# Data Protection Policy.

**021 866 5557**

**info@payat.co.za**

**www.payat.co.za**

# Policy Information

| | |
|---|---|
| Code: | PP_DPP_002 |
| Version: | 2.1 |
| Date of version: | 2024-10-30 |
| Created by: | Olivia Pienaar |
| Reviewed by: | Nicho Bouma, Marlinda De Klerk, Louise Botha, Thabiso Serake |
| Approved by: | Marlinda De Klerk |
| Confidentiality level: | Company Confidential |
| Review frequency | Annual |

## Change history

| Date | Version | Edited by | Description of change |
|---|---|---|---|
| 2021-04-01 | 1.0 | Olivia Pienaar | Document initiation |
| 2021-06-02 | 1.1 | Olivia Pienaar | Updated transfer of PI outside South Africa in point 7 and updated the reference to Pay@'s process activity mapping instead of Information Asset Register in point 8 below. |
| 2022-09-30 | 2.0 | Olivia Pienaar | Small updates as per POPI Act |
| 2024-09-06 | 2.1 | Louise Botha | Added definitions, elaborated on the personal information definition under point 4,<br>Added to the "Accountability - Condition 1 (7.1.)<br>Made reference to the complaint's procedure under 7.8.1<br>Other small updates. |
| | | | |
| | | | |
| | | | |

# Table of contents

## Definitions and abbreviations

| Word / Phrase / Abbreviation | Definition |
|---|---|
| **POPIA** | No 4 of 2013: Protection of Personal Information Act, 2013. Herein referred to as the Act. |
| **GDPR** | European Union General Data Protection Regulation |
| **ISO 27001** | International Organisation for Standards Information Security Management System (SMS) |
| **ISO 27002** | Code of Practice for ISO 27001 (ISMS |
| **PAIA** | Promotion of Access to Information Act 2 of 2000 |
| **CEO** | Chief Executive Officer |
| **IO** | Information Officer |
| **PI** | Personal Information |
| **IR** | Information Regulator of South Africa (Department of Justice) |
| **DPIA** | Data Protection Impact Assessment |
| **Personal Information** | Means personal information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, exiting juristic person. Refer to point 4 for a detailed definition. |
| **Special Personal Information** | Means religious or Philosophical beliefs, race or ethnic origin, trade union membership, pollical persuasion, health or sex life or biometric information of the data subject. |
| **Child** | Means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him or herself. |
| **Competent person** | Means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child. |
| **Consent** | Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information. |
| **Data Subject** | Means a natural or juristic person to whom personal information relates. |
| **Direct Marketing** | Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: |

| | |
|---|---|
| | a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or<br><br>b) requesting the data subject to make a donation of any kind for any reason. |
| **Electronic communication** | Means any text, voice, sound or image message sent over an electronic communication network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient. |
| **Responsible Party** | The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the organisation is the responsible party. |
| **Operator** | Means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. |
| **Information Officer** | The Information Officer is responsible for ensuring the organisation's compliance with POPIA. |
| **Person** | Means a natural person or a juristic person. |
| **Processing** | Means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information. |
| **Binding corporate rules** | Means PI processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring PI to a responsible party or operator within that same group of undertakings in a foreign country. |
| **Group of undertakings** | Means a controlling undertaking and its controlled undertakings. |

## 1. Purpose, scope and users

The purpose of this Policy is to describe what are Pay@'s data protection rules in compliance with the POPIA requirements.

This document is applied to the entire POPIA scope, i.e. to all Practices as well as to the documentation within the scope.

Users of this Policy are all employees and relevant interested parties associated with Pay@'s handling of PI.

## 2. Reference documents

- POPIA
- PAIA
- GDPR
- ISO 27001

## 3. What is POPIA

POPI as per the Act is *"To promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith."*

## 4. What is Personal Information

Personal information as per the Act is "is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;

- the personal opinions, views or preferences of the person; ▪ correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person;
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person."

## 5. Policy statement

- The Board