may perform a privacy impact assessment or data protection impact assessment in order to determine privacy risks and potential impacts of non-compliance on the PII principals. The record shall indicate the latest assessment applicable at the time of creation along with the type of assessment (e.g. PIA or DPIA). The assessment instance is a reference to the latest assessment and shall include an assessment name (e.g. PIA or DPIA), when the assessment was signed off and reference to the assessment firm. If certification is provided for the assessment, it shall be included.

The presence of impact_assessment is optional.

Recommended encoding format: string.

See ISO/IEC 29184:2020, 5.2.7, 5.3.3, and 5.3.16.

Requirements and guidance: The impact_assessment field may be expressed as an URL or an identifier to a document. The location of an assessment report of the organization's privacy practices takes the form of an URL. It is potentially certified and associated with the receipt. The assessment should focus on risks and impacts, and the security practices used to manage PII. The impact assessment should identify risks and impacts of the specified processing and the adopted mitigation and their effectiveness. The specifics of this information shall be determined by the organization based on factors such as legal requirements.

NOTE Known risks are listed. It is the responsibility of each regulatory body to determine what type or risk merits are included.

Requirements and guidance: This field may be included as part of PII controller party's identification section instead of under Purpose section. This document does not prescribe which option is used, leaving that as an implementation decision.

6.3.4.23 authority_party

This refers to the information about the authority or authorities to whom the PII principal may issue an inquiry or complaint with regards to the processing of their data and exercising of their rights.

The presence of authority_party is optional.

See ISO/IEC 29184:2020, 5.3.13.

Requirements and guidance: PII controllers are expected to determine the suitable and appropriate authorities based on the applicable jurisdictions and provide information regarding their contact, applicability of rights and lodging complaints.

6.3.5 PII information

6.3.5.1 General

Table 3 summarizes the structure and contents of the PII information section.

Table 3 — PII information section

Data element identifier	Description	Presence
pii_type (see 6.3.5.2)	An explicit list of PII types, categories or elements to be processed for the specified purpose. The PII types shall be defined using language meaningful to the users and consistent with the purposes of processing.	Required
pii_attribute_id (see 6.3.5.3)	An unambiguous identifier to the attribute relating to the PII type.	Optional
pii_optional (see 6.3.5.4)	This field is used to indicate whether it was mandatory or optional for the PII principal to release the PII type for specified purposes.	Optional
sensitive_pii_category (see 6.3.5.5)	A PII controller may explicitly note if the PII type is considered sensitive where this has an impact on the consent or its use for the specified purpose, or in other contexts such as the sharing with other parties.	Optional
special_pii_category (see 6.3.5.6)	A PII controller may explicitly note if the PII type is considered special where it falls under the special category of highly impactful personal data based on requirements in the jurisdiction.	Optional

6.3.5.2 pii_type

This refers to an array of PII type, category or elements to be processed for the specified purpose. The PII types shall be defined using language meaningful to the users and consistent with the purposes of processing. The PII types may be represented implicitly, across all consent records of this type in the consent record handling system.

The presence of pii_type is required.

Recommended encoding format: array.

See ISO/IEC 29184.

Requirements and guidance: The PII categories expressed in this field shall be sufficiently clear and comprehensible to the PII principal.

Actual data shall not be conveyed in the pii_type field. For example, if the PII for which consent was granted is a specific email address, this field shall refer only to the category "email" and not the actual email address.

6.3.5.3 pii_attribute_id

This refers to an unambiguous identifier to the attribute which is related to the pii_type.

The presence of pii_attribute_id is optional.

Recommended encoding format: string.

See ISO/IEC 29184.

Requirements and guidance: The attribute ID shall be directly tied to the pii_type. There shall be a one-to-one relation. The representation of the attribute ID is an implementation decision but can be schema ID or another form of identification.

6.3.5.4 pii_optional

This field is used to indicate whether it was mandatory or optional for the PII principal to release the PII type for specified purposes. A value of “true” indicates the PII_type has been released by the PII principal, even though the PII principal has been informed that it was not mandatory to release that PII type. Without the presence of the pii_optional field, the PII category is considered mandatory for the specified purposes.

The presence of pii_optional is optional.

Recommended encoding format: True/False.

See ISO/IEC 29184:2020, 5.4.6.

Requirements and guidance: none.

6.3.5.5 sensitive_pii_category

The PII controller may explicitly denote the sensitivity of PII with respect to its potential for risks and impacts to the PII, and whose processing requires additional considerations, such as when sharing with other parties.

The presence of sensitive_pii_category is optional.

Recommended encoding format: True/False.

See ISO/IEC 29184.

Requirements and guidance: none.

6.3.5.6 special_pii_category

A PII controller may explicitly note if the PII category is considered special where it falls under the special category of highly impactful personal data based on requirements in the jurisdiction.

The presence of special_pii_category is optional.

Recommended encoding format: True/False.

See ISO/IEC 29184.

Requirements and guidance: For jurisdictions where sensitive PII is regulated or identified with specific terms, this field may be used to denote this information. For example, "special" referring to regulated categories of PII under GDPR, Article 9-1.[1] Another example is the "retained personal data" and "privilege information" under the Act on the Protection of Personal Information of Japan[9] and the Data Privacy Act of the Philippines.[10] These terms are specific under their jurisdictions and can have a different treatment or requirement from PII and sensitive PII.

6.3.6 Party identification section contents

6.3.6.1 General

Table 4 describes the structure and contents of the party identification section.

Table 4 — Party identification section contents

Data element identifier	Description	Presence
party_id (see 6.3.6.2)	An unambiguous identifier indicating the party within the record.	Required
party_address (see 6.3.6.3)	Contact information in the form of a postal address.	Required
party_email (see 6.3.6.4)	Contact information in the form of an email address.	Optional
party_url (see 6.3.6.5)	A url of a website or resource containing information about the party and/or its services, policies, and contact information.	Optional
party_phone (see 6.3.6.6)	Contact information in the form of a phone number.	Optional
party_name (see 6.3.6.7)	The name of the party through which it is identified as a legal entity.	Required
party_role (see 6.3.6.8)	Indicates the role of party in context of the record it is specified in.	Optional
party_contact (see 6.3.6.9)	Unbounded form of communication mediums.	Required
party_type (see 6.3.6.10)	The type or category with which the party is relevant for the specific processing.	Required

6.3.6.2 party_id

This refers to an unambiguous identifier indicating the party within the record.

