PAIA MANUAL

Prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000 (as amended)

DATE OF COMPILATION: 13th October 2024
DATE OF REVISION: 25th May 2026

TABLE OF CONTENTS

Contents

1. LIST OF ACRONYMS AND ABBREVIATIONS 3
2. PURPOSE OF PAIA MANUAL 3
3. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF TP 4
4. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE 5
6. DESCRIPTION OF THE RECORDS OF TP WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION 7
7. DESCRIPTION OF THE SUBJECTS ON WHICH THE BODY HOLDS RECORDS AND CATEGORIES OF RECORDS HELD ON EACH SUBJECT BY TP 9
8. PROCESSING OF PERSONAL INFORMATION 10
9. AVAILABILITY OF THE MANUAL 17
10. FORMS 19

1. LIST OF ACRONYMS AND ABBREVIATIONS

1.1	**"CEO"**	Chief Executive Officer
1.2	**"CFO"**	Chief Finance Officer
1.3	'**COO'**	Chief Operating Officer
1.4	'**DPO'**	Data Protection Officer (Information Officer)
1.5	'**CPL'**	Country Privacy Lead (Deputy Information Officer)
1.6	**"Minister"**	Minister of Justice and Correctional Services;
1.7	**"PAIA"**	Promotion of Access to Information Act No. 2 of 2000(as Amended;
1.8	**"POPIA"**	Protection of Personal Information Act No.4 of 2013;
1.9	**"Regulator"**	Information Regulator; and
1.10	**"Republic"**	Republic of South Africa

2. PURPOSE OF PAIA MANUAL

This PAIA Manual is useful for the public to-

2.1 check the categories of records held by a body which are available without a person having to submit a formal PAIA request;

2.2 have a sufficient understanding of how to make a request for access to a record of the body, by providing a description of the subjects on which the body holds records and the categories of records held on each subject;

2.3 know the description of the records of the body which are available in accordance with any other legislation;

2.4 access all the relevant contact details of the Data Protection officer (Information Officer) and Country Privacy Lead (Deputy Information Officer) who will assist the public with the records they intend to access;

2.5 know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;

2.6 know if the body will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;

2.7 know the description of the categories of data subjects and of the information or categories of information relating thereto;

2.8 know the recipients or categories of recipients to whom the personal information may be supplied;

2.9 know if the body has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and

2.10 know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

3. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF TP

3.1. Information Officer

Name:	Justin Stevens
Country	Vice President of Compliance
Email:	Privacy@TP.com or
	Privacy.UK.SA@TP.co.uk

3.2. Deputy Information Officer

Name:	Rishi Nepaul
	Compliance Director
Email:	Privacy.UK.SA@TP.co.uk

Admin Officer

Name:	Emma Meacham
	Privacy Risk Manager
Email:	Privacy@TP.com or
	Privacy.UK.SA@TP.co.uk

Access to information general contacts

Email:	Privacy@TP.com or
	Privacy.UK.SA@TP.co.uk

3.3 **National or Head Office**

Postal Address: 2 Grand Parade Centre, 11 Adderley Street, Cape Town, Western Cape
Physical Address: 2 Grand Parade Centre, 11 Adderley Street, Cape Town, Western Cape
Telephone: 021 408 0100
Email: enquiries@**TP**.co.uk
Website: www.TP.com

4. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

4.1. The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised Guide on how to use PAIA ("Guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

4.2. The Guide is available in each of the official languages and in braille.

4.3. The aforesaid Guide contains the description of-

4.3.1. the objects of PAIA and POPIA;

4.3.2. the postal and street address, phone and fax number and, if available, electronic mail address of-

4.3.2.1. the Information Officer of every public body, and

4.3.2.2. every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA and section 56 of POPIA

4.3.3. the manner and form of a request for-

4.3.3.1. access to a record of a public body contemplated in section 11 and

4.3.3.2. access to a record of a private body contemplated in section 50

4.3.4. the assistance available from the IO of a public body in terms of PAIA and POPIA;

4.3.5. the assistance available from the Regulator in terms of PAIA and POPIA;

4.3.6. all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging-

4.3.6.1. an internal appeal;

4.3.6.2. a complaint to the Regulator; and

4.3.6.3. an application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;

4.3.7. the provisions of sections 14 and 51 requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;

4.3.8. the provisions of sections 15 and 52 providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

4.3.9. the notices issued in terms of sections 22 and 54 regarding fees to be paid in relation to requests for access; and

4.3.10. the regulations made in terms of section 92.

