

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
Annex A (informative) Correspondence between ISO/IEC 29100 concepts and ISO/IEC 27000 concepts	20
Bibliography.....	21

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

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.

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.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE In order to make it easier to use the ISO/IEC 27000 family of International Standards in the specific context of privacy and to integrate privacy concepts in the ISO/IEC 27000 context, the table in Annex A provides the ISO/IEC 27000 concepts that correspond with the ISO/IEC 29100 concepts used in this International Standard.

2.1

anonymity

characteristic of information that does not permit a personally identifiable information principal to be identified directly or indirectly

2.2

anonymization

process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party

2.3

anonymized data

data that has been produced as the output of a personally identifiable information anonymization process

2.4

consent

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