The presence of party_id is required.

Recommended encoding format: string.

See ISO/IEC 29184:2020, 5.3.4.

Requirements and guidance: The party_id is used in other sections of the record or receipt structure to refer to the party identification information.

6.3.6.3 party_address

This refers to the contact information in the form of a postal address.

The presence of party_address is required.

Recommended encoding format: ISO 19160-4.

See ISO/IEC 29184:2020, 5.3.4.

Requirements and guidance: none.

6.3.6.4 party_email

Description: Contact information in the form of an email address.

The presence of party_email is optional.

Recommended encoding format: RFC 5322 (Internet Message Format).[16]

See ISO/IEC 29184:2020, 5.3.4.

Requirements and guidance: none.

6.3.6.5 party_url

This refers to a url of a website or resource containing information about the party and/or its services, policies, and contact information.

The presence of party_url is optional.

Recommended encoding format: URL.

See ISO/IEC 29184:2020, 5.3.4.

Requirements and guidance: none.

6.3.6.6 party_phone

This refers to a contact information in the form of a phone number.

The presence of party_phone is optional.

Recommended encoding format: ITU-T E.164:2010, Chapter 6.[17]

See ISO/IEC 29184:2020, 5.3.4.

Requirements and guidance: none.

6.3.6.7 party_name

This indicates the name of party in context of the record it is specified in.

The presence of party_name is required.

Recommended encoding format: string.

See ISO/IEC 29184.

Requirements and guidance: Name should reflect the legal name of the party.

6.3.6.8 party_role

This indicates the role of the party in context of the record it is specified in.

The presence of party_role is optional.

Recommended encoding format: string.

See ISO/IEC 29184.

Requirements and guidance: The specific terms used to indicate roles may be based on the applicable jurisdictions. Examples of roles are PII controller, PII Processor and third party.

6.3.6.9 party_contact

This refers to an unbounded form of communication medium.

The presence of party_contact is required.

Recommended encoding format: string.

See ISO/IEC 29184.

Requirements and guidance: A party may offer communication through various mediums, such as a social media, or even messaging services. For example, a social media user can provide a contact point on their own network, such as a dedicated handle for contact or complaints.

6.3.6.10 party_type

This refers to the type or category with which the party is relevant for the specific processing. For example, as recipients in data sharing.

The presence of party_type is required.

Recommended encoding format: string.

See ISO/IEC 29184.

Requirements and guidance: The expression of party category can assist in informing the PII principal of the relevance for that party's involvement (e.g. as recipient) in addition to its legally defined role (e.g. as a data processor or third party or authority).

6.3.7 Event section contents

6.3.7.1 General

Table 5 summarizes the structure and contents of the consent section.

Table 5 — Event section contents

Data element identifier	Description	Presence
event_time (see 6.3.7.2)	Date and time that the associated event took place, for example, when consent was obtained expressed using the date and time format specified in the ISO 8601 series using the UTC time zone.	Required
validity_duration (see 6.3.7.3)	The duration for which the consent is considered valid for justification of processing based on it, and after which it is no longer considered valid. The PII controller should "refresh", "confirm" or "re-affirm" consent periodically, where the period is considered the duration of that consent.	Required
entity_id (see 6.3.7.4)	The identifier or reference to the entity associated with performing the event.	Required
event_type (see 6.3.7.5)	The PII controller shall indicate the event type associated with the event state change, for example, when consent is used to justify the validity of expressing consent.	Required
event_state (see 6.3.7.6)	The state of an event specifies its existence and applicability within a life cycle. For consent, state refers to the events related to the request (e.g. notice), provision of or obtaining consent, or termination due to withdrawal.	Required

6.3.7.2 event_time

This refers to the date and time that the associated event took place, for example when consent was obtained, which is expressed using the date and time format specified in the ISO 8601 series using the UTC time zone.

The presence of event_time is required.

Recommended encoding format: date and time format according to the ISO 8601 series.

See ISO/IEC 29184.

Requirements and guidance: The time the consent was obtained is considered the time the user indicated their consent. In case there are substantial processing times, for instance due to missing network connections, the time that the consent was received by the pii controller can be different.

6.3.7.3 validity_duration

This refers to the duration for which the consent is considered valid for justification of processing based on it, and after which it is no longer considered valid. The PII controller should 'refresh', 'confirm' or 're-affirm' consent periodically, where the period is considered the duration of that consent. Duration shall be present where the event is regarding expression of consent.

The presence of validity_duration is conditionally required.

Recommended encoding format: duration format specified in the ISO 8601 series [PYMWDTHMS].

See ISO/IEC 29184:2020, 5.4.7 and 5.4.8.

Requirements and guidance: The PII controller may utilize this field to denote durations associated with other events such as notices, consent given and re-affirm. See Annex C for an example.

The duration of consent is not necessarily the same as the duration of processing. It is possible that the duration of consent is longer than the duration of processing.

6.3.7.4 entity_id

This refers to the identifier or reference to the entity associated with performing the event.

The presence of entity_id is required.

Recommended encoding format: string.

See ISO/IEC 29184.

Requirements and guidance: The entity_id captures whose action resulted in the state of the event. For example, when consent is requested, the agent is the PII controller, when given it is PII principal, when withdrawn it is PII principal, when terminated it is PII controller.

6.3.7.5 event_type

The PII controller shall indicate the event type type associated with the event state change, for example when consent is used to justify the validity of expressing consent.

The presence of event_type is required.

Recommended encoding format: string.

See ISO/IEC 29184

Requirements and guidance: The definition of the consent type, including specific terms and their interpretation, can vary depending on the jurisdiction, regulation (e.g. GDPR[1]), International

Standard (e.g. ISO 29184), or codes of conducts for specific domains. The organization shall choose the appropriate consent type based on these criteria for use within the record and shall indicate their basis for interpretation where it is not clearly evident. The following consent types are given as examples.

— explicit (e.g. indicates consent through explicit action such as clicking on “I agree to…”)

— implicit (e.g. consent is assumed, such as through creation of an account)

— regular (e.g. indicates consent meeting criteria for validity, such as freely given, without additional requirements such as being expressed in a specific manner).

