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)

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

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.

3.3
assessor
person who leads and conducts a *privacy impact assessment* (3.7)

Note 1 to entry: The assessor may be supported by one or more other internal and/or external experts as part of their team.

Note 2 to entry: The assessor may be an expert internal or external to the organization.

3.4
process
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: ISO/IEC 27000:2018, 3.54]

3.5
device
combination of hardware and software, or solely software, that allows a user to perform actions

3.6
privacy impact
anything that has an effect on the privacy of a PII principal and/or group of PII principals

Note 1 to entry: The privacy impact can result from the processing of PII in conformance or in violation of privacy safeguarding requirements.

3.7
privacy impact assessment
PIA
overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information, framed within an organization's broader risk management framework

[SOURCE: ISO/IEC 29100:2011, 2.20, modified — Note 1 to entry has been deleted.]

3.8
privacy risk map
diagram that indicates the level of impact and likelihood of privacy risks identified

Note 1 to entry: The map is typically used to determine the order in which the privacy risks should be treated.

3.9
programme
group of projects managed in a coordinated way to obtain benefits not available from managing them individually

[SOURCE: ISO 14300-1:2011, 3.2]

3.10
project
unique process, consisting of a set of coordinated and controlled activities with start and finish dates, undertaken to achieve an objective conforming to specific requirements, including the constraints of time, cost and resources

[SOURCE: ISO 9000:2015, 3.4.2]

3.11
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO/IEC 27000:2018, 3.50]

3.12
severity
estimation of the magnitude of potential impacts on the privacy of a PII principal

3.13
system
information system
set of applications, services, information technology assets, or other information handling components

[SOURCE: ISO/IEC 27000:2018, 3.36, modified — "system" has been added as a preferred term.]

3.14
stakeholder
person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

Note 1 to entry: Includes personally identifiable information principals, management, regulators and customers.

Note 2 to entry: Consultation with stakeholders is integral to a privacy impact assessment.

[SOURCE: ISO 37000:2021, 3.3.1, modified — Notes 1 and 2 to entry have been modified.]

3.15
technology
hardware, software, and firmware systems and system elements including, but not limited to, information technology, embedded systems, or any other electro-mechanical or processor-based systems

[SOURCE: ISO/IEC 16509:1999, 3.3]

4 Abbreviated terms

API	application programming interface
BYOD	bring your own device
ICT	information and communication technologies
IPMA	International Project Management Association
ISMS	information security management system
PII	personally identifiable information
PRINCE	PRojects IN controlled environments
SME	small and medium-sized enterprises

5 Preparing the grounds for PIA

5.1 Benefits of carrying out a PIA

This document provides guidance that can be adapted to a wide range of situations where PII is processed. However, in general, a PIA can be carried out for the purpose of:

— identifying privacy impacts, privacy risks and responsibilities;

— providing input to design for privacy protection (sometimes called privacy by design);

— reviewing a new information system's privacy risks and assessing its impact and likelihood;

— providing the basis for the provision of privacy information to PII principals on any PII principal mitigation action recommended;

— maintaining later updates or upgrades with additional functionality likely to impact the PII that are handled;

— sharing and mitigating privacy risks with stakeholders, or providing evidence relating to compliance.

NOTE A PIA is sometimes referred to by other terms, for example, a "privacy review" or a "data protection impact assessment". These particular instances of a PIA can come with specific implications for both process and reporting.

A PIA has often been described as an early warning system. It provides a way to detect potential privacy risks arising from the processing of PII and thereby informing an organization of where they should take precautions and build tailored safeguards before, not after, the organization makes heavy investments. The costs of amending a project at the planning stage is usually a fraction of those incurred later on. If the privacy impact is unacceptable, the project can even have to be cancelled altogether. Thus, a PIA helps to identify privacy issues early and/or to reduce costs in management time, legal expenses and potential media or public concern by considering privacy issues early. It can also help an organization to avoid costly or embarrassing privacy mistakes.

Although a PIA should be more than simply a compliance check, it does nevertheless contribute to an organization's demonstration of its compliance with relevant privacy and data protection requirements in the event of a subsequent complaint, privacy audit or compliance investigation. In the event of a privacy risk or breach occurring, the PIA report can provide evidence that the organization acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any liability, negative publicity and loss of reputation.

