ICS 35.020, 35.040 SLOVENSKÁ TECHNICKÁ NORMA November 2020

STN	**Informačné technológie Bezpečnostné metódy Rámec ochrany osobných údajov (ISO/IEC 29100: 2011, vrátane zmeny A1: 2018)**	**STN EN ISO/IEC 29100 36 9758**

Information technology - Security techniques - Privacy framework (ISO/IEC 29100:2011, including Amd 1:2018)

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 10/20

Obsahuje: EN ISO/IEC 29100:2020, ISO/IEC 29100:2011, ISO/IEC 29100:2011/Amd 1:2018

131460

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 29100

June 2020

ICS 35.030

English version

Information technology - Security techniques - Privacy framework (ISO/IEC 29100:2011, including Amd 1:2018)

Technologies de l'information - Techniques de sécurité - Cadre privé (ISO/IEC 29100:2011, y compris Amd 1:2018)

Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Datenschutz (ISO/IEC 29100:2011, einschließlich Amd 1:2018)

This European Standard was approved by CEN on 31 May 2020.

This European Standard was corrected and reissued by the CEN-CENELEC Management Centre on 1 July 2020.

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

Contents

Page

European foreword

The text of ISO/IEC 29100:2011, including Amd 1:2018 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 29100:2020 by Technical Committee CEN/CLC/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of an identical text or by endorsement, at the latest by December 2020, and conflicting national standards shall be withdrawn at the latest by December 2020.

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

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 29100:2011, including Amd 1:2018 has been approved by CEN as EN ISO/IEC 29100:2020 without any modification.

INTERNATIONAL STANDARD

ISO/IEC 29100

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)

COPYRIGHT PROTECTED DOCUMENT

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
Web www.iso.org

Published in Switzerland

Contents

Page

Figures

Tables

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.

INTERNATIONAL STANDARD **ISO/IEC 29100:2011(E)**

Information technology — Security techniques — Privacy framework

1 Scope

This International Standard provides a privacy framework which

- specifies a common privacy terminology;
- defines the actors and their roles in processing personally identifiable information (PII);
- describes privacy safeguarding considerations; and
- provides references to known privacy principles for information technology.

This International Standard is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.