NOTE The field name event_type was intentionally chosen to allow future compatibility with a different lawful basis other than consent.

6.3.7.6 event_state

The state of an event specifies its existence and applicability within a life cycle. For consent, state refers to the events related to the request (e.g. notice), provision of or obtaining consent, or termination due to withdrawal.

The presence of event_state is required.

Recommended encoding format: string.

See ISO/IEC 29184.

Requirements and guidance: A state or a change to a state can necessitate the creation and maintenance of records describing the state and state change. Such changes can result in additional obligations, for example halting the processing of personal data based on consent when its state changes to "terminated". The state of a consent determines its suitability for justification of processing as a lawful basis. For example, the state "given" is a valid use of consent as a lawful basis whereas the states "withdrawal" or "requested" are not. For an example of how the state of the consent can change, refer to Annex B.

6.4 Receipt information structure

6.4.1 General

The objective is to define the receipt information structure in a manner that enables accurate recordkeeping about notice and consent activities and exchange of receipts between PII controller and PII principal.

6.4.2 Structure of the receipt — control

The receipt shall be organized into four major sections: the receipt metadata section, the PII processing section, the party identification section, and the consent section.

6.4.3 Consent management — control

The organization shall ensure the PII principal is aware of and has the necessary information regarding how they can change, modify, or withdraw their consent by using the receipt. ISO/IEC 29184:2020, 5.4 and 5.5 provides controls when consent is the legal basis of processing and if there are changes in the conditions.

6.4.4 PII principal participation — control

Where the consent receipt is intended to be used as a record of information for inquiries, complaints or exercising of rights, the organization shall include sufficient information in the receipt for how or where the PII principal may do so.

6.4.5 Receipt metadata section contents

6.4.5.1 General

Table 6 summarizes the structure and contents of the receipt metadata section.

Table 6 — Receipt metadata section contents

Data element identifier	Description	Presence
schema_version (see 6.4.5.2)	A unique identifier for the implementation documentation describing the interpretation of the receipt structure and the contents in conformance with this document.	Required
receipt_id (see 6.4.5.3)	A unique identifier for a record.	Required

6.4.5.2 schema_version

This refers to a unique identifier for the implementation documentation describing the interpretation of the receipt structure and the contents in conformity with this document.

The presence of schema_version is required.

Recommended encoding format: string.

See ISO/IEC 29184.

Requirements and guidance: none.

6.4.5.3 receipt_id

A unique identifier for a record.

Presence: Required.

Recommended encoding format: UUID-4.[9]

See ISO/IEC 29184.

Requirements and guidance: The consent receipt is used to establish shared information between stakeholders for identifying and referring to consent records.

6.4.6 Receipt content — control

The receipt may contain equivalent information from the consent record. All fields in a consent record that are expressed as required are also required in a consent receipt.

Where the information requirements in a receipt are different from that of the consent record, the implementation documentation associated with schema_version shall specify details of the receipt structure.

Annex A
(informative)

Examples of consent records and receipts

A.1 Consent receipt example using JSON

This clause shows an example of how this document can be used to encode and provide consent records using JSON as the serialization format. It uses a hypothetical schema called "27560-CIB", as per 6.3.2.2 and 6.3.3.1 to define the structure, requirements, and interpretation of fields and their values.


```
{
    "record": {
        "schema_version": "27560-CIB",
        "record_id": "63ded36f-4acd-4f3c-991e-6cb636698523",
        "pii_principal_id": "96121fde-199f-4848-8942-4436e27051a3"
    },
    "pii_processing": {
        "privacy_notice": "https://example.com/notice/WD5",
        "language": "en",
        "purposes": [ {
            "purpose": "Send Newsletters with Seasonal Offers",
            "purpose_type": "Marketing",
            "lawful_basis": "consent",
            "pii_information": [
                {
                    "pii_type": "email",
                    "pii_optional": true,
                    "sensitive_pii_category": false,
                    "special_pii_category": false,
                }
                {
                    "pii_type": "passport",
                    "pii_optional": false,
                    "sensitive_pii_category": true,
                    "special_pii_category": true,
                }
            ],
            "pii_controllers": [ "C01", "C02" ],
            "collection_method": [
                "directly provided by individual",
                "inferred from service use"
            ],
            "processing_method": [ "collect", "store", "profiling" ],
            "storage_locations": [ "IE" ],
            "retention_period": 63115200,
            "processing_locations": [ "IE" ],
            "geographic_restrictions": [ "EU" ],
            "services": [ "News Website XYZ Subscription" ],
            "jurisdiction": "EU",
            "recipient_third_parties": [ "T01", "T02" ],
            "withdrawal_method": "https://example.com/notice",
            "privacy_rights": {
                "Right to Object": "https://example.com/object-to-direct-marketing",
                "Data Portability": "https://example.com/data-portability"
            },
            "codes_of_conduct": "https://example.com/CoC-news-media",
            "impact_assessment": "https://example.com/dpia",
            "authority_party": "DPC-IE",
        } ]
    },
    "party_identification": [
        {
```

```
            "party_id": "C01",
            "party_address": "Dublin, Ireland",
            "party_email": "acme@example.com",
            "party_url": "https://example.com/AcmeInc",
            "party_name": "Acme Inc.",
            "party_role": "PII Controller",
            "party_contact": {
                "SocialMedia": "@acme"
            },
            "party_type": "Service Provider"
        },
        {
            "party_id": "C02",
            "party_address": "Frankfurt, Germany",
            "party_url": "https://example.com/BetaInc",
            "party_name": "Beta Inc.",
            "party_role": "PII Controller",
            "party_type": "Service Provider"
        },
        {
            "party_id": "T01",
            "party_address": "Paris, France",
            "party_url": "https://example.com/Delta",
            "party_name": "Delta",
            "party_role": "PII Processor",
            "party_type": "Recipient"
        },
        {
            "party_id": "T02",
            "party_address": "Dublin, Ireland",
            "party_url": "https://example.com/Epsilon",
            "party_name": "Epsilon Co.",
            "party_role": "Third Party",
            "party_type": "Recipient"
        },
        {
            "party_id": "DPC-IE",
            "party_address": "Dublin, Ireland",
            "party_url": "https://www.dataprotection.ie/",
            "party_name": "Data Protection Commission",
            "party_role": "Data Protection Authority",
            "party_type": "Lead Authority"
        }
    ],
    "event": [
        {
            "event_time": "2021-05-28T12:24:00",
            "validity_duration": 63115200,
            "entity_id": "96121fde-199f-4848-8942-4436e270513a",
            "event_type": "explicit",
            "event_state": "consent given",
        },
        {
            "event_time": "2022-02-21T20:44:00",
            "validity_duration": 0,
            "entity_id": "96121fde-199f-4848-8942-4436e270513a",
            "event_type": "explicit",
            "event_state": "consent withdrawn",
        }
    ]
}
```