4.4. Members of the public can inspect or make copies of the Guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.

4.5. The Guide can also be obtained-

4.5.1. upon request to the Information Officer; or deputy Information Officer

4.5.2. from the website of the Regulator (https://www.justice.gov.za/inforeg/). The Guide can be requested from them in any of South Africa's 11 official languages,

4.6 A copy of the Guide is also available in the following two official languages, for public inspection during normal office hours-

4.6.1 English and Afrikaans

5. CATEGORIES OF RECORDS OF TP WHICH ARE AVAILABLE WITHOUT A PERSON HAVING TO REQUEST ACCESS

Category of records	**Types of the Record**	Available on Website
Corporate Communications	Company Information	X
Policies/Procedures General – Classification 'Public'	Company Codes and Policies	X
Intellectual Property	Legal statements	X
Policies/Procedures General	Ethics hotline	X
Public Filings	Investor relations	X

6. DESCRIPTION OF THE RECORDS OF TP WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION

TP maintains a range of records that are required to be kept or made available in terms of legislation other than the Promotion of Access to Information Act, 2000. Access to these records will be granted only to the extent that the relevant legislation permits or requires such access.

The following categories of records are held in compliance with the statutes listed below legislation is not limited to this list and is reviewed upon changes:

Companies Act 71 of 2008

Statutory company records — Memorandum of Incorporation, registers of directors, shareholders, and company secretaries.

Annual financial statements and related reports.

Resolutions and minutes of shareholders and directors.

Basic Conditions of Employment Act 75 of 1997 (BCEA)

Employee records — employment contracts, attendance registers, remuneration details, leave records, termination records. Health information regarding your health, safety and well being including physical and mental health conditions, related to leave, provided by you and all relevant parties as required or allowed by law. For the purpose of Managing and reporting on sickness absence, occupational health, services, leave, the health, safety and well-being of Workforce Members, disabilities, sickness absence records, accident reporting, notes, occupational health information.

Labour Relations Act 66 of 1995 (LRA)

Disciplinary and grievance records.

Collective agreements and union-related documentation.

Records of consultations (retrenchments, organisational rights, etc.).

Employment Equity Act 55 of 1998 (EEA)

Employment Equity Plans.

EEA Reports and workforce profiles submitted to the Department of Labour.

Skills Development Act 97 of 1998 & Skills Development Levies Act 9 of 1999

Training records.

Workplace Skills Plans (WSPs) and Annual Training Reports (ATRs) submitted to the SETA.

Occupational Health and Safety Act 85 of 1993 (OHSA)

Health and safety incident records.

Risk assessments and safety plans.

Compliance certificates and training records.

Income Tax Act 58 of 1962 & Tax Administration Act 28 of 2011

Tax return supporting documents — PAYE, UIF, SDL, VAT (if applicable).

Payroll tax records.

Financial statements and tax schedules.

Unemployment Insurance Act 63 of 2001

UIF contribution records.

Employee declarations submitted to the UIF.

Immigration Act 13 of 2002

Work permit and visa documentation for foreign employees.

Electronic Communications and Transactions Act 25 of 2002 (ECTA)

Electronic communication records.

Consumer transaction records where applicable.

Protection of Personal Information Act 4 of 2013 (POPIA)

Records of processing activities.

Information Officer documentation.

Data subject request logs.

Sector-Specific or Contractual Compliance Records

(Where applicable to TP's BPO operations)

Client-mandated compliance records (e.g., call recordings, quality assurance logs, service-level documentation).

Information security certifications (ISO/PCI-DSS documentation where required).

Telecommunications regulatory records.

7. DESCRIPTION OF THE SUBJECTS ON WHICH THE BODY HOLDS RECORDS AND CATEGORIES OF RECORDS HELD ON EACH SUBJECT BY TP

Categories of Records	Subjects on which the body holds records	Data Subjects
Administration and Operational support	General Correspondence Planning and Forecasting Policies and Procedures Reference Materials Non Record Reference Materials Clients	Customers Vendors Visitors
Facilities and Security	Maintenance (including inspections) Destruction Investigations CCTV Visitors Access	Customers Vendors Visitors Employees Candidates
Finance and Accounting	Accounting Budgeting Forecasting Payroll Tax	Customers Vendors
Human Resources	Personnel records Benefits Pensions Recruitment Training	Employees Candidates Ex Employees Vendors
Information Technology	System activity System documentation	Employees Vendors
Legal	Contractual Insurance Intellectual Property	Customers Vendors Employees

Categories of Records	Subjects on which the body holds records	Data Subjects
	Litigation Public Filings	
Marketing	Communications Sales	Customers
Procurement	Insurance Purchases and Requisitions Vendors	Customers Vendors Employees

8. PROCESSING OF PERSONAL INFORMATION

Purpose of Processing Personal Information

TP are an outsourcer providing services to our clients, the purpose of processing personal information relates to and is required for the performance of a contract and to comply with legal obligations.

