

# American National Standard

INCITS/ISO/IEC 29100:2011[2012]

(ISO/IEC 29100:2011, IDT)

*Information technology - Security techniques -  
Privacy framework*

**Developed by**



*Where IT all begins*



## INCITS/ISO/IEC 29100:2011[2012]

### PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

**Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.**

Date of ANSI Approval: 9/6/2012

Published by American National Standards Institute,  
25 West 43rd Street, New York, New York 10036

Copyright 2012 by Information Technology Industry Council  
(ITI). All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1101 K Street NW, Suite 610, Washington DC 20005.

Printed in the United States of America

First edition  
2011-12-15

---

---

## Information technology — Security techniques — Privacy framework

*Technologies de l'information — Techniques de sécurité — Cadre privé*

---

---

Reference number  
ISO/IEC 29100:2011(E)



This is a preview of "INCITS/ISO/IEC 29100...". Click [here](#) to purchase the full version from the ANSI store.



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "INCITS/ISO/IEC 29100...". Click here to purchase the full version from the ANSI store.

## Contents

Page

Foreword .....	v
Introduction.....	vi
1 Scope .....	1
2 Terms and definitions .....	1
3 Symbols and abbreviated terms .....	4
4 Basic elements of the privacy framework.....	5
4.1 Overview of the privacy framework.....	5
4.2 Actors and roles .....	5
4.2.1 PII principals .....	5
4.2.2 PII controllers.....	5
4.2.3 PII processors.....	5
4.2.4 Third parties .....	6
4.3 Interactions .....	6
4.4 Recognizing PII.....	7
4.4.1 Identifiers .....	7
4.4.2 Other distinguishing characteristics.....	7
4.4.3 Information which is or might be linked to a PII principal .....	8
4.4.4 Pseudonymous data .....	9
4.4.5 Metadata .....	9
4.4.6 Unsolicited PII.....	9
4.4.7 Sensitive PII .....	9
4.5 Privacy safeguarding requirements .....	10
4.5.1 Legal and regulatory factors .....	11
4.5.2 Contractual factors.....	11
4.5.3 Business factors.....	12
4.5.4 Other factors .....	12
4.6 Privacy policies .....	13
4.7 Privacy controls.....	13
5 The privacy principles of ISO/IEC 29100.....	14
5.1 Overview of privacy principles .....	14
5.2 Consent and choice .....	14
5.3 Purpose legitimacy and specification .....	15
5.4 Collection limitation .....	15
5.5 Data minimization.....	16
5.6 Use, retention and disclosure limitation .....	16
5.7 Accuracy and quality .....	16
5.8 Openness, transparency and notice .....	17
5.9 Individual participation and access.....	17
5.10 Accountability.....	18
5.11 Information security .....	18
5.12 Privacy compliance .....	19
<b>Annex A (informative) Correspondence between ISO/IEC 29100 concepts and ISO/IEC 27000 concepts .....</b>	<b>20</b>
<b>Bibliography.....</b>	<b>21</b>

This is a preview of "INCITS/ISO/IEC 29100...". [Click here to purchase the full version from the ANSI store.](#)

**Figures**

Figure 1 – Factors influencing privacy risk management ..... 11

**Tables**

Table 1 – Possible flows of PII among the PII principal, PII controller, PII processor and a third party and their roles 7

Table 2 – Example of attributes that can be used to identify natural persons 8

Table 3 – The privacy principles of ISO/IEC 29100 14

Table A.1 – Matching ISO/IEC 29100 concepts to ISO/IEC 27000 concepts 20

This is a preview of "INCITS/ISO/IEC 29100...". [Click here to purchase the full version from the ANSI store.](#)

## 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 29100 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

## Introduction

This International Standard provides a high-level framework for the protection of personally identifiable information (PII) within information and communication technology (ICT) systems. It is general in nature and places organizational, technical, and procedural aspects in an overall privacy framework.

The privacy framework is intended to help organizations define their privacy safeguarding requirements related to PII within an ICT environment by:

- specifying a common privacy terminology;
- defining the actors and their roles in processing PII;
- describing privacy safeguarding requirements; and
- referencing known privacy principles.

In some jurisdictions, this International Standard's references to privacy safeguarding requirements might be understood as being complementary to legal requirements for the protection of PII. Due to the increasing number of information and communication technologies that process PII, it is important to have international information security standards that provide a common understanding for the protection of PII. This International Standard is intended to enhance existing security standards by adding a focus relevant to the processing of PII.

The increasing commercial use and value of PII, the sharing of PII across legal jurisdictions, and the growing complexity of ICT systems, can make it difficult for an organization to ensure privacy and to achieve compliance with the various applicable laws. Privacy stakeholders can prevent uncertainty and distrust from arising by handling privacy matters properly and avoiding cases of PII misuse.

Use of this International Standard will:

- aid in the design, implementation, operation, and maintenance of ICT systems that handle and protect PII;
- spur innovative solutions to enable the protection of PII within ICT systems; and
- improve organizations' privacy programs through the use of best practices.

The privacy framework provided within this International Standard can serve as a basis for additional privacy standardization initiatives, such as for:

- a technical reference architecture;
- the implementation and use of specific privacy technologies and overall privacy management;
- privacy controls for outsourced data processes;
- privacy risk assessments; or
- specific engineering specifications.

Some jurisdictions might require compliance with one or more of the documents referenced in ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD2) — *Official Privacy Documents References* [3] or with other applicable laws and regulations, but this International Standard is not intended to be a global model policy, nor a legislative framework.