A.2 Consent record example using JSON-LD

This clause shows an example of how this document can be used to encode and provide information from consent records through a consent receipt, by using the JSON-LD serialisation format. The example uses the external vocabulary, in this case the W3C Data Privacy Vocabulary (DPV)[12] for defining domain- and jurisdiction-specific terms. It uses a hypothetical schema called “27560-CIB”, as

per 6.4.5.1, to define the structure, requirements, and interpretation of fields and their values. In this case, the schema creates a receipt without any identifiers or identifying fields from the record.

```
{
  "@context": {
    "@vocab": "https://w3id.org/dpv#",
    "dpv": "https://w3id.org/dpv#",
    "dpv-gdpr": "https://w3id.org/dpv/dpv-gdpr#",
    "dct": "https://purl.org/dc/terms/",
    "foaf": "http://xmlns.com/foaf/0.1/",
    "ex": "https://example.com/"
  },
  "@id": "ex:a1368f5d-0d26-453c-bd55-b7abacc286fa",
  "@type": "dpv:ConsentReceipt",
  "dct:conformsTo": "27560-CIB",
  "dct:subject": {
    "@id": "ex:63ded36f-4acd-4f3c-991e-6cb636698523",
    "@type": "dpv:ConsentRecord",
    "hasPersonalDataHandling": {
      "hasNotice": { "@id": "https://example.com/notice/29184" },
      "hasAuthority": { "@id": "https://www.dataprotection.ie/" },
      "hasPurpose": [{
        "dct:title": "Send Newsletters with Seasonal Offers",
        "@type": "dpv:Marketing",
        "hasLegalBasis": { "@id": "dpv:Consent" },
        "hasPersonalData": [
          { "@type": "dpv:pd_Email",
            "hasContext": "dpv:Optional" },
          { "@type": "dpv:pd_Passport",
            "@type": "dpv:SpecialCategoryPersonalData",
            "hasContext": "dpv:Required" }
        ],
        "hasDataController": [ { "@id": "ex:C01" }, { "@id": "ex:C02" }],
        "hasStorageCondition": {
          "hasLocation": "IE",
          "hasDuration": 63115200
        },
        "hasJurisdiction": "EU",
        "dct:subject": [ "News Website XYZ Subscription" ],
        "hasRecipient": [ { "@id": "ex:T01" }, { "@id": "ex:T02" } ],
        "hasRight": [
          {
            "@type": [ "dpv-gdpr:A7-3", "dpv-gdpr:A20" ],
            "isExercisedAt": "ex:notice"
          }
        ],
        "hasOrganisationalMeasure": [
          {
            "@id": "ex:CoC-news-media",
            "@type": "dpv:CodeOfConduct"
          }, {
            "@id": "ex:dpia",
            "@type": "dpv:DPIA"
          }
        ]
      }]
    },
    "hasEntity": [
      {
        "@id": "ex:C01",
        "foaf:mbox": "acme@example.com",
        "foaf:page": "https://example.com/AcmeInc",
        "foaf:name": "Acme Inc.",
        "@type": [ "dpv:DataController", "dpv:ServiceProvider" ],
        "foaf:OnlineAccount": {
          "foaf:name": "SocialMedia",
          "foaf:accountName": "@acme"
        }
      },
      {
        "@id": "ex:C02",
```

```
        "foaf:page": "https://example.com/BetaInc",
        "foaf:name": "Beta Inc.",
        "@type": [ "dpv:DataController", "dpv:ServiceProvider" ]
      },
      {
        "@id": "ex:T01",
        "foaf:page": "https://example.com/Delta",
        "foaf:name": "Delta",
        "@type": [ "dpv:DataProcessor", "dpv:Recipient" ]
      },
      {
        "@id": "ex:T02",
        "foaf:page": "https://example.com/Epsilon",
        "foaf:name": "Epsilon Co.",
        "@type": [ "dpv:ThirdParty", "dpv:Recipient" ]
      },
      {
        "@id": "https://www.dataprotection.ie/",
        "foaf:page": "https://www.dataprotection.ie/",
        "foaf:name": "Data Protection Commission",
        "@type": [ "dpv:DataProtectionAuthority", "dpv-gdpr:LeadSA" ]
      }
    ],
    "dct:hasPart": [
      {
        "dct:date": "2021-05-28T12:24:00",
        "hasDuration": 63115200,
        "@type": "dpv:ExplicitlyExpressedConsent",
        "hasConsentStatus": "dpv:ConsentGiven"
      },
      {
        "dct:date": "2022-02-21T20:44:00",
        "hasDuration": 0,
        "@type": "dpv:ExplicitlyExpressedConsent",
        "hasConsentStatus": "dpv:ConsentWithdrawn"
      }
    ]
  }
}
```

Annex B
(informative)

Example of consent record life cycle

B.1 General

This annex provides a reference consent life cycle to help implementers with the development of the consent record and receipt.

B.2 Consent record schema governance

B.2.1 General

Prior to requesting consent or generating any consent records, the PII controller identifies the information to be maintained in the consent record based on requirements of organizational processes and practices based on domain or industry sectors it operates within.

NOTE Legal requirements can also apply.

This information is then used to define the "schema" of the consent record, such as through pre-populating fields e.g. PII controller's information, or adding additional fields as necessary. The schema is given an identifier, which is denoted within the consent record using the schema_version field.

