Personal Information Impact Assessment Platform

AI Assurance

www.aiassurance.co.za

Contents

Introduction to the Personal Information Impact Assessment

The Protection of Personal Information Act No. 4 of 2013 (POPIA), effective from 1 July 2020, establishes a legal framework to safeguard personal information in South Africa, aligning with the constitutional right to privacy. POPIA applies to all public and private bodies, with limited exceptions, and defines personal information as any data relating to an identifiable living natural person or existing juristic person, such as a company. Responsible parties must comply with POPIA's conditions for lawful processing and ensure data subjects can exercise their rights, including access, rectification, and objection. The Act mandates the adoption of reasonable technical and organizational measures to protect the integrity and confidentiality of personal information, preventing loss, damage, unauthorized destruction, or unlawful access. These measures include identifying foreseeable risks, implementing and maintaining safeguards, verifying their effectiveness, and updating them to address new risks or deficiencies, in line with generally accepted information security practices and industry-specific regulations. Additionally, responsible parties must ensure personal information is complete, accurate, and updated as necessary.

Central to POPIA compliance is the requirement under Regulation 4(1)(b) to conduct a **Personal Information Impact Assessment (PIIA)**. A PIIA is a critical tool for identifying and analysing risks to data subjects arising from an organization's use of specific technologies or systems, and for determining appropriate measures to mitigate these risks. Unlike traditional enterprise risk management, which focuses on organizational risks, a PIIA prioritizes the rights and freedoms of data subjects, requiring the identification of all reasonably foreseeable internal and external risks to personal information, with no acceptable residual risk. Every instance of processing is considered an interference with data subjects' rights and must be justified. The PIIA process begins with a systematic description of the envisaged data processing and its purposes, including any legitimate interests of the responsible party under Section 11(1)(f) of POPIA. Where appropriate, data subjects must be involved to express their views on the processing's impact, enabling an assessment of its necessity and proportionality under Sections 10 and 11(1)(d).

The PIIA is complete when it includes measures to address identified risks, such as safeguards, security mechanisms, and compliance measures, including protocols for breach notifications under Section 22(1) of POPIA. The standard for risk identification is objective foreseeability, meaning responsible parties are liable for negligence if they fail to anticipate risks a reasonable person would foresee. This liability extends to risks caused by service providers, with the burden of proof on the responsible party to demonstrate comprehensive risk assessment and mitigation. The PIIA process, structured into three

stages - Preparation, Evaluation, and Report and Safeguards—combines procedural and evaluative elements to ensure reproducible, verifiable results. This technology-neutral approach facilitates compliance verification by the Information Regulator, supports comparison of solutions, and ensures adherence to POPIA's rigorous data protection standards.

Safeguarding personal information

The purpose of POPIA includes giving effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible party. It requires the integrity and confidentiality of personal information in the possession or under the control of a responsible party to be secured by taking appropriate, reasonable technical and organisational measures to prevent—

a) loss of, damage to or unauthorised destruction of personal information; and
b) unlawful access to or processing of personal information.

Responsible parties are required to take reasonable measures to:

- ensure all reasonably foreseeable internal and external risks to personal information in its possession or under its control are identified,
- appropriate safeguards against the identified risks are established and maintained,
- the effectiveness of the implemented safeguards are regularly verified, and
- the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguard

Process to Conduct a Personal Information Impact Assessment

The Personal Information Impact Assessment (PIIA) process is a continuous improvement approach that ensures personal information processing respects data subjects' right to privacy while mitigating privacy risks. It is typically performed by the responsible party, with support from the Information Officer (IO), project owners, and other stakeholders. The process is divided into four main stages: Context Study, Conditions for Lawful Processing Study, Data Protection Risks Study, and PIIA Validation. Each stage includes specific steps, objectives, and deliverables, supported by templates for documentation in a PIIA online tool.

1. Study of the Context

Objective: Gain a comprehensive understanding of the personal information processing operations under consideration to define the scope and focus of the PIIA.