An appropriate PIA also demonstrates to an organization's customers and/or citizens that it respects their privacy and is responsive to their concerns. Customers or citizens are more likely to trust an organization that performs a PIA than one that does not.

A PIA enhances informed decision-making and exposes internal communication gaps or hidden assumptions on privacy issues about the project. A PIA is a tool to undertake the systematic analysis of privacy issues arising from a project in order to inform decision makers. A PIA can be a credible source of information.

A PIA enables an organization to learn about the privacy pitfalls of a process, information system or programme upfront, rather than having its auditors or competitors point them out. A PIA assists in anticipating and responding to the public's privacy concerns.

A PIA can help an organization gain the public's trust and confidence that privacy has been built into the design of a process, information system or programme.

Trust is built on transparency, and a PIA is a disciplined process that promotes open communications, common understanding and transparency. An organization that undertakes a PIA demonstrates to its employees and contractors that it takes privacy seriously and expects them that they do too. A PIA is a way of educating employees about privacy and making them alert to privacy problems that can damage

the organization. It is a way to affirm the organization's values. A PIA can be used as an indication of due diligence and can reduce the number of customer audits.

5.2 Objectives of PIA reporting

The PIA reporting objective is to communicate assessment results to stakeholders. Expectations from a PIA exist from multiple stakeholders.

The following are typical examples of stakeholders and their expectations.

— PII principal: PIA is an instrument to enable subjects of PII to have assurance that their privacy is being protected.

— Management: Several viewpoints apply with:

  — PIA as an instrument to manage privacy risks, create awareness and establish accountability; visibility over PII processing within the organization, and possible risks and impacts of the same; inputs to business or product strategy;

  — Building the PIA into the earliest stages of the project ensures the privacy requirements are included in the functional and non-functional requirements, are achievable, viable and traced through change and risk management and can result in the project not happening or being cancelled. The effort to classify and manage project PII should be funded as a separate investment line item and amount in a project or programme budget, acceptable to all stakeholders;

  — PIA as an opportunity to better understand privacy requirements and assess activities against these requirements; inputs for product or service design and delivery; reviewed and amended through the change management process after delivery;

  — PIA as an instrument to understand the privacy risks at the function/project/unit level; consolidation of risks; input to privacy policy design and enforcement mechanisms; inputs for re-engineering privacy processes.

— Regulator: PIA is an instrument that contributes evidence which supports compliance with applicable legal requirements. It can provide evidence of due diligence taken by the organization in case of breach, non-compliance, complaint, etc.

— Customer: PIA is a means to assess how the PII processor or PII controller is handling PII and provides evidence that it follows the contractual obligations.

PIA reporting should fulfil two basic functions. The first (inventory) keeps the specific stakeholders informed of identified affected entities, affected environment and privacy risks about the life cycle of the affected entities, whether it is inherent or mitigated. The second (action items) is a tracking mechanism on the actions/tasks that improve and/or resolve the identified privacy risks. Sensitivity to the distribution and release of the reporting information should be clearly assessed and classified (private, confidential, public, etc.).

5.3 Accountability to conduct a PIA

A PIA should be undertaken of processes or information systems by one of a number of different entities within the organization, but may also be carried out on a process, information system or programme by consumer organizations or non-governmental organizations.

Typically, the responsibility for ensuring that a PIA is undertaken should, in the first instance, lie with the person in charge of PII protection, otherwise with the project manager developing the new technology, service or other initiative that can impact privacy.

Accountability for ensuring the PIA is undertaken and the quality of the result (PIA accountability) should lie with the top management of the PII controller. The person who has been assigned responsibility for conducting the PIA may conduct it themselves, may enlist the help of other internal

and/or external stakeholders or may contract an independent third party to do the work. There are advantages and disadvantages to each approach.

However, when the PIA is performed directly by the organization, end-user associations or governmental agencies may request to have the PIA's adequacy verified by an independent auditor.

The organization should ensure that there is accountability and authority for managing privacy risks, including the implementation and maintenance of the privacy risk management process and for ensuring the adequacy and effectiveness of any controls. This can be facilitated by:

— specifying who is accountable for the development, implementation and maintenance of the framework for managing privacy risk, and

— specifying risk owners for implementing privacy risk treatment, maintaining privacy controls and reporting of relevant privacy risk information.

