Information Officers Association

Helping you understand

POPIA

prior authorisation

Your guide to the Protection of Personal Information Act

www.informationofficers.co.za

Contents

The importance of protecting personal information

The Protection of Personal Information Act No 4 of 2013, (POPIA) commenced on 1 July 2020. All public and private bodies, with few specific exceptions, are required to comply with the POPIA requirements. Personal information is any information that relates to a living, identifiable natural person or an existing juristic person (e.g. a company). To process such information, one must comply with the information processing conditions contained in POPIA and enable data subjects to exercise the related rights.

POPIA compliance requires a comprehensive and ongoing focus on a broad range of operational activities that use personal information. It requires accountability and oversight (i.e. governance) of how personal information is being looked after and data subject rights are respected throughout its lifecycle.

Through the growing use of digital technologies, organisations are producing more personal information than ever before – making robust governance, safeguarding personal information, compliance with the conditions for the lawful processing of personal information and enabling data subjects to protect their personal information from processing that is not in accordance with the Act, more important than ever.

The way personal information is used and maintained is a key responsibility and is fundamental to the way responsible parties look after their staff, customers and other data subjects' rights, whether digitally or otherwise.

The Protection of Personal Information Act and its Regulations require information officers to fulfil certain responsibilities including:

- encouraging responsible parties to comply with the conditions for the lawful processing of personal information
- dealing with requests made to responsible parties from data subjects and the Regulator related to POPIA
- developing, implementing, monitoring and maintaining a compliance framework
- conducting personal information impact assessments to ensure that adequate measures and standards exist to comply with the conditions
- developing internal measures together with adequate systems to process requests from the Regulator, data subjects, and other interested parties.

As these are legal requirements, the Information Officers Association aims to assist information officers by sharing knowledge and promoting best practices.

How these guidelines can help

The Information Officers Association has developed this best practice guideline to assist members, affiliates and other interested parties in the processing of personal information so that they can make more informed decisions and, in turn, ensure their duties are fulfilled and the rights of data subjects are respected and enabled.

This document shares current best practices relating to data protection in South Africa, as well as the most relevant current legislation, regulations and guidance available from the Information Regulator.

What do these guidelines include?

Prior authorisation.

It's recommended that you explore the information provided and review the recommended practices against your current practices.

Disclaimer: The content of this document is for guidance and illustrative purposes only. These guidelines are neither advice nor a checklist to be used prescriptively to manage data protection obligations.

Introduction

“Prior authorisation” is a mechanism to alert the Information Regulator of processing that has the potential to significantly impact the rights of data subjects. On receipt of an application, the Regulator will record the request on its system and send the responsible party an acknowledgement email or letter with a reference number for the application.

Processing that requires prior authorisation

The responsible party must obtain prior authorisation from the Regulator prior to any processing if that responsible party plans to—

Unique identifiers of data subjects process for another purpose

a) Process any unique identifiers of data subjects—

i. for a purpose other than the one for which the identifier was specifically intended at collection; and

ii. with the aim of linking the information together with information processed by other responsible parties.

b) Where permission is granted the unique identifier can only be processed only under appropriate safeguards.

b) In general terms, a data subject can be considered as “identified” when, within a group of data subjects, he, she or it is "distinguished" from all other data subjects in the group.

Examples of unique identifiers:

- Bank account numbers, policy numbers,; supplier code or other account number;
- Reference number, membership number, subscription number, registration number;
- Identity number, passport number, employee number, student number, company number;
- Social media account handles, account login-ID, clickstream data;
- Telephone or cell phone number, MCC, MNC, LAC, Cell ID, CID/TAC: (Cell tower ID);
- Physical address, residential address, geo-location, ISP, Wi-Fi-location data;

- Service set identifier (“SSID”), International Mobile Subscriber Identity (“IMSI”) and International Mobile Equipment Identity (“IMEI”);
- Internet protocol (IP) addresses, Radio frequency identification (RFID) tags;
- Cookie identifiers (first-party, third-party), advertising IDs (Google), pixel tags, eTags;
- MAC (media access control) addresses; device fingerprints;
- Device type, software used, software settings;
- Car registration number and/or VIN;
- Biometric template (fingerprint, palm print, facial-recognition)
- Individual behaviour, patterns, topics of interest, websites visited;
- Combination of personal attributes (e.g. age);
- Combination of physical, physiological, genetic, mental, economic, cultural or social identity.

