ISO/IEC ~~TS~~ DTS 27560 ~~(DTS DoC Version 1~~:2023(E)

ISO/IEC JTC 1/SC 27/WG 5

Secretariat: DIN

Date: 2023-~~01-11~~03-15

Privacy technologies — Consent record information structure

~~Structure de l'information pour l'enregistrement des consentements~~

iTeh STANDARD PREVIEW
(standards.iteh.ai)

~~DTS stage~~

ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/sist/5913d3d0-a4d7-41a2-a88e-fb0f5a2fe268/iso-iec-dts-27560

~~**Warning for WDs and CDs**~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.~~

© ISO 2021 – All rights reserved

Style Definition ...
Formatted: Font: 11 pt
Formatted ...
Formatted: zzCover, Left
Formatted ...
Formatted: Font: Not Bold, English (United States)
Formatted: English (United States)
Formatted: zzCover, Left, Space After: 0 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: 11 pt, English (United States)
Formatted: zzCover, Line spacing: single, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/sist/5913d3d0-a4d7-41a2-a88e-fb0f5a2fe268/iso-iec-dts-27560

~~© ISO 2021~~

© ISO 2023

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

ISO ~~copyright office~~Copyright Office

CP 401 • ~~Ch. de Blandonnet 8~~
CH-1214 Vernier, Geneva

Phone: + 41 22 749 01 11

~~Email: copyright@iso.org~~
Email: copyright@iso.org

Website: ~~www.iso.org~~www.iso.org

Published in Switzerland

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/sist/5913d3d0-a4d7-41a2-a88c-[illegible]/iec-dts-27560

Formatted: Font: 11 pt, Font color: Blue

Formatted: Indent: Left: 0 cm, Right: 0 cm, Border: Left: (No border), Right: (No border)

Formatted: Font: 11 pt, Font color: Blue

Formatted: Font: 11 pt, Font color: Blue

Formatted: Font: 11 pt, Font color: Blue

Formatted: Font: 11 pt

Formatted: Font: 11 pt, Font color: Blue

Formatted: Indent: Left: 0 cm, First line: 0 cm, Right: 0 cm, Border: Left: (No border), Right: (No border)

Formatted: Font: 11 pt, Font color: Blue

Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)

Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)

Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)

Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)

Formatted: Indent: Left: 0 cm, First line: 0 cm, Right: 0 cm, Border: Bottom: (No border), Left: (No border), Right: (No border)

Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)

Formatted: Font: 11 pt, Font color: Blue, English (United Kingdom)

Contents

Formatted: Space Before: 48 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Foreword v
Introduction vi
1. Scope *(mandatory)* 1
2. Normative references *(mandatory)* 1
3. Terms and definitions *(mandatory)* 1
4. Symbols and abbreviated terms 2
5. Overview of consent records and consent receipts 2
5.1 General 2
5.2 Consent record 2
5.3 Consent receipt 2
6. Elements of a consent record and consent receipt 2
6.1 Overall objectives 2
6.2 Recordkeeping for online privacy notices and consent 3
6.2.1 General 3
6.2.2 PII controller recordkeeping 3
6.2.3 Recordkeeping for consent receipts 4
6.2.4 Relationship between records and receipts - control 5
6.3 Record information structure 5
6.3.1 General 5
6.3.2 Structure of the consent record 5
6.3.3 Record header section contents 6
6.3.4 PII processing section contents 8
6.3.5 PII information 15
6.3.6 Party identification section contents 17
6.3.7 Event section contents 20
6.4 Receipt information structure 22
6.4.1 General 22
6.4.2 Structure of the receipt - control 22
6.4.3 Consent management- control 22
6.4.4 PII principal participation - control 22
6.4.5 Receipt metadata section contents 22
6.4.6 Receipt content - control 23
Annex A (informative) Examples of consent records and receipts 24
A.1 Consent receipt example using JSON 24
A.2 Consent record example using JSON-LD 26
Annex B (informative) Example of consent record lifecycle 30
B.1. Consent record schema governance 30
B.1.1 Consent notice and request 30
B.1.2. Consent given 31
B.1.3. Consent not given or refused 31
B.1.4. Consent withdrawn or revoked 31
B.1.5. Consent re-confirmed or reaffirmed 31
B.1.6. Consent terminated 32

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/sist/...-41a2-a88e-fb0f5a2fe268/iso-