The purposes for which TP South Africa processes personal information includes but is not limited to:

- *Rendering of services to our clients;*
- *Employee administration;*
- *Transacting with our suppliers and third-party service providers;*
- *Maintaining records;*
- *Recruitment;*
- *General administration;*
- *Financial requirements;*
- *Compliance with legal and regulatory requirement*
- *Facilities management*

8.1 Description of the categories of Data Subjects and of the information or categories of information relating thereto

Categories of Data Subjects	Personal Information that may be processed
Employees	BMS number, contact details, physical and postal address, date of birth, age, marital status, race, religion, employment history, criminal/background checks, CVs, education history, banking details, income tax reference number, remuneration and benefit information (including medical aid, pension information), details related to employee

Categories of Data Subjects	Personal Information that may be processed
	performance, disciplinary procedures, employee disability information, employee pension and provident fund information, employee contracts, employee performance records, payroll records, electronic access records, physical access records, CCTV records, health and safety records, training records, employment history, time and attendance records. Health information regarding your health, safety and well being including physical and mental health conditions, related to leave, provided by you and all relevant parties as required or allowed by law. For the purpose of Managing and reporting on sickness absence, occupational health, services, leave, the health, safety and well-being of Workforce Members, disabilities, sickness absence records, accident reporting, notes, occupational health information.
Clients	Client Contact information, entity name, registration details, VAT numbers, Invoicing details
Suppliers and service providers	name, registration number, income tax number, tax information, contact details for representative persons, Due diligence documentation, certificates, invoices, agreements, Insurance details, Contact details, invoicing details, spend information
Visitors	Physical access records, electronic access records and CCTV records
Website visitors	Contact details where relevant
Members of the Public	External CCTV footage

8.2 The recipients or categories of recipients to whom the personal information may be supplied

Recipients or Categories of Recipients to whom the personal information may be supplied	Category of personal information
South African Police Services	Identity number and names, for criminal checks
South African Qualifications Authority	Qualifications, for qualification verifications
Credit Bureaus	Credit and payment history, for credit information
Clients	Employee Information
TP Subsidiaries	Employee Information, Client Customer Information
Recruitment Agencies	Agency agent performance
Service providers	Employee information

8.3 Planned trans-border flows of personal information

TP South Africa may from time to time need to transfer personal information to its group companies, service providers, other third parties located in a country outside of South Africa, including for the purposes of rendering services to clients or for TP South Africa administration purposes (including employee administration).

Where personal information is transferred to or outside of South Africa, TP will take steps to ensure that such transfer is subject to laws, binding corporate rules or binding agreements that provide an adequate level of protection. Transfer risk assessments will be completed where legally required, where sensitive information is transferred or the information is considered high risk

8.4 General description of Information Security Measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information

Information Security Program Overview

TP is committed to improving information security throughout its organization. It has implemented a deliberately layered series of mechanisms and controls to protect the confidentiality, integrity, and availability of its systems, networks, and data whether in-transit or at-rest. Our information security program is a combination of policies, security architecture, classification of information, risk management processes , incident response plans, security

operations, security awareness training, and monitoring security metrics to assess the achievement of our security objectives.

TP's information security program is geared to protecting the entire business ecosystem: clients, customers, and employees

The Global Chief Information Security Officer leads TP's information security team. This team includes security governance, risk management, IT security operations, incident response, security engineering, and cyber security management. The team's training programs and certifications demonstrate our proactive approach to keeping up and aware of current threats and technologies to be able to protect our environment. Moreover, the company's regional CISOs oversee the information security program from both a region and subsidiary level.

TP Enhanced Cyber Security Program

Network Architecture designed to reduce attack surface area ¬White Hat hackers supported by reputed organization¬Multi-layer approach from perimeter to end point including proprietary security technology products¬Established organization-wide security awareness (e.g., anti-phishing)¬Aligned to industry best practices¬End to end detection and response framework



TP is the first company in the industry to comply with the Binding Corporate Rules (BCRs) in the European Union. We have BCR status as a controller and processor.