Based on the specifics of each consent record, the organization can opt to distinguish its practices through separate schema versions, such as for each "service", or utilize the same schema for all its consent requirements with variances in the field values, such as purpose descriptions. The organization can also opt to maintain separate schemas based on factors such as temporal periods, jurisdictions, or business processes.

When utilizing a schema for the creation of a consent for a specific PII principal, the PII controller is required to add the relevant contextual information to the record, such as an identifier for the PII principal whose consent the record relates to, or the event_times for specified events. The PII controller then stores the consent record within their system.

In the case of a prior record existing for the same consent i.e. the same processing conditions involving the same PII principal, the PII controller can choose for the record to be updated (overwriting the prior record) or extended (to maintain all prior interactions) instead of creating a separate record. In such situations, the PII controller should be careful with respect to requirements regarding documentation of consent which are required in certain jurisdictions. Such requirements can require not overwriting a prior consent record or ensuring the information is maintained elsewhere.

The following subclauses B.2.2 to B.2.7 describe the typical consent record life cycle depicted in Figure B.1.

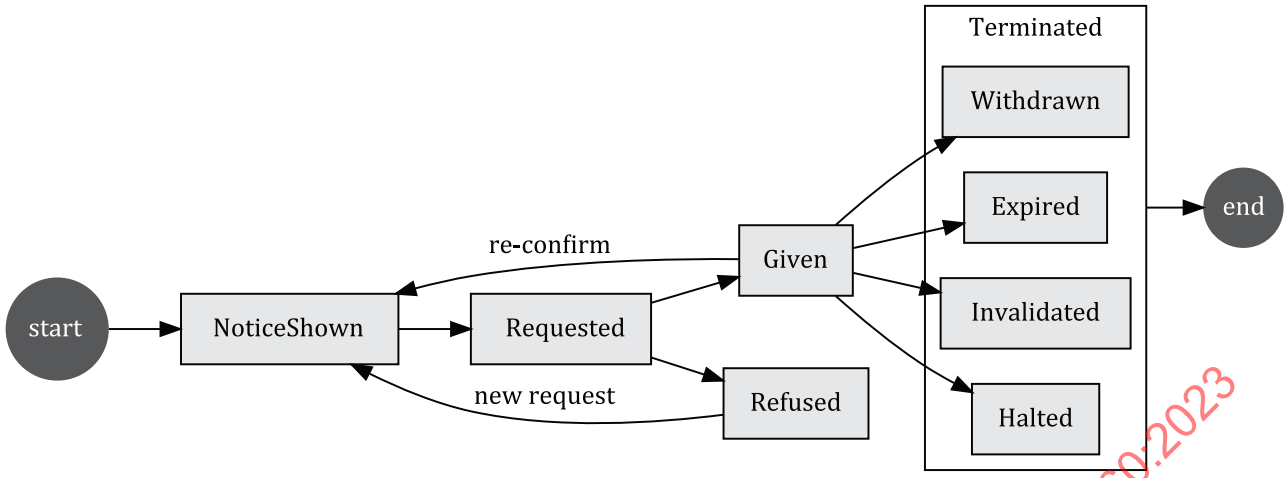


Figure B.1 — Overview of a typical consent record life cycle

B.2.2 Consent notice and request

The first step in the consent life cycle is the creation and presentation of a notice, as outlined in ISO/IEC 29184, to inform the PII principal information of the specifics of the PII processing, identities of relevant parties, and other pertinent details. A notice may also be accompanied with a request for consent.

Based on requirements, such as those arising from jurisdictional obligations, the PII controller may choose to maintain a record of the notice and/or request by utilizing the Event section fields. For example:

— event_time: time at which notice was shown and/or consent was requested;

— duration: optional field indicating temporal period for which the notice and/or request is valid;

— entity_id: identifier of the entity that provided the notice and/or request;

— type: the type of consent for which notice is provided and/or consent is requested;

— state: an indication of the state of consent at this point e.g. “notice” or “request”.

B.2.3 Consent given

Based on the notice and request, the PII principal may choose to accept the specified processing and give their consent. In this case, the PII controller is required to create a consent record for documenting this event.

A typical Event field reflecting a given consent state would contain:

— event_time: time at which consent was expressed by the PII principal;

— duration: temporal period for which the given consent is valid (this field is mandatory i.e. conditionally required) for this event;

— entity_id: identifier of the entity that provided consent e.g. PII principal or their representative or delegate (e.g. parent);

— type: the type of consent expressed by the PII principal e.g. “explicit” or “regular”;

— state: an indication of the state of consent at this point e.g. “given” or “obtained”.

B.2.4 Consent not given or refused

Based on the notice and request, the PII principal may choose to not indicate acceptance or refuse to give their consent. In this case, the PII controller may choose to create a consent record for documenting this event.

A typical Event field reflecting a not given of refused consent state would contain:

— event_time: time at which consent was refused by the PII principal, or the time at which the PII controller established the consent has not been given;

— entity_id: identifier of the entity that refused consent e.g. PII principal, or the PII controller establishing consent was not given;

— type: the type of consent requested e.g. “explicit” or “regular”;

— state: an indication of the state at this point e.g. “not given” or “refused”.

B.2.5 Consent withdrawn or revoked

The PII principal may choose to withdraw their previously given consent. In this case, the PII controller shall document this event in a consent record.

A typical Event field reflecting withdrawal or revocation of consent would contain:

— event_time: time at which consent was withdrawn by the PII principal;

— entity_id: identifier of the entity that withdrew or revoked consent e.g. PII principal or their representative or delegate (e.g. parent);

— type: the type of consent that was expressed by the PII principal e.g. “explicit” or “regular”, and that has now been withdrawn;

— state: an indication of the state at this point e.g. “withdrawn” or “revoked”.

B.2.6 Consent re-confirmed or reaffirmed

The PII controller may choose to re-confirm or reaffirm an existing given consent, based on contextual changes such as lapse of temporal period, changes to the underlying processing activities, or jurisdictional requirements. In this case, the PII controller shall create a consent record for documenting this event. A "reaffirmed" consent shall still fulfil the requirements for "given" consent, and therefore can be considered as such. That is, it can be indicated as consent being given (again) for the same PII processing.

Under these circumstances, the PII controller may choose to terminate the earlier consent and utilize this as a new consent instance or update the earlier consent record to maintain continuation. The PII controller may also choose to maintain a record of the notice and/or request for re-confirmation or reaffirmation in a manner similar to the example indicated earlier in this annex.