© ISO 2021 – All rights reserved

~~Annex C (informative) Performance and efficiency considerations ..... 33~~
~~C.1 General ..... 33~~
~~C.2 System properties ..... 33~~
~~C.2.1 High input rates ..... 33~~
~~C.2.2 Fine-grained consents ..... 33~~
~~C.2.3 Real-time access and consent propagation ..... 33~~
~~C.2.4 Designing for consistent consent experiences ..... 33~~
~~C.2.5 Acceptable propagation-time delay limits ..... 34~~
~~C.2.6 Flexibility and evolvability ..... 34~~
~~C.2.7 Real-world events ..... 34~~
~~C.2.8 User identification ..... 34~~
~~C.2.9 Consent records as "join hazards" ..... 34~~
~~C.2.10 User deletion requests ..... 34~~
~~C.2.11 Near-static information ..... 35~~
~~C.3 Common near-static data fields ..... 35~~
~~C.4 Consent purpose handling ..... 35~~
~~C.5 Consent receipt generation ..... 36~~
~~Annex D (informative) Storage and transmission of consent records ..... 37~~
~~Annex E (informative) Security of consent records and receipts ..... 38~~
~~E.1 Overview ..... 38~~
~~E.2 Confidentiality ..... 38~~
~~E.3 Forgery or unauthorized modification and repudiation ..... 38~~
~~E.4 Auditability ..... 38~~
~~Annex F (informative) Signals as controls communicating PII principal's preferences and decisions ..... 39~~
~~Annex G (informative) Guidance on the application of consent receipts in the context of a privacy information management systems ..... 40~~
~~G.1 General ..... 40~~
~~Annex H (informative) Mapping to ISO/IEC 29184: 2020 ..... 48~~
~~Bibliography ..... 50~~
Foreword v
Introduction vi
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Abbreviated terms 2
5 Overview of consent records and consent receipts 3
5.1 General 3
5.2 Consent record 3
5.3 Consent receipt 3
6 Elements of a consent record and consent receipt 3
6.1 Overall objectives 3
6.2 Recordkeeping for online privacy notices and consent 4
6.2.1 General 4
6.2.2 PII controller recordkeeping 4
6.2.3 Recordkeeping for consent receipts 5

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/iso/...a88e-fb0f5a2fe268/iso-iec-dts-27560

© ISO 2021 – All rights reserved

6.2.4 Relationship between records and receipts — control 6
6.3 Record information structure 6
6.3.1 General 6
6.3.2 Structure of the consent record 7
6.3.3 Record header section contents 9
6.3.4 PII processing section contents 11
6.3.5 PII information 20
6.3.6 Party identification section contents 22
6.3.7 Event section contents 24
6.4 Receipt information structure 27
6.4.1 General 27
6.4.2 Structure of the receipt — control 27
6.4.3 Consent management — control 27
6.4.4 PII principal participation — control 27
6.4.5 Receipt metadata section contents 27
6.4.6 Receipt content — control 28
Annex A (informative) Examples of consent records and receipts 29
Annex B (informative) Example of consent record life cycle 35
Annex C (informative) Performance and efficiency considerations 40
Annex D (informative) Consent record encoding structure 45
Annex E (informative) Security of consent records and receipts 46
Annex F (informative) Signals as controls communicating PII principal's preferences and decisions 48
Annex G (informative) Guidance on the application of consent receipts in the context of privacy information management systems 50
Annex H (informative) Mapping to ISO/IEC 29184 60
Bibliography 63

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/sist/5915d5d0-a4d1-41a2-a88e-fb0f5a2fe268/iso-iec-dts-27560

© ISO 2021 – All rights reserved

Foreword

ISO (the International Organization for Standardization) ~~is a~~ and IEC (the International Electrotechnical Commission) form the specialized system for worldwide ~~federation of national standards~~standardization. National bodies ~~(~~that are members of ISO ~~member bodies). The work~~or IEC participate in the development of ~~preparing~~ International Standards ~~is normally carried out~~ through ~~ISO~~ technical committees~~. Each member body interested in a subject for which a technical committee has been~~ established ~~has the right to be represented on that committee. International~~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. ~~ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.~~

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 ~~ISO documents~~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~~ 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

~~Attention is drawn~~ISO and IEC draw attention to the possibility that ~~some of~~ the ~~elements~~implementation of this document may ~~be~~involve the ~~subject~~use of (a) patent ~~rights. ISO~~(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. ~~Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).~~

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~~) 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~~www.iso.org/members.html and www.iec.ch/national-committees.