Steps:

- **Overview of the Processing:**
    - Provide a brief description of the processing, including its **nature, scope, context, purposes, and focus** (e.g., expected benefits for the organization, data subjects, or society).
    - Identify the **responsible party** and any **operators** involved.
    - List applicable mandatory legislation, regulations and approved codes of conduct and voluntary standards or sector-specific requirements.
    - **Template**: Use the PIIA tool template for "Overview of the processing" to document:
        - Description of the processing (nature, scope, context).
        - Processing purposes and expected benefits.
        - Responsible party and operator(s) details.
        - Applicable legislation, standards and their consideration.
- **Information, Processes, and Supporting Assets:**
    - Define the scope by detailing:
        - **Personal information** involved, their recipients, and retention periods.
        - **Processes** and **supporting assets** (e.g., hardware, system software, AI models, training data, AI application, networks, people, paper) across the data lifecycle (collection to erasure).
- Create a **data flow diagram** to illustrate subsystems, stakeholders, interfaces, and connections.
- **Template**: Use the PIIA tool template for "Data description, recipients and storage durations" and "Description of the processes and supporting assets" to document:
    - System components
    - Data types, recipients, and storage durations.
    - Detailed process descriptions and associated supporting assets.

Deliverable: A scoping statement that outlines the processing context, stakeholders, and assets, ensuring a clear foundation for the PIIA.

2. Study of the Fundamental Principles

Objective: Ensure compliance with POPIA conditions related to the proportionality, necessity, and lawfulness of processing, as well as the protection of data subjects' rights.

Steps:

- **Assessment of Controls Guaranteeing Proportionality and Necessity**:
    - Justify compliance with POPIA requirements:
        - **Purpose(s)**: Ensure they are specific, explicitly defines, and lawful (Sec. 13(1) POPIA).
        - **Lawfulness**: Verify the legal basis for processing (Sec. 11(1) POPIA, e.g., consent, contract, legitimate interest, legal obligation, public law duty).
        - **Data Minimization**: Confirm data is adequate, relevant, and limited to what is necessary (Sec. 10 POPIA).
        - **Information Quality**: Ensure data is complete, accurate, not misleading, and up-to-date (Sec. 16 POPIA).
        - **Retention and restriction**: Verify limited retention periods (Sec. 14(1) POPIA).
    - Check if improvements to controls are necessary or possible.
    - **Template**: Use the PIIA tool template for "Assessment of the controls guaranteeing the proportionality and necessity of the processing" to document:
        - Purposes and their legitimacy.
        - Lawfulness criteria and justifications.
        - Data minimization controls and justifications.
        - Information quality controls and justifications.
        - Retention periods, justifications, and erasure mechanisms.
        - Assessment of controls (acceptable or needs improvement) and corrective actions.

- **Assessment of Controls Protecting Data Subjects' Rights**:
    - Identify and describe controls to comply with GDPR rights:
        - **Information**: Ensure fair and transparent processing (Sec. 5, 8, 9, 10, 11, 13, 18, 22, 24, and 71 POPIA).
        - **Consent**: Obtain express, demonstrable, and withdrawable consent where applicable (Sec. 1, 11 POPIA).
        - **Access and Portability**: Facilitate rights of access and data portability (Sec. 23, 25, 14(6)(d) POPIA).
        - **Rectification and Erasure**: Enable rights to rectify and erase data (Sec. 24 POPIA).
        - **Restriction and Objection**: Support rights to restrict processing and object (Sec. 24 POPIA).
        - **Operators**: Ensure operators are identified and governed by contracts (Sec. 20, 21 POPIA).
        - **Information Transfers**: Comply with rules for information transfers outside South Africa (Sec. 72 POPIA).
    - Check if improvements to controls are necessary or possible.
    - **Template**: Use the PIIA tool template for "Assessment of controls protecting data subjects' rights" to document:
        - Controls for information (e.g., terms and conditions, accessibility, clarity).
        - Controls for consent (e.g., express consent, segmented consent, parental consent for minors).
        - Controls for access/portability, rectification/erasure, restriction/objection.
        - Processor contracts and compliance with Sec. 20, 21 POPIA.
        - Information transfer controls (e.g., processing and storage location, contractual clauses, safeguards).
        - Assessment of controls (acceptable or needs improvement) and corrective actions.

    Deliverable: A documented assessment of controls ensuring compliance with POPIA conditions and data subject rights, with identified corrective actions.

3. Study of Information Security Risks

Objective: Ensure compliance with POPIA conditions related to the proportionality, necessity, and lawfulness of processing, as well as the protection of data subjects' rights.