A typical Event field reflecting re-confirmed or reaffirmed consent would contain:

— event_time: time at which consent was reaffirmed given by the PII principal;

— duration: temporal period for which the reaffirmed consent is valid (this field is mandatory i.e. conditionally required for this event).

— entity_id: identifier of the entity that provided consent e.g. PII principal or their representative or delegate (e.g. parent).

— type: the type of consent expressed by the PII principal e.g. “explicit” or “regular”.

— state: an indication of the state at this point e.g. “re-confirmed” or “reaffirmed”.

B.2.7 Consent terminated

Termination of consent indicates its inability to be used as a justification for further PII processing. Termination can be a consequence of several distinct events, such as withdrawal by the PII principal, expiry of the duration for which a consent was valid, termination by the PII controller, or invalidation by an authority. In case of termination, the PII controller shall create a consent record for documenting this event. In case of withdrawal, the PII controller may opt to create a separate record denoting the withdrawal or revocation of consent to distinguish it from other causes of termination. Legal requirements can also apply in such cases.

A typical Event field reflecting a termination of consent state would contain:

— event_time: time at which the consent was terminated. In this, it is important to note that terminated consent cannot be used as a justification and does not have a specific temporal period after which it can be assumed to be given. The PII controller is required to request consent again.

— entity_id: identifier of the entity that terminated consent e.g. PII principal in withdrawing the consent, or the PII controller as stopping use of this consent.

— type: the type of consent that was expressed by the PII principal e.g. “explicit” or “regular”, and that has now been terminated.

Annex C
(informative)

Performance and efficiency considerations

C.1 General

There are technical and implementation challenges for large consent record handling systems, managing millions, tens of millions or billions of consent records. Optimizations are required when working at such scales. This annex describes issues that are worth considering when implementing large-scale consent management systems. This annex also helps to differentiate between the fundamental concepts embodied in consent records in the abstract (conceptual issues), articulation of those concepts as presented in the main body of this document (abstract representation) and specific issues of practical concern that arise when implementing large scale consent record handling systems.

C.2 System properties

C.2.1 General

In designing a large-scale consent record handling system, a number of practical factors arise, depending on the specific use cases that are to be supported by that system. These practical factors are outlined in C.2.2 to C.2.12.

Although this document is primarily focused on the structure and content of individual consent records, some of the implementation challenges arise because of the implicit and explicit relationships that exist involving multiple such records. For example, over time a user may grant and withdraw consent repeatedly in the context of a specific form of processing by a single application. Consent can have been granted by that user at times t_0, t_2 and t_4, and withdrawn at times t_1 and t_3, with $t_0 < t_1 < t_2 < t_3 < t_4$. Those five consent-related moments each represent an event at a distinct point in time and can imply the existence of (at least) three consent records with implicit relationships to one another. Similarly, if a user asks an organisation to provide them with information about the consents that the organization believes the user has granted, the response implicitly takes the form of a set of consent receipts, but can also include a summary listing the current set of extant consents omitting those that have been withdrawn, for added clarity. If the consent management system is required to scan all of the consent records in order to determine whether consent remains applicable in a specific context, or to find all the consent records associated with a particular user, the system will not scale.

Organizing the records to enable rapid determination of the current situation for a specific user in a specific consent-related context can be achieved in many ways, and this is a technical choice made by the system developer. In this annex, when referring to the need for relationships between consent records to be considered by the developer, the term “linking” is used. This is not intended to imply that records contain direct links to one another, and no such cross-references are defined in this document. Instead, this is intended to be read as indicating that any necessary meta-structure is in place, or established, to allow such relationships to be rapidly and efficiently inferred or discovered. These implicit links can be achieved, for example, by inserting references to the consent records in an indexing system keyed by the user identity, or by keeping duplicate records in per-user caches that summarise the current consent status for that user in the context of a specific consent point, or overall, for the application as a whole. In large scale systems, the chosen approach can lead to challenges related to distributed consensus or consistency, or involve processing times maintaining indexes or data structures that grow as the system becomes responsible for handling more records.

C.2.2 High input rates

For systems supporting large numbers of users, especially in regulatory domains that require explicit notice and consent on every engagement, consent records are generated in a near continuous stream, potentially with hundreds of millions of records created per day. One million records per day is approximately 11 records per second. Each new record potentially shall be linked to existing records for the same user, system, purpose or application consent point. This introduces the possibility of race conditions when manipulating the underlying data structures.

C.2.3 Fine-grained consents

If consent records are generated based on user engagement during their use of an application, e.g. when they enable particular controls in a user interface, the number of records involved is even larger and the system capacity and throughput shall be planned accordingly. Cross-linking of fine-grained consents is then used in order to create meaningful consent receipts and the need to support this is taken into account when designing the concrete representation.

C.2.4 Real-time access and consent propagation

If the consent records are used by applications, in real-time, to determine whether the user has a valid active consent in place for the functionality being invoked, the read capacity and timeliness of response require careful consideration. Such approaches assume the consent record system reliably responds in millisecond timescales, under heavy load. Reliability is essential as such "in-line" systems can be critical single points of failure. This raises new problems including:

— Most organizations are unlikely to wish to make large investments in the engineering of such a high-reliability high-throughput system.

— If the real-time or in-line consent checking is handled separately from the consent record handling system, new problems arise: for example, if consent data are held in multiple places (e.g. caches), it can be temporarily inconsistent.

C.2.5 Designing for consistent consent experiences

Taken together, the consent system implementation challenges require very careful consideration. As part of that effort, application developers and backend systems architects can work with user experience designers and researchers to design user interfaces and application experiences that take into account special case handling of critical consents when they are revoked or withheld.

C.2.6 Acceptable propagation-time delay limits

For any consent record handling system, whether it incorporates in-line consent-checking functionality or is purely a backend system of record (i.e. with the primary outputs being consent receipts generated when requested by users), propagation delays matter. Consider, for example:

— The maximum propagation time, between users giving or revoking consent and the new consent status being used by all applications, shall be addressed on a case-by-case basis, to satisfy user expectations.