Examples of processing unique identifiers for a purpose other than original:

- Access control or identity verification for system access
- Application of artificial intelligence
- Data aggregation platforms
- Digital assistants and helpdesks
- Direct marketing
- Facial recognition systems
- Federated identity assurance services.
- Fraud prevention
- Hardware/software offering fitness / lifestyle / health monitoring
- Internet of Things devices, applications and platforms
- Lifestyle monitoring
- List brokering
- Loyalty schemes
- Monitoring personal use/uptake of statutory services or benefits
- Online advertising
- Online tracking by third parties

- Processing location data of employees
- Re-use of publically available data
- Research – academic and medical
- Social media networks
- Tracing services (tele-matching, tele-appending)
- Video surveillance of public areas
- Voice recognition/fingerprint/facial recognition access control
- Wealth profiling – identification of high net-worth individuals for direct marketing
- Web and cross-device tracking
- Wi-Fi/Bluetooth/RFID tracking.

Criminal behaviour or on unlawful or objectionable conduct

c) Process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties, including but is not limited to any reference check pertaining to past conduct or disciplinary action taken against a data subject.

Examples of processing:

- Conducting a criminal record enquiry (note SAPS Act prohibits this if not for law enforcement)
- Crime and fraud prevention co-operation with entities in a foreign country
- Reference check pertaining to the past conduct (e.g. credit check) or disciplinary action taken against a data subject
- Fraud detection and prevention
- Research into unlawful or objectionable conduct.

Credit reporting

d) Process information for the purposes of credit reporting, including processing of personal payment history, lending, and creditworthiness of a data subject by creating a credit report based on that information, and lenders or credit providers use credit reports along with other personal information to determine a data subject's creditworthiness;

Examples of processing:

- Credit bureaux registered with the National Credit Regulator or any person processing personal information for credit reporting purposes, including:

    - accept the filing of consumer credit information from any credit provider on payment of the credit bureau's filing fee, if any;
    - accept the filing of consumer credit information from the consumer concerned for the purpose of correcting or challenging information otherwise held by that credit bureau concerning that consumer;
    - take reasonable steps to verify the accuracy of any consumer credit information reported to it;
    - retain any consumer credit information reported to it for the prescribed period,irrespective of whether that information reflects positively or negatively on the consumer;
    - maintain its records of consumer credit information in a manner that satisfies the prescribed standards;
    - promptly expunge from its records any prescribed consumer credit information that, in terms of the regulations, is not permitted to be entered in its records or is required to be removed from its records;
    - issue a report to any person who requires it for a prescribed purpose or a purpose contemplated in the NCA, upon payment of the credit bureau's fee except where the Act explicitly provides that no fee be charged;
    - not draw a negative inference about, or issue a negative assessment of, a person's creditworthiness merely on the basis that the credit bureau has no consumer credit information concerning that person; and not knowingly or negligently provide a report to any person containing inaccurate information.

- *Investigating* fraud, corruption or theft, provided that the South African Police Service or any other statutory enforcement agency conducts such an investigation;
- Fraud detection and fraud prevention services;
- Considering a candidate for employment in a position that requires honesty in dealing with cash or finances;
- Assessing the debtors book of a business for the purposes of acquisition;