Steps:

- **Assessment of Existing or Planned Security Controls**:
  - Identify controls in three categories:
    - **Information-Specific Controls**: Encryption, anonymization, partitioning, access control, traceability, integrity monitoring, archiving, paper document security.
    - **General Security Controls**: Operating security, antivirus software, workstation management, website security, backups, maintenance, network security, monitoring, physical access control, hardware security, environmental risk avoidance, non-human risk protection.
    - **Organizational Controls**: Defined roles, data protection policies, risk management, project management, incident/breach management, personnel management, third-party relations, supervision.
  - Assess whether controls align with best security practices and identify improvements.
  - **Template**: Use the PIIA tool template for "Assessment of security controls" to document:
    - Implementation details for each control (e.g., encryption methods, access control rules).
    - Assessment of controls (acceptable or needs improvement) and corrective actions.
- **Risk Assessment: Potential Privacy Breaches**:
- For each feared event (illegitimate access, unwanted change, or loss of data):
    - Determine **potential impacts** on data subjects' privacy (e.g., unwanted solicitations, personal harm).
    - Estimate **severity** based on the prejudicial nature of impacts and existing controls.
    - Identify **threats** to supporting assets and **risk sources** (e.g., employees, external attackers).
    - Estimate **likelihood** based on vulnerabilities, risk source capabilities, and controls.

- Assess whether risks are acceptable given existing/planned controls
- Propose additional controls to reduce residual risks if necessary.
- **Template**: Use the PIIA template for "Risk assessment: potential privacy breaches" to document:
    - Risks (illegitimate access, unwanted change, loss of data).
    - Main risk sources, threats, potential impacts, and controls reducing severity/likelihood.
    - Severity and likelihood estimates.
    - Assessment of risks (acceptable or needs improvement), corrective controls, and residual severity/likelihood.

Deliverable: A risk assessment report detailing security controls, identified risks, their severity and likelihood, and an action plan for additional controls to mitigate unacceptable risks.

4. Validation of the PIIA

Objective: Formalize the PIIA findings, ensure stakeholder involvement, and decide whether to accept, improve, or refuse the processing based on the study.

Steps:

- **Preparation of Material for Validation**:
    - Consolidate findings:
        - Summarize controls for the constitutional right to privacy, indicating POPIA compliance (e.g., compliant, needs improvement).
        - Summarize security controls, indicating alignment with best practices.
        - Map risks (initial and residual) based on severity and likelihood.
        - Develop an **action plan** for additional controls, specifying responsible persons, costs, timeframes, and progress.
    - Document stakeholder involvement:
        - Advice from the Information Officer.
        - Views of data subjects or their representatives.
    - **Template**: Use the PIIA tool template for "Preparation of the material required for validation" to document:
    - Synthesis of controls for fundamental principles (with symbols: non-applicable, unsatisfactory, planned improvement, compliant).

- Synthesis of security controls.
- Risk mapping (visual representation of severity vs. likelihood).
- Action plan (additional controls, manager, frequency, difficulty, cost, progress).
- Information officer advice and data subject views, with justifications.

- **Formal Validation**:
  - The responsible party reviews the findings, focus, and stakeholder inputs to decide whether the PIA is:
    - **Validated**: Controls and residual risks are acceptable.
    - **Conditional on Improvement**: Specify required changes.
    - **Refused**: Processing cannot proceed due to high residual risks.
  - If improvements are needed, repeat previous steps until validation is achieved.
  - **Template**: Use the PIIA tool template for "Formal validation of the PIIA" to document:
    - Validation decision, date, and responsible person (e.g., Managing Director).
    - Processing purposes and justification for acceptability.
    - Signature of the data controller.

Deliverable: A validated PIA report, including a comprehensive action plan and documentation of stakeholder input, with a decision on the processing's acceptability.

Continuous Improvement and Monitoring

- **Monitoring**: Regularly review the PIIA (e.g., annually) to assess changes in context, controls, or risks.
- **Updates**: Revise the PIIA whenever significant changes occur (e.g., new processing purposes, technologies, or risks).
- **Early Implementation**: Conduct the PIIA during the design phase of processing to optimize controls and minimize costly retroactive changes.

