INTERNATIONAL STANDARD

ISO/IEC 29134

First edition
2017-06

Information technology — Security techniques — Guidelines for privacy impact assessment

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'évaluation d'impacts sur la vie privée

Reference number
ISO/IEC 29134:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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 ISO documents 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 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 on 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 the following URL: www.iso.org/iso/foreword.html.

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

Introduction

A privacy impact assessment (PIA) is an instrument for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes personally identifiable information (PII) and, in consultation with stakeholders, for taking actions as necessary in order to treat privacy risk. A PIA report may include documentation about measures taken for risk treatment, for example, measures arising from the use of the information security management system (ISMS) in ISO/IEC 27001. A PIA is more than a tool: it is a process that begins at the earliest possible stages of an initiative, when there are still opportunities to influence its outcome and thereby ensure privacy by design. It is a process that continues until, and even after, the project has been deployed.

Initiatives vary substantially in scale and impact. Objectives falling under the heading of "privacy" will depend on culture, societal expectations and jurisdiction. This document is intended to provide scalable guidance that can be applied to all initiatives. Since guidance specific to all circumstances cannot be prescriptive, the guidance in this document should be interpreted with respect to individual circumstance.

A PII controller may have a responsibility to conduct a PIA and may request a PII processor to assist in doing this, acting on the PII controller's behalf. A PII processor or a supplier may also wish to conduct their own PIA.

A supplier's PIA information is especially relevant when digitally connected devices are part of the information system, application or process being assessed. It may be necessary for suppliers of such devices to provide privacy-relevant design information to those undertaking the PIA. When the provider of digital devices is unskilled in and not resourced for PIAs, for example:

— a small retailer, or

— a small and medium-sized enterprise (SME) using digitally connected devices in the course of its normal business operations,

then, in order to enable it to undertake minimal PIA activity, the device supplier may be called upon to provide a great deal of privacy information and undertake its own PIA with respect to the expected PII principal/SME context for the equipment they supply.

A PIA is typically conducted by an organization that takes its responsibility seriously and treats PII principals adequately. In some jurisdictions, a PIA may be necessary to meet legal and regulatory requirements.

This document is intended to be used when the privacy impact on PII principals includes consideration of processes, information systems or programmes, where:

— the responsibility for the implementation and/or delivery of the process, information system or programme is shared with other organizations and it should be ensured that each organization properly addresses the identified risks;

— an organization is performing privacy risk management as part of its overall risk management effort while preparing for the implementation or improvement of its ISMS (established in accordance with ISO/IEC 27001 or equivalent management system); or an organization is performing privacy risk management as an independent function;

— an organization (e.g. government) is undertaking an initiative (e.g. a public-private-partnership programme) in which the future PII controller organization is not known yet, with the result that the treatment plan could not get implemented directly and, therefore, this treatment plan should become part of corresponding legislation, regulation or the contract instead;

— the organization wants to act responsible towards the PII principals.

Controls deemed necessary to treat the risks identified during the privacy impact analysis process may be derived from multiple sets of controls, including ISO/IEC 27002 (for security controls) and ISO/IEC 29151 (for PII protection controls) or comparable national standards, or they may be defined by the person responsible for conducting the PIA, independently of any other control set.

Information technology — Security techniques — Guidelines for privacy impact assessment

1 Scope

This document gives guidelines for

— a process on privacy impact assessments, and

— a structure and content of a PIA report.

It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations.

This document is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII.

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 Guide 73:2009, *Risk management — Vocabulary*

ISO/IEC 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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