Our clients can trust us with customer data and be assured of receiving the same level of protection in Europe and any other country where we operate.

Certifications



ISO 27701:2019



ISO 27001:2013



The Payment Card Industry
Data Security Standard

Alignments







Information Security Policies and Standards

Acceptable Use

TP resources should be used for business purposes only. The acceptable use standards describe how these resources (network, system, software, email, internet among others) must be restricted and used. TP management ensures that all members of the workforce are well-informed and adhered to this standard

Media and Information Handling

All forms of information are appropriately managed through data classification labeling, storage, distribution, and disposal. All employees who use TP information processing facilities or handle information must either comply with this policy and/or be aware of relevant local laws. TP uses proven and legally approved cryptography technologies in all IT systems that process, store, or transmit confidential or restricted data. Confidential and restricted data are stored in portable storage devices using cryptographic controls and are decrypted only when necessary and appropriate for business use. Where encryption is used, TP ensures encryption keys are protected by assigning individuals to implement the encryption policy and oversee the generation and management of cryptographic keys. TP has a global record retention and disposition schedule for all TP records and information as well as those of its clients. To ensure confidential data is adequately protected, an annual inventory and assessment is performed, including but not limited to: the identification of any new systems put in place since the last inventory assessment; spot checks on endpoints and databases to ensure no unexpected confidential data exists where it should not be; and a risk and compliance assessment on storage locations. All media containing internal use or higher data classification labels are inventoried annually. A system is in place to ensure that portable storage devices and

other media which contain confidential information are safely and securely disposed.In addition, call center clean desk and clear screen policies are implemented to ensure confidential or restricted data are not visible to unauthorized personnel.

Personnel Management

The purposes of the personnel management standard are to have a formal standard process and requirements as they relate to the life cycle of TP employees, contractors, staffing agencies and vendors. The standard includes all phases of the employment lifecycle including, but not limited to, recruiting, vetting of candidates, confidentiality requirements, security and privacy training, and separation or termination of employment

Physical Security

TP's physical security standards aim to protect onsite personnel, hardware, software, network, data and the facility from threats, loss and/or damage. Physical security standards establish the rules for granting, controlling, monitoring, and removing physical access to TP sites. TP facilities follow a defined security perimeter with appropriate entry controls and security barriers. Delivery and loading areas are controlled and isolated from call center/production areas.Fire exit doors are equipped with an intruder alarm system or monitored by a 24/7 security staff. Access to sensitive information and sensitive information processing areas are controlled and restricted to authorized personnel only. Badges are issued to all personnel for identification and access control purposes. CCTV cameras are strategically located to cover the entire facility and provide 24/7 monitoring

Backups

TP ensures that data, IT systems and other business systems that support our processes are resilient to failure. This standard includes minimum requirements for backup media, scheduling, off-site storage, and media handling to minimize outages and enable acceptable recovery and restoration for business services in case of loss.

Vulnerability Management

Endpoint protection is a vital tool for mitigating attacks against computer hosts and systems. TP has malware protection or endpoint detection and response software to protect against, detect, contain, and remove viruses and other forms of malicious software including worms, spyware, malicious code, and adware. Trained TP staff are available 24/7 to respond to malware alerts. To proactively control risks, TP performs vulnerability scans on both internal and external facing devices and applications on a quarterly basis. Penetration tests are also performed on all in-scope internal and external devices with a remediation process based on the severity of the vulnerabilities discovered.

System and Network

TP system and network infrastructures are designed to run services focusing on confidentiality, integrity, and availability. From acceptance, configuration, hardening, and deployment of systems and network, TP follows a standard secure baseline. The use of these resources is monitored and tuned, and projections made for future capacity requirements, to ensure required system performance. TP follows the OSI model and Zero-Trust framework as part of its network management.

Access Management

Each member of the workforce is provided a unique account that allows them access based on their role or business need. This standard ensures that the provisioning and deprovisioning of user accounts are enforced on both physical and logical access basis. TP conducts a periodic account review and implements a set of minimum password requirements to help prevent unauthorized access.

Logging and Monitoring

Logging events on all computer systems, network devices and appliances are critical for audit purposes and to support forensic investigations on potential or realized breaches. TP requires critical log sources to be stored in a central repository with sufficient information recorded to enable a thorough review of any suspected incidents. In addition, to daily log reviews, TP employs a 24/7 monitoring staff ready to respond to alerts discovered critical at any time.