Key Features of the POPIA PIIA Process

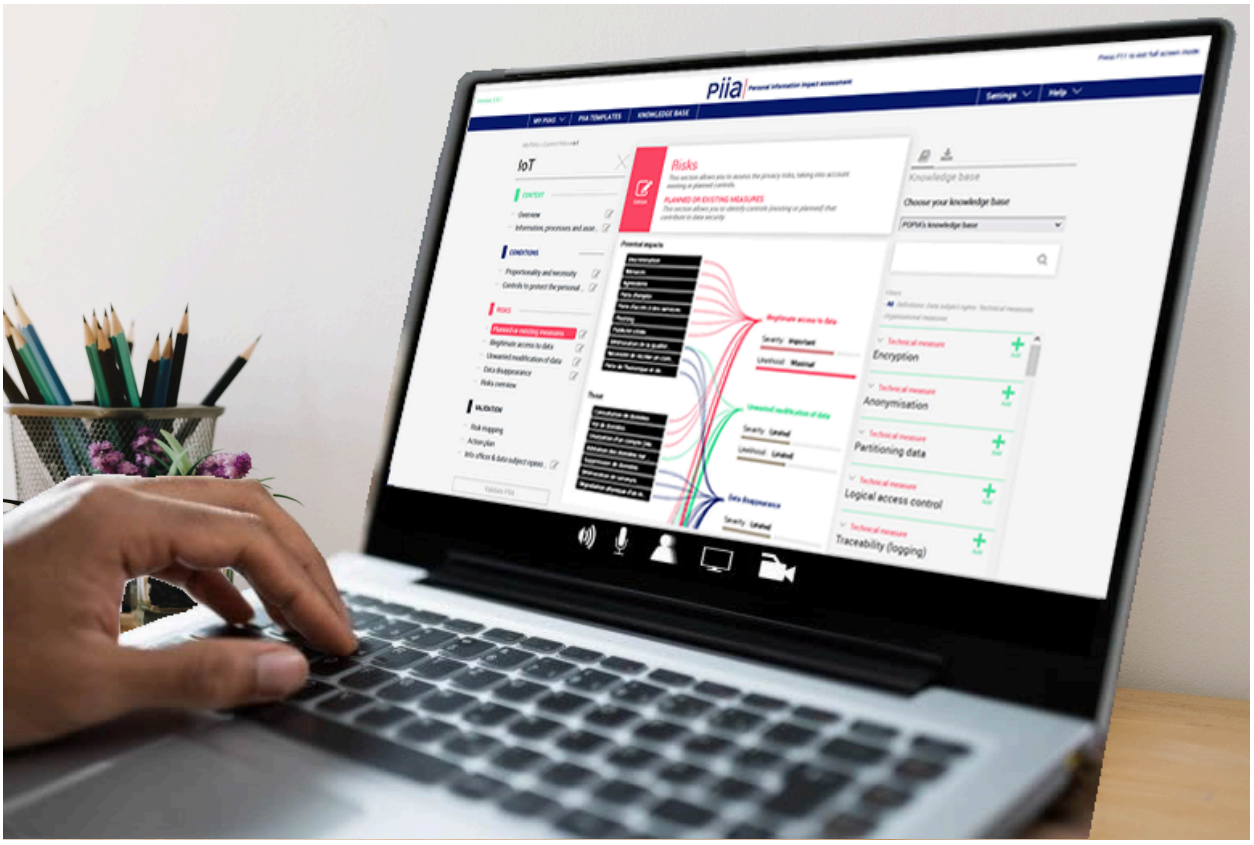
- **Compliance Focus**: Emphasizes POPIA compliance through adherence to conditions for lawful processing (e.g., lawfulness, data minimization) and protection of data subjects' rights.
- **Risk-Based Approach**: Assesses privacy risks from the data subjects' perspective, focusing on illegitimate access, unwanted changes, and data loss.
- **Stakeholder Involvement**: Requires input from the information officer and, where feasible, data subjects or their representatives to ensure transparency and accountability.
- **Iterative Nature**: Allows multiple iterations to refine controls and reduce risks to an acceptable level.
- **Standardized Documentation**: Provides templates to ensure reproducible, verifiable results that facilitate regulatory oversight and stakeholder review.
- **Privacy by Design**: Encourages early integration of privacy protections.

Benefits

- **For Responsible Parties**: Demonstrates accountability, optimizes risk management, and prevents costly breaches or penalties.
- **For Data Subjects**: Enhances trust by ensuring their rights and privacy are prioritized.
- **For Regulators**: Simplifies compliance verification through standardized reports.
- **For Technology Providers**: Supports Privacy by Design, enhancing market competitiveness.

Automation

Leverage the PIIA tool to enable seamless collaboration, empowering multiple users to efficiently conduct personal information impact assessments with enhanced accuracy and compliance.



AI Assurance

© AI Services

www.aiassurance.co.za

info@aiassurance.co.za