- The sale of the business or debtors book of that business;
- Undertaking transactions that is dependent upon determining the value of the business or debtors book of that business;
- Setting a limit of in respect of the supply of goods, services or utilities;
- Assessing an application for insurance (requires consent);
- Verifying educational qualifications and employment (requires consent);
- Obtaining consumer information to distribute unclaimed funds, including pension funds and insurance claims;
- Tracing a consumer by a credit provider in respect of a credit agreement entered into between the consumer and the credit provider;
- Developing a credit scoring system by a credit provider or credit bureau;
- investigating an application for debt review made by a consumer
- Credit reporting
    - Building loan (but not bond account)
    - Credit card transactions
    - Debt recovery (written-off debt being recovered)
    - Single credit facility (with agreed availability limit)
    - Open-services (for example: Telkom, cellphone contract, security contract)
    - Garage cards (not linked to credit cards)
    - Home loan (bond account)
    - Instalment (instalment agreements, hire purchase agreements)
    - Life insurance premiums
    - One-month personal loans
    - Secured pension or if insurance policy backs a loan
    - Open-limitless (repayment at period end)
    - Personal loan (repayment terms > 1 month)
    - Revolving credit store cards
    - Short term insurance (only premium details)
    - Student loan (from tertiary institution)
    - Utility bills (rates, water, electricity, levies)
    - Overdraft facility
    - Rental of assets (vehicles, white goods)
    - Rental of property
    - Vehicle asset finance
    - Revolving non-store card paid by instalment;

Data receiving

- Maintaining an effective and accessible credit market and industry;
- Encouraging responsible borrowing, avoidance of over indebtedness and fulfilment of financial obligations by consumers;

Data sharing via the Transmission hub

- Submission of credit information to credit bureaux using the data transfer service.

International transfers of special or children's personal information

e) Transfer special personal information (*religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information, criminal behaviour*), or the personal information of children or vulnerable persons to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

Examples:

Cloud computing that processes the personal information of children or vulnerable persons in a foreign country

- Schools using technology processing and/or storing personal information in a foreign country (Microsoft Office365 – Ireland, Google Docs, WhatsApp, FaceBook)
- Schools using data backup technologies located in a foreign country

Computing services that processes special personal information in a foreign country:

- Life, employee benefit, medical insurance and administration companies providing services in foreign countries and processing the health data in South Africa
- Life, employee benefit, medical insurance and administration companies using cloud services based in a foreign country
- Administrative bodies, pension funds, employers or institutions working for them, processing personal inforation for:
    - the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or
    - the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.
- Data backup to a storage location outside South Africa by insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations

- Companies assessing the working capacity of employees, performing medical diagnosis, providing health or social care, or treatment, or the management of health or social care systems and services using technologies based in a foreign country (e.g. Microsoft Azure in Ireland)

Social welfare organisations sharing personal information with donors in a foreign country, including information on a disease, information derived from the testing or examination of a body part or bodily substance including biological samples, a disability and disease risk of a person, tobacco consumption, lifestyle, medical history, clinical treatment or the physiological or biomedical state of the data subject

Foreign healthcare providers processing health data of South Africans across the border, including:

- data that are clearly medical data
- data that are raw sensor data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person (including stress, anxiety or sadness)
- conclusions that are drawn about a person's health status or health risk

International transfer of health data by foreign technology providers

- COVID-19 apps using Google or Apple technologies
- Lifestyle tracking devices

- Mobile phone apps that process health-related data of data subjects in South Africa
- Performance in a foreign country of a health-related contract between the data subject and a responsible party in South Africa
- Processing special personal information in a foreign country for the legitimate interest of the responsible party
- International organisations (health care, research, etc.)
    - conducting research studies, clinical trials, testing adverse drug reaction, epidemiology, genomic research, etc. by collecting, linking, and analysing diverse patient indicators and disease features of data subjects in South Africa
    - conducting that aim for an international scope, with results being compared and matched to achieve greater statistical significance
    - maintaining genomic databases that reflect the genetic diversity of patients across the world
    - providing personalised medicine
    - using algorithms in the diagnosis and treatment and requiring the collection of statistics from data subjects in South Africa
- Co-operation by a South African subsidiary with an international pharmaceutical or healthcare holding company
- Inter-governmental co-operation that includes the processing of health-related information.

Completing personal information impact assessments

Regulation 4(1)(b) of the regulations relating to the protection of personal information creates a legal obligation for responsible parties to perform personal information impact assessments. This regulation states that “a personal information impact assessment must be done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal”.

The personal information impact assessment (PIIA) is an instrument to identify and analyse the risks for data subjects, which exist due to the use of a certain technology or system by an organisation, and determine the most appropriate measures and standards to remedy the risks.