— If there are mandated propagation delay limits, or implicit societal expectations, it is advisable to create and maintain documentation explaining how related legal or regulatory requirements are satisfied, as part of the consent handling system's design material.

C.2.7 Flexibility and evolvability

For organizations with many applications, consideration shall be given to the likely rate of change in consent record structures. For example, adding new functionality can require re-acquisition of consent, or acquisition of a supplementary consent. Such changes can lead to new consent records, implicitly or explicitly linked to other such records. Alternatively, the concrete representation of the consent record

or the linkages between existing fine-grained consents can require modification in line with the newly acquired consent.

C.2.8 Real-world events

Where large-scale consent systems are being used, awareness of key real-world events is also advisable. For example, if a significant legislative change, requiring new consents, coincides with a major shopping event, which triggers substantial and widespread initial use of new devices, the increase in load on consent record handling systems can be substantial. Handling such peaks in demand relies upon temporary increases in system capacity, potentially at the same time as data model changes are being rolled out. Advance planning for such events and combinations of events is an important consideration for engineering teams and company management, if adverse consequences for system availability are to be avoided.

C.2.9 User identification

Consent receipts contain information associated with the person giving the consent, and also personal, depending on the consent being given. Thus, care should be taken with respect to the user identification mechanism, during both consent record generation (to avoid impersonation) and consent receipt issuance (to avoid privacy breaches). Developing a separate identity system for consent management is unlikely to be helpful to users. Instead, using the same user identification technology as the application is more natural. If many applications are sharing a consent record handling system, and also share a user identification mechanism, this is generally not a problem. However, a general-purpose consent handling system that is intended for use in the context of many organizations and applications, with disparate user identification mechanisms, can face additional challenges.

C.2.10 Privacy risks of linked consent records

Consent records and consent receipts are particularly privacy sensitive as they often combine multiple identifiers that are normally, wherever possible, separated, e.g. identifiers for users and timestamps associated with specific functionality being used. Device identifiers are often held in consent records, as they describe the scope where the consent is effective. Having access to two correlated consent records, one for a logged-in user and another one for an incognito person implicated in closely correlated actions, enables linking of their sessions or potential re-identification of the incognito user.

C.2.11 User deletion requests

Since the consent records are themselves personal data, technical capabilities will be required in support of user rights such as access (transparency), correction (of errors) and erasure (deletion requests by users). This can be particularly complex where one or more inter-linked consent records involving multiple people are concerned, for example if several family members use a common device. Erasure of some, but not all, of such linked records can require special care and handling. Automation of such cases in large-scale high-throughput systems, where it is not feasible to hold a global lock on the data structures, can be even more challenging.

C.2.12 Near-static information

Most consent records are not expected to change over time. Nonetheless, systems storing consent records shall be able to modify consent records in rare cases, for instance due to companies changing their physical address or contact details such as telephone numbers. When they do so, it has fundamental consequences for existing records that contain original contact information. Approaches to identifying and isolating such materials, so they are held as a single copy, with an explicit plan for updating those details, are presented in C.3.

C.3 Common near-static data fields

In the case of an organization's contact details, there are many possible representations with significant implications for the concrete implementation. The contact details can be described, abstractly, as

a single complex datum, e.g. as a referenceable record with several fields. The implementation in a database system is then a record matching a specific data model.

If the contact details record is explicitly referenced from all consent records, this incurs a storage cost proportionate to the number of records in the system. If this is an eight-byte (64 bit) reference in a system with a billion records, those links alone occupy 8 GB of space. Alternatively, if the location of that record is implicitly embedded in the consent record system software, that cost can be avoided.

If, instead, the address was separately copied for each record, the overall space requirement would be vastly larger. This is unlikely to be an effective approach in anything other than very small systems, containing perhaps hundreds or thousands of records. There is a risk that initial prototypes are built in this way and subsequently suffer from scaling problems. Such a risk can be avoided by considering this issue from the beginning of the development of a consent record handling system.

If the contact details subsequently change and the concrete record is edited in situ, no apparent cost is incurred for the wider system, however important information is lost. For example, a user who has evidence of communicating with the organization by registered letter, may wish to be able to demonstrate the official address of the organization at the time they sent their letter. Rather than overwriting the contact information, using a new contact detail record would allow the old information to be retained. However, updating every consent record to point at a new contact details record would be inefficient and unworkable in large systems.

If consent records are directly referencing the contact details valid at their time of creation, a workable system is achievable if the contact records chain together and contain validity event times. If instead the contact detail record is embedded in the application software, this is workable if a chain of records stretches into the historical past from the current contact information, relying on the consent record event times for disambiguation. These concerns are not unique to consent record handling systems, arising in all complex applications that support changes over time.

Similar practical concerns arise for other near-static material in the abstract consent record. For example, privacy notices can change very infrequently, but consent handling systems shall be designed with consideration of the possibility of change in notices.

C.4 Consent purpose handling

If an abstract consent record is associated with a single consent event but multiple purposes, attention is required if the consent for one of those purposes is subsequently withdrawn. If the conceptual representation distinguishes between purposes, representing them separately, then invalidation of the consent for a specific purpose is likely to be simpler. This suggests fine-grained consents are easier to handle if purpose descriptions are linked to, but separate from, the body of the main consent record. Such an approach also allows a single purpose description to be common to all consent records related to that purpose, avoiding duplication of material. The alternative, in which a separate consent record is created for each purpose, is workable, provided they are mutually linked to allow a consent receipt to be generated for the event in which those consents were given. By way of contrast, requiring a separate user action for each purpose risks creating consent blindness. Guidance on online privacy notices and consent is available in ISO/IEC 29184.

C.5 Consent receipt generation

Outbound consent receipts are likely to be created far less often than inbound consent records. Nonetheless, creation and delivery in near real-time is helpful for users. Ensuring that receipts can be assembled and returned promptly, without manual intervention, is therefore advisable for large scale systems. This relies upon access to the same abstract data model as the consent record creation and update mechanisms, and use of the same user identification facilities.

Requirements and guidance: A new record shall supersede the previous record based on the event counter. The counter helps to avoid issues of race condition if several events take place in a short period of time.