Secure Data Environment

To protect clients' and customers' confidential and sensitive data, and comply with regulatory requirements such as ISO, HIPAA, PCI DSS and other standards or privacy laws as applicable, TP has defined a set of rules to protect credit card, healthcare, and other sensitive information. These standards detail the configuration and maintenance of secure environments that are storing and processing sensitive data.

Software Development

Secure coding practices for developing web applications and other types of code are critical within TP. There are six phases in TP's development standards taken from OWASP best practices. These phases are design, pre-implementation testing, code review, approval, change control and implementation. TP's developers are required to attend trainings on secure software development at least annually.

Change Management

To ensure all changes made to IT systems (such as the addition, modification or removal of a hardware, software, system, application, or associated process) have minimal or non-

disruptive impact to TP operations and services, a change request process and back-out plan are in place

Business Continuity Management
To minimize disruption during unexpected events that could interrupt business operations, TP requires its regions and subsidiaries to have localized business continuity plans (BCP) aligned with the global BCM program. Each BCP should take into consideration most threats, from extreme weather conditions to terrorism, IT systems failure and staff sickness.

Compliance
It is important that TP' policies and standards comply with legal requirements and regulatory standards, and that all members of the workforce remain in compliance with all internal security and privacy standards. However, in limited situations where compliance may not be possible, TP has an exception process that requires a risk mitigation plan to minimize risks.

Mobile Device Management and Bring Your Own Device
While TP allows the use of personally owned devices for work purposes, with explicit authorization, the company is likewise committed to protecting the privacy, confidentiality and integrity of all information maintained by TP. TP' Mobile Device Management ("MDM") and Bring Your Own Device ("BYOD") standard governs how to appropriately configure corporate or personally owned devices, including smart phones and tablets, for approved business purposes, including access to corporate e-mail and calendaring systems. Authorized personnel must sign a BYOD agreement and follow the application, approval, and registration process in combination with the implementation of technical controls

9. AVAILABILITY OF THE MANUAL

9.1 A copy of the Manual is available-

9.1.1 on www.TP.com

9.1.2 at the head office of TP for public inspection during normal business hours;

9.1.3 to any person upon request and upon the payment of a reasonable prescribed fee; and

9.1.4 to the Information Regulator upon request.

9.2 A fee for a copy of the Manual, as contemplated in annexure B of the Regulations, shall be payable per each A4-size photocopy made.

Access and Reproduction fees respectively

a)	The request fee payable by each requester	R140.00
b)	For every photocopy/printed black and white copy of A4 size page	R2.00 per page or part thereof
c)	For every printed copy of an A4-size page	R2.00 per page or part thereof
d)	For a copy in a computer-readable form on –	
	Flash drive (to be provided by the Requestor)	R40.00
	Compact disc (if provided *by* the Requestor)	R40.00
	Compact disc (if provided *to* the Requestor)	R60.00
e)	For the transcription of visual images, for an A4-size or part thereof	Service to be outsourced. Will depend on the quotation from the service provider
f)	a copy of visual images	
g)	For a transcription of an audio record, or an A4-size page or part thereof	R24,00
h)	For a copy of an audio record on –	
	Flash drive (to be provided by the Requestor)	R40.00
	Compact disc (if provided *by* the Requestor)	R40.00
	Compact disc (if provided *to* the Requestor)	R60.00
i)	To search for and prepare the record for disclosure for each hour or part of an hour, excluding the first hour, reasonably required for such search and preparation.	R145.00
	To not exceed the cost of –	R435.00
j)	Deposit: If search exceeds 6 hours	One third of amount per request calculated in terms of (a) – (f)

k)	Postage, email and any other electronic transfer	Actual expense if any

If the request for access is refused, the Data Protection Officer (Information Officer) shall advise the requester in writing of the refusal, including adequate reasons for the refusal and that the requester may lodge an appeal with a court of competent jurisdiction against the refusal of the request (section 56(3) of PAIA).

Upon the refusal by the Data Protection Officer (Information Officer), any deposit paid by the requester will be refunded.

The requester may lodge an appeal with a court of competent jurisdiction against any process set out in this paragraph 5.

10. FORMS

Access to the latest forms is provided in the link below. If you are unable to access please contact the Administration Officer for further support

https://inforegulator.org.za/paia-forms/

Form 3 can be obtained from - https://www.justice.gov.za/legislation/notices/2021/20210827-gg45057gon757-PAIAregulations.pdf

11. UPDATING OF THE MANUAL

The Information Officer will on a regular basis ensure this manual is updated.

Issued by Justin Stevens

_____

Vice President Compliance