INTERNATIONAL STANDARD

ISO/IEC 29134

Second edition
2023-05

Information technology — Security techniques — Guidelines for privacy impact assessment

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

Reference number
ISO/IEC 29134:2023(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **3**
5 Preparing the grounds for PIA **4**
5.1 Benefits of carrying out a PIA 4
5.2 Objectives of PIA reporting 5
5.3 Accountability to conduct a PIA 5
5.4 Scale of a PIA 6
6 Guidance on the process for conducting a PIA **6**
6.1 General 6
6.2 Determine whether a PIA is necessary (threshold analysis) 7
6.3 Preparation of the PIA 7
6.3.1 Set up the PIA team and provide it with direction 7
6.3.2 Prepare a PIA plan and determine the necessary resources for conducting the PIA 9
6.3.3 Describe what is being assessed 10
6.3.4 Stakeholder engagement 11
6.4 Perform the PIA 13
6.4.1 Identify information flows of PII 13
6.4.2 Analyse the implications of the use case 14
6.4.3 Determine the relevant privacy safeguarding requirements 15
6.4.4 Assess privacy risk 16
6.4.5 Prepare for treating privacy risks 19
6.5 Follow up the PIA 23
6.5.1 Prepare the report 23
6.5.2 Publication 24
6.5.3 Implement privacy risk treatment plans 24
6.5.4 Review and/or audit of the PIA 25
6.5.5 Reflect changes to the process 26
7 PIA report **26**
7.1 General 26
7.2 Report structure 27
7.3 Scope of PIA 27
7.3.1 Process under evaluation 27
7.3.2 Risk criteria 29
7.3.3 Resources and people involved 29
7.3.4 Stakeholder consultation 29
7.4 Privacy requirements 29
7.5 Risk assessment 29
7.5.1 Risk sources 29
7.5.2 Threats and their likelihood 29
7.5.3 Consequences and their level of impact 30
7.5.4 Risk evaluation 30
7.5.5 Compliance analysis 30
7.6 Risk treatment plan 30
7.7 Conclusion and decisions 30
7.8 PIA public summary 30
Annex A (informative) **Scale criteria on the level of impact and on the likelihood** **32**

Annex B (informative) **Generic threats** **34**
Annex C (informative) **Guidance on the understanding of terms used** **38**
Annex D (informative) **Illustrated examples supporting the PIA process** **41**
Bibliography **43**

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 29134:2017), which has been technically revised.

The main changes are as follows:

— minor editorial changes have been made.

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 and www.iec.ch/national-committees.

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);

— taking necessary actions, in consultation with stakeholders, to treat privacy risk.

A PIA report can 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 circumstances.

A PII controller can have a responsibility to conduct a PIA and can request a PII processor to assist in doing this, acting on the PII controller's behalf. A PII processor or a supplier can 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 can be necessary for suppliers of such devices to provide privacy-relevant design information to those undertaking the PIA. It is possible that 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.

In such circumstances, in order to enable it to undertake minimal PIA activity, the device supplier can 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, legal and regulatory requirements regarding PIA can apply.

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 an 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 cannot be implemented directly and, therefore, it is presupposed that this treatment plan becomes part of corresponding legislation, regulation or the contract instead;

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

Controls deemed necessary to treat the risks identified during the privacy impact analysis process can 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 can 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 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29100, ISO/IEC 27000, ISO Guide 73 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
acceptance statement
formal management declaration to assume responsibility for risk ownership, risk treatment and residual risk

3.2
asset
things that have value to anyone involved in the processing of personally identifiable information (PII)

Note 1 to entry: In the context of a privacy risk management process, an asset is either PII or a supporting asset.