A well-prepared PIIA will ensure the request for prior authorisation is successful as, on submission of a request, the Regulator will investigate the lawfulness of the processing. It is therefore essential that the application form used to notify the regulator of the processing requiring prior authorisation is carefully prepared. It must address all of the POPIA requirements and include all the information the Regulator will require to investigate the processing.

Further, the responsible party must make certain that the processing requiring authorisation does comply with all the conditions for the lawful processing of personal information, and appropriate information security and data protection measures are implemented to safeguard the personal information to be processed by the responsible party and to enable the privacy rights of data subjects. If the processing doesn’t comply, the Regulator will not authorise the processing, and delays will be experienced in commencing this processing.

Submission of application form to Regulator

The Information Regulator has published a form that must be used by responsible parties to notify the Regulator of processing that requires prior authorisation.
Currently, the only electronic channel to submit the form is email (priorauthorisationIR@justice.gov.za).

Alternatively, the form can be submitted more securely via the postal service (Information Regulator, P.O Box 31533, Braamfontein, Johannesburg, 2017) or by hand (Information Regulator, JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001).

Investigation by Information Regulator

On receipt of a form notifying the Regulator of the processing requiring prior authorisation, the Regulator will investigate the lawfulness of the information processing.

Responsible parties may not carry out information processing that has been notified to the Regulator until the Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.

In the case of the notification of information processing which is subject to prior authorisation, the Regulator will inform the responsible party which applied for a prior authorisation in writing within four (4) weeks of the notification as to whether or not it will conduct a more detailed investigation.

Therefore, the Regulator may approve or reject an application for prior authorisation within four (4) weeks of receipt of prior authorisation application, unless the Regulator decides to conduct a detailed investigation.

In the event that the Regulator decides to conduct a more detailed investigation, the Regulator will inform the responsible party in writing of the reasonable period within which it plans to conduct a detailed investigation. This period will not exceed thirteen weeks.

A responsible party that has suspended its processing as required, and which has not received the Regulator's decision within thirteen weeks, may presume a decision in its favour and continue with its processing.

Conclusion of investigation

At the conclusion of the investigation, the Regulator must issue a written statement to the responsible party concerning the lawfulness of the processing. Should the Regulator find that the information processing is unlawful an enforcement notice will be served on the responsible party. The enforcement notice will contain a statement indicating the nature of the interference with the protection of the personal information of data subjects and the reasons for reaching that conclusion. It will also require the responsible party to do either or both of the following:

a) to take specified steps within a period specified in the notice, or to refrain from taking such steps; or

b) to stop processing personal information specified in the notice, or to stop processing personal information for a purpose or in a manner specified in the notice within a period specified in the notice.

Offences

Failure to notify the Regulator of processing subject to prior authorisation

A responsible party who fails to notify the Regulator of any processing that is subject to prior authorisation is guilty of an offence and upon conviction is liable to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment

Processing personal information before the investigation is complete

A responsible party who has notified the Regulator of processing that is subject to prior authorisation and carries out personal information processing before the investigation by the Regulator is completed or before receiving a notice that a more detailed investigation will not be conducted, is guilty of an offence and upon conviction is liable to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.

Non-compliance with a statement concerning the lawfulness of the information processing

A responsible party who fails to comply with a statement issued by the Regulator concerning the lawfulness of the information processing which is subject to prior authorisation, is guilty of an offence and upon conviction is liable to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment.

Administrative fine

Alternatively, the Regulator may impose an administrative fine not exceeding R10 million, payable by the responsible party who is alleged to have committed any of the offences mentioned above.

Automate

Automate the process to prepare a prior authorisation request using an online system. It comprises the predefined process and templates to capture the information required to prepare a submission.

Glossary and abbreviations

Credit Reporting	processing of personal payment history, lending, and credit worthiness of a data subject by creating a credit report based on that information, and lenders or credit providers use credit reports along with other personal information to determine a data subject's creditworthiness.
Criminal Behaviour	a criminal record enquiry.
Processing	the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure or destruction of information.
Unique Identifier	any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.
Unlawful or Objectionable Conduct	any reference check or information gathering pertaining to past behaviour, conduct or disciplinary action taken against a data subject.

If you have any queries, comments or suggestions regarding this document, please contact us at info@informationofficers.co.za.