



NSAI
Standards

Irish Standard
I.S. EN ISO/IEC 29101:2021

Information technology - Security techniques - Privacy architecture framework (ISO/IEC 29101:2018)

I.S. EN ISO/IEC 29101:2021

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on:

EN ISO/IEC 29101:2021

Published:

2021-10-13

This document was published under the authority of the NSAI and comes into effect on:

2021-10-31

ICS number:

35.030

NOTE: If blank see CEN/CENELEC cover page

NSAI
1 Swift Square,
Northwood, Santry
Dublin 9

T +353 1 807 3800
F +353 1 807 3838
E standards@nsai.ie
W NSAI.ie

Sales:
T +353 1 857 6730
F +353 1 857 6729
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

National Foreword

I.S. EN ISO/IEC 29101:2021 is the adopted Irish version of the European Document EN ISO/IEC 29101:2021, Information technology - Security techniques - Privacy architecture framework (ISO/IEC 29101:2018)

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

For relationships with other publications refer to the NSAI web store.

Compliance with this document does not of itself confer immunity from legal obligations.

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

This page is intentionally left blank

EUROPEAN STANDARD

EN ISO/IEC 29101

NORME EUROPÉENNE

EUROPÄISCHE NORM

October 2021

ICS 35.030

English version

Information technology - Security techniques - Privacy architecture framework (ISO/IEC 29101:2018)

Technologies de l'information - Techniques de sécurité
- Architecture de référence de la protection de la vie
privée (ISO/IEC 29101:2018)

Informationstechnik - Sicherheitstechniken -
Rahmenwerk für Datenschutz (ISO/IEC 29101:2018)

This European Standard was approved by CEN on 27 September 2021.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



**CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels**

Contents	Page
European foreword.....	3

European foreword

The text of ISO/IEC 29101:2018 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 29101:2021 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by April 2022, and conflicting national standards shall be withdrawn at the latest by April 2022.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 29101:2018 has been approved by CEN-CENELEC as EN ISO/IEC 29101:2021 without any modification.

This page is intentionally left blank

**INTERNATIONAL
STANDARD**

**ISO/IEC
29101**

Second edition
2018-11

**Information technology — Security
techniques — Privacy architecture
framework**

*Technologies de l'information — Techniques de sécurité —
Architecture de référence de la protection de la vie privée*



Reference number
ISO/IEC 29101:2018(E)

© ISO/IEC 2018

ISO/IEC 29101:2018(E)



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

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
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	1
5 Overview of the privacy architecture framework	1
5.1 Elements of the framework.....	1
5.2 Relationship with management systems.....	3
6 Actors and PII	3
6.1 Overview.....	3
6.2 Phases of the PII processing life cycle.....	4
6.2.1 Collection.....	4
6.2.2 Transfer.....	5
6.2.3 Use.....	5
6.2.4 Storage.....	6
6.2.5 Disposal.....	6
7 Concerns	6
7.1 Overview.....	6
7.2 The privacy principles of ISO/IEC 29100.....	6
7.3 Privacy safeguarding requirements.....	7
8 Architectural views	7
8.1 General.....	7
8.2 Component view.....	8
8.2.1 General.....	8
8.2.2 Privacy settings layer.....	9
8.2.3 Identity management and access management layer.....	12
8.2.4 PII layer.....	14
8.3 Actor view.....	19
8.3.1 General.....	19
8.3.2 ICT system of the PII principal.....	20
8.3.3 ICT system of the PII controller.....	20
8.3.4 ICT system of the PII processor.....	21
8.4 Interaction view.....	22
8.4.1 General.....	22
8.4.2 Privacy settings layer.....	22
8.4.3 Identity and access management layer.....	23
8.4.4 PII layer.....	23
Annex A (informative) Examples of the PII-related concerns of an ICT system	25
Annex B (informative) A PII aggregation system with secure computation	30
Annex C (informative) A privacy-friendly, pseudonymous system for identity and access control management	37

ISO/IEC 29101:2018(E)

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. 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.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 29101:2013) which has been technically revised. The main change compared to the previous edition is that old Annex D has been removed.

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.

Introduction

This document describes a high-level architecture framework and associated controls for the safeguarding of privacy in information and communication technology (ICT) systems that store and process personally identifiable information (PII).

The privacy architecture framework described in this document:

- provides a consistent, high-level approach to the implementation of privacy controls for the processing of PII in ICT systems;
- provides guidance for planning, designing and building ICT system architectures that safeguard the privacy of PII principals by controlling the processing, access and transfer of personally identifiable information; and
- shows how privacy enhancing technologies (PETs) can be used as privacy controls.

This document builds on the privacy framework provided by ISO/IEC 29100 to help an organization define its privacy safeguarding requirements as they relate to PII processed by any ICT system. In some countries, privacy safeguarding requirements are understood to be synonymous with data protection/privacy requirements and are the subject of data protection/privacy legislation.

Information technology — Security techniques — Privacy architecture framework

1 Scope

This document defines a privacy architecture framework that:

- specifies concerns for ICT systems that process PII;
- lists components for the implementation of such systems; and
- provides architectural views contextualizing these components.

This document is applicable to entities involved in specifying, procuring, architecting, designing, testing, maintaining, administering and operating ICT systems that process PII.

It focuses primarily on ICT systems that are designed to interact with PII principals.

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, *Information technology — Security techniques — Privacy framework*

ISO/IEC/IEEE 42010, *Systems and software engineering — Architecture description*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29100 and ISO/IEC/IEEE 42010 apply.

4 Symbols and abbreviated terms

The following abbreviations apply to this document.

ICT Information and Communication Technology

PET Privacy Enhancing Technology

PII Personally Identifiable Information

5 Overview of the privacy architecture framework

5.1 Elements of the framework

The privacy architecture framework presented in this document is intended as a technical reference for developers of ICT systems that process PII. This document does not set requirements for privacy policies; it assumes that a privacy policy is in place and that privacy safeguarding requirements have been defined and that appropriate safeguards are implemented within the ICT system.

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

-
- [Looking for additional Standards? Visit Intertek Inform Infostore](#)
 - [Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation](#)
-