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Font: Font color: Auto

Formatted: std_publisher, Font: Font color: Auto

Formatted: Font: Font color: Auto

Formatted: std_docNumber, Font: Font color: Auto

Formatted: Foreword Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border), Between : (No border), Tab stops: Not at 1.4 cm + 2.1 cm + 2.8 cm + 3.5 cm + 4.2 cm + 4.9 cm + 5.6 cm + 6.3 cm + 7 cm

Formatted: std_docNumber, Font: Font color: Auto

Formatted: Font: Font color: Auto

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5913d3d0-a4d7-41a2-a88e-fb0f5a2fe268/iso-iec-dts-27560

© ISO 2021 – All rights reserved

Introduction

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

- consent obtained from individuals prior to ~~the~~ collecting and processing personally identifiable information (PII); and
- the means by which individuals keep track of such content.

ISO/IEC 29184 ~~[9]~~ specifies controls which shape the content and the structure of online privacy notices, and~~,~~ the process of asking for consent to collect and process ~~personally identifiable information (~~PII~~)~~ from PII principals. ISO/IEC 29184 ~~[9]~~ 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 ~~[9]~~ does not address the needs of PII principals.

This document builds upon ISO/IEC 29184 ~~[9],~~ by addressing the concept of giving the PII principal a record for their own recordkeeping, which includes information about the PII processing agreement and interaction. We call this record the "consent receipt".

This document specifies a structure that is used by both principals in consent management: an organization that keeps records with good integrity (subject to the defined controls), and an ~~artifact~~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.

iTeh Standards (https://standards.iteh.ai) Document Preview
ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/sist/5913d3d0-a4d7-41a2-a88e-fb0f5a2fe268/iso-iec-dts-27560

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: List Continue 1, No bullets or numbering, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Formatted: std_publisher, Font:

Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: std_docNumber, Font:

Formatted: std_publisher, Font:

Formatted: std_docNumber, Font:

Formatted: std_publisher, Font:

Formatted: std_docNumber, Font:

Formatted: std_publisher, Font:

Formatted: std_docNumber, Font:

© ISO 2021 – All rights reserved

~~Information~~

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/sist/5913d3d0-a4d7-41a2-a88e-fb0f5a2fe268/iso-iec-dts-27560

~~© ISO 2021 – All rights reserved~~

© ISO/IEC 2023 – All rights reserved

Formatted: Font: 11.5 pt, Bold, English (United Kingdom)

Formatted: Font: 11.5 pt, Bold, English (United Kingdom)

Formatted: Normal

Formatted: Font: 11.5 pt, Bold, English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: Font: 11 pt

Formatted: Space After: 0 pt, Line spacing: single

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/sist/5913d3d0-a4d7-41a2-a88e-fb0f5a2fe268/iso-iec-dts-27560

Privacy technologies — Consent record information structure

~~1.~~1 Scope

This document specifies an interoperable, open and extensible information structure for recording PII principals' consent to PII processing. This document ~~— further~~ 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 ~~lifecycle~~life cycle of the recorded consent.

~~2.~~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* ~~[9]~~

ISO/IEC ~~-~~29184:2020, *Information technology — Online privacy notices and consent* ~~[10]~~

~~3.~~3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29100~~: 2011 [9],~~ ISO/IEC 29184~~: 2020 [10]~~ and the following apply.

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

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

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

© ISO/IEC 2023 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 27560
iec-dts-27560

Formatted: Section start: New page, Different first page header
Formatted: Space Before: 20 pt, After: 38 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font color: Blue, English (United Kingdom)
Formatted: Font: Bold, Font color: Blue, English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Bullets and Numbering
Formatted: List Continue 1, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted ...
Formatted: Bullets and Numbering
Formatted: std_publisher, Font:
Formatted ...
Formatted: std_docNumber, Font:
Formatted: std_year, Font:
Formatted: std_docTitle, Font:
Formatted: std_publisher, Font:
Formatted: std_docNumber, Font:
Formatted: std_year, Font:
Formatted: std_docTitle, Font:
Formatted ...
Formatted: Bullets and Numbering
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_publisher
Formatted: std_docNumber
Formatted ...
Formatted: No underline, Font color: Auto
Formatted ...
Formatted ...
Formatted ...
Formatted ...

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 ~~[9]~~, 2.4, modified – Notes 1 and 2 to entry have been added]

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

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

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

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

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

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

~~[SOURCE:ISO/IEC 29100:2011 [9], 2.8 opt-in]~~

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/sist/5913d3d0-a4d7-41a2-a88e-iec-dts-27560

~~4.~~4 ~~Symbols and abbreviated~~Abbreviated terms

~~GDPR General Data Protection Regulation~~
~~JSON JavaScript Object Notation~~
~~UUID Universally Unique Identifier~~

ASCII American Standard Code for Information Interchange
GDPR general Data Protection Regulation
HMAC hash-based message authentication code
JSON JavaScript object notation
UTF unicode transformation format
UUID universally unique identifier

Formatted: Normal, Space After: 36 pt, Line spacing: Exactly 12 pt
Formatted: Font: 12 pt
Formatted: Source, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_year
Formatted: std_section
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Default Paragraph Font, Font: Cambria, English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Default Paragraph Font, Font: Cambria, English (United Kingdom)
Formatted: Default Paragraph Font, Font: Cambria, English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Bullets and Numbering
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

~~5.~~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~~:2020 [10], see~~. See Annex H for the mapping ~~of~~between the clauses ~~to~~of this document and those in ISO/IEC 29184~~: 2020 [10]~~.

5.2 Consent record

A consent record documents the PII principal's decision regarding ~~consenting~~consent to ~~processing of~~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 ~~within a consent record~~therein. Receipts are intended for entities to share information regarding consent, such as a PII controller ~~providing~~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.~~6 Elements of a consent record and consent receipt

6.1 Overall objectives

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

- the PII requested by a PII controller to perform certain activities ~~using the PII~~;
- 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 ~~of~~when: the PII ~~request~~is requested by the PII controller, the PII principal ~~giving~~gives consent, and the PII ~~receipt~~is received by the PII controller.

~~© ISO #### – All rights reserved~~

© ISO/IEC 2023 – All rights reserved

Formatted: Normal, Right, Space After: 36 pt, Line spacing: Exactly 12 pt
Formatted: Font: 12 pt
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Bullets and Numbering
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...
Formatted ...
Formatted: Not Highlight
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...
Formatted: Bullets and Numbering
Formatted ...
Formatted: Font: Cambria, English (United Kingdom)
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

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

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

See Annex G for guidance to implementors of ISO/IEC 27701~~: 2019 [8]~~.

6.2 Recordkeeping for online privacy notices and consent

6.2.1 General

~~Clause 6.2~~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 ~~of~~ sufficient details to enable ongoing reference to the notice provided in accordance with ISO/IEC 29184:2020 ~~[10] clause~~ 6.2.8 and to enable management of changing conditions with respect to the notice and consent in ISO/IEC 29184:2020 ~~[10], clause~~ 6.5.

6.2.2 PII controller recordkeeping

6.2.2.1 Presentation of notice ~~—~~ control

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

6.2.2.2 Timeliness of notice ~~—~~ control

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

NOTE The content of notices is described in ISO/IEC 29184:2020 ~~[10], clause~~ 5.3.

6.2.2.3 Obtaining consent ~~—~~ control

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

6.2.2.4 Time and manner of consent ~~—~~ control

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

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/sist/59b3d3d0-a4d7-41a2-a88e-2fe268/iso-iec-dts-27560

Formatted: Normal, Space After: 36 pt, Line spacing: Exactly 12 pt
Formatted: Font: 12 pt
Formatted: English (United Kingdom)
Formatted ...
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...
Formatted ...
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left + 0.99 cm, Left + 1.27 cm, Left
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...
Formatted ...
Formatted: std_section
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left + 0.99 cm, Left + 1.27 cm, Left
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted: std_section
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted: cite_sec
Formatted ...
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

See Annex E for security of consent records and receipt.

6.2.2.6 Unique reference — control

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

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

6.2.2.7 Legal compliance — control

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

6.2.3 Recordkeeping for consent receipts

6.2.3.1 Provision of consent receipt — control

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

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

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

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

6.2.3.2 Contents of consent receipts — control

The information provided as a consent receipt ~~may~~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~~, data protection~~ requirements and the rights of the PII principal ~~has about independence of action~~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 ~~this document (see~~ 6.3~~).~~.

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

~~© ISO #### – All rights reserved~~

© ISO/IEC 2023 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC DTS 27560
https://standards.iteh.ai/catalog/standards/sist/5913d3d0-a4d7-41a2-a...-2fe268/iso-iec-dts-27560

Formatted: Normal, Right, Space After: 36 pt, Line spacing: Exactly 12 pt
Formatted: Font: 12 pt
Formatted: cite_app
Formatted: cite_app
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left + 0.99 cm, Left + 1.27 cm, Left + 1.55 cm, Left + 1.9 cm, Left
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Font: Cambria
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.71 cm, Left + 0.99 cm, Left + 1.27 cm, Left
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted ...
Formatted: cite_app
Formatted: cite_app
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted ...
Formatted: cite_sec
Formatted ...
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single