There are multiple reasons that a record can be updated.

a) The record may track the order of events related to the interactions with a PII principal. There can be a notification event, confirmation event when consent is given and withdrawal event.

b) Conditions relating to the consent can require updating. Here are some examples:

   1) new data attributes collected for the same purpose;

   2) removed data attributes possibly due to data minimization concerns;

   3) change in storage_duration if the PII principal has such a control.

Annex D
(informative)

Consent record encoding structure

This document defines the encoding structure of a single consent record, but does not specify how a set of consent records should be stored or transmitted.

A consent record is conceptually composed of a set of elements where each element can either be a container that contains several other elements or an individual element with a specified semantics and specified data type.

A consent record may be encoded using one or more encoding techniques.

The encoding technique of each container, data type and semantics is not specified in this document.

For each individual element of a consent record, this document recommends its syntax (e.g. an ASCII character string, a UTF-8 character string, a UTC date, 8 bits unsigned integer) and its semantics (e.g. a date/ time of the event, a record identifier unique to the PII controller). It also defines the mandatory or optional presence of that element and the acceptable values of each data element, if necessary.

The goal of encoding techniques is to represent different data elements using some encoding rules. Some encoding techniques may use a fixed length encoding for some types of values, while a variable length encoding for other types of values may also be necessary.

While it is not usually a major problem to encode a single consent record using a verbose encoding technique (e.g. XML), using the same encoding technique when a large number of consent records are stored would lead to storage blow-up and excessive network bandwidth usage. This would not be economical and would lead to low performance.

A set of consent records may be associated with a schema. This offers the advantage of being able to factorize values and field semantics when they are present in several consent records. The prime example is the notice which may consist of several pages. Duplicating the same notice in each individual consent record would lead to waste of storage capacity and/or a loss of throughput.

For a set of consent records, a schema should be defined. Such a schema can refer to one or more dictionaries which contain values that have been factorized for that set of consent records. In this way, a given consent record may then point to any item present in one of the dictionaries.

Annex E
(informative)

Security of consent records and receipts

E.1 Overview

Since notice or consent receipts can contain PII, transmission of notice and consent receipts shall be done over secure communications e.g. HTTPS. The requirements for implementers of consent records and consent management solutions include signing, encryption, key management and other operations for their creation, transmission, use, and storage if the consent record is to be used for proof of notice and consent, withdrawal of consent or any other rights. For more information on these, refer to ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27701, with respect to information security techniques.

A simplified threat model for consent records, involving either the PII controller and the PII principal (the parties), relies on the following:

— compromise of confidentiality, if data-in-motion can be intercepted or storage of records is not adequately secured (such as in a breach);

— non-forgery or unauthorized modification, if a party produces records that are not authentic as per the original context that produced the records;

— repudiation, if a party denies at a later point in time not having received the data as is claimed (in whole or in part);

— auditability, considering records and receipts are key instruments in investigations such as from a regulator.

E.2 Confidentiality

Data used in populating consent records and receipts shall be transferred using secure protocols.

Consent records or receipts should not hold PII except for the PII principal identification material required by 6.3.3.4.

E.3 Forgery or unauthorized modification and repudiation

Consent records and receipts shall be protected against modification by calculating a hash-based message authentication code (HMAC) that protects an appropriate subset of fields.

The consent record shall have, as a minimum, all the information of the consent receipt given to the PII principal. The HMAC shall be part of the consent receipt.

The HMAC shall use a sufficiently strong and commonly used algorithm. The associated cryptographic secret key shall be unique to each PII principal. The secret shall not be shared with the PII principal.

It is presumed that the onus of proving authentic records is on the PII controller and not the PII principal. It is possible that this is not always be the case, but it is expected to be the most relevant case. The scenario is a PII principal challenging a PII controller (e.g. after a breach) about having validly consented in the past. The PII controller shall keep any cryptographic material (such as keys) and the PII controller shall produce the secret key and related linked information and demonstrate a calculation of a HMAC that shall match the one in the consent receipt in possession of the PII principal.

E.4 Auditability

On possession of a consent receipt, its authenticity as a consent receipt (the HMAC) and the identity of the PII controller should be publicly verifiable. PII controllers shall keep historical records of all linked information in the consent records or consent receipts, such as the content of the privacy notice at the time of consent.

Annex F
(informative)

Signals as controls communicating PII principal's preferences and decisions

A consent record is intended to represent the decision and events relevant to using the PII principal's consent for processing of PII. In a typical notice and consent process, the PII principal is presented with a request (as a notice), following which they make an informed decision regarding their consent. This decision is then represented within the consent record.

Where the PII principal makes use of automated signals or communication mechanisms to convey a preference or a decision alongside their consenting decisions, a PII controller that supports such signals may choose to record its application in the consent record to accurately represent all relevant information necessary to interpret the validity and applicability of that record towards PII processing.

Given that interpretation and applicability of signals can be contextually defined, including for specific jurisdictions, a PII controller or a relevant stakeholder group can decide to create a schema based on the document's consent record structure permitting indication of the signal. An example of this is given below.

EXAMPLE The Global Privacy Control (GPC)[13] is a unary signal indicating prohibition to "sell" or "share" data with third parties, as legally defined and enforceable under the California Consumer Privacy Act of 2018 (CCPA). [14] A PII principal expressing GPC requires a PII controller to not share or sell obtained PII with other third parties. To acknowledge this preference expressed through the GPC, the controller extends the schema with a 'signal' field as follows (indicated using JSON):

```
{
      "record": {
          "schema_version": "27560-TS-GPC",
          "record_id": "63ded36f-4acd-4f3c-991e-6cb636698523",
          "authorty": "California Privacy Protection Agency",
          "pii_principal": "Jane Doe"
      },
      "pii_processing": {
          "privacy_notice": "https://example.com/notice/wd4",
         "signal": "GPC"
         ...
      }
      ...
 }
```

In recording a signal's expression, this document makes no assumptions about the legality or enforceability of that signal with the rest of the consent record. For example, in the above EXAMPLE, if the expression of the GPC, which prohibits selling data to third parties, conflicted with the other fields

in the record that indicate permission to sell data to third parties, the resulting validity of that signal should be determined by the PII controller. For example, in jurisdictions where one of the conditions for valid consent is that it is unambiguous, it is possible that the conflict between the signal and the expressed consent decision does not fulfill these criteria.