5.4 Scale of a PIA

The scale of the PIA will depend on how significant the impacts are assumed to be. For example, if the impacts are assumed to affect only employees of the organization (e.g. in case the organization wishes to improve its access control by means of a biometric such as a thumbprint from each employee), then the PIA can engage only employee representatives and be relatively small scale. However, if a government department wishes to introduce a new identity management system for all citizens, it should conduct a much larger PIA involving a wide range of external stakeholders.

It is presupposed that organizations provide self-assessment on the required scale of the PIA, in compliance with laws and regulations. The amount and granularity of the PII per person, the degree of sensitivity of PII, the number of PII principals and the number of people who have access to the PII that will be processed are the critical factors in determining this scale.

In the case of SMEs, non-profit or governmental organizations, the determination of the appropriate scale of the PIA can be jointly, but not bindingly, achieved by the person conducting a PIA (as per 5.3), the SME's senior management and/or advice from external experts, as appropriate.

6 Guidance on the process for conducting a PIA

6.1 General

The scope of a PIA, the specific details of what it covers and how it is conducted all should be adapted to the size of the organization, the local jurisdiction and the specific programme, information system or process that is the subject of the PIA. In Clause 6:

— the "objective" is something that should be achieved,

— the "input" provides guidance on information can be necessary to achieve the "objective",

— the "expected output" is the recommended target for the "actions",

— "actions", or their equivalents, are guidance on activities necessary to be carried out to achieve the "objective" and create the recommended "expected output", and

— "implementation guidance" provides more details of matters which have possible needs to be considered in performing the "actions".

The "actions" in this clause, or equivalents, adapted to the desired scope and scale of a PIA may be implemented stand-alone by an organization. They are intended to form a reasonable basis for planning, implementing and following up the PIA in a wide range of circumstances.

The organization conducting a PIA process may wish to directly adapt the process guidance below to its specific PIA scale and scope or as one possible alternative to select a suitable risk-based management

system, such as ISO/IEC 27001, and integrate into it appropriately adapted elements of the guidance below, including the use of the PIA report (see Clause 7) to treat the privacy risks it identifies.

In this document, the term “conducting a PIA” is used to cover both an initial PIA where the necessary steps and actions are selected to match the particular PIA requirement and an update to an existing PIA where only the steps and actions necessary for the update are carried out.

Annex C provides further guidance on the understanding of terms used in this document.

To support SMEs in the PIA process, industry associations or bodies of SMEs should be encouraged to draw up codes of conduct providing valuable guidelines, and SMEs should be encouraged to take part in these activities. Reasonable codes of conduct should respect the values set forth in this document and can be endorsed by data protection authorities.

6.2 Determine whether a PIA is necessary (threshold analysis)

Objective: To determine whether a new or updated PIA is necessary.

Input: Information about the programme, information system or process under assessment.

Expected output: Threshold analysis result, and mandate to prepare a new or updated PIA if required, terms of reference and scope of the PIA decided.

Actions:

The organization’s management should decide if a new or updated PIA is required.

If a new or updated PIA is required, the organization’s management, in conjunction with the assessor to be, should define the terms of reference and determine the boundaries and applicability of the PIA to establish its scope. The organization should also decide on and document the scale of the PIA, the process to be used to perform the PIA, and on the target audiences, hence the nature and contents of the PIA reports to be produced.

Output of this process in terms of the threshold analysis result and the PIA scope and terms of reference should be documented in the PIA report (see 7.2).

Implementation guidance:

An organization should conduct a new or updated PIA if it perceives impacts on privacy from:

— a new or prospective technology, service or other initiative where PII is, or will be, processed,

— a decision that sensitive PII (see ISO/IEC 29100:2011, 2.26) is going to be processed,

— changes in applicable privacy related laws and regulations, internal policy and standards, information system operation, purposes and means for processing data, new or changed data flows, etc.; and

— business expansion or acquisitions.

There is a possibility that an organization wishes to establish a policy setting out thresholds for triggering a new or updated PIA and initial technical and organizational measures to apply. Such a policy should take account of any applicable issues from those listed above, setting boundaries within which processing of PII can be developed and operated without triggering a new PIA.

6.3 Preparation of the PIA

6.3.1 Set up the PIA team and provide it with direction

Objective: To determine the scope of the PIA and the needed expertise and to formulate the terms of reference for conducting the PIA.