PD ISO/IEC TS 27560:2023



BSI Standards Publication

Privacy technologies — Consent record information structure

bsi.

National foreword

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

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

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

Contractual and legal considerations

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

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

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

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

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

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

ISBN 978 0 539 28510 9

ICS 35.030

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

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

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/IEC TS 27560:2023

TECHNICAL SPECIFICATION

ISO/IEC TS 27560

First edition
2023-08

Privacy technologies — Consent record information structure

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

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

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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

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

Published in Switzerland

© ISO/IEC 2023 – All rights reserved

Contents

Page

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

© ISO/IEC 2023 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2023 – All rights reserved

Introduction

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

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

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

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

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

This document specifies a structure that is used by both principals in consent management: namely a specification for data to be held by the organization to allow record-keeping with good integrity (subject to the defined controls), and an artefact (the “consent receipt”) that is given to the individual whose PII is being processed.

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

© ISO/IEC 2023 – All rights reserved

Privacy technologies — Consent record information structure

1 Scope

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

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

— exchange of consent information between information systems;

— management of the life cycle of the recorded consent.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

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

3 Terms and definitions

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

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

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

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

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

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

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

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

© ISO/IEC 2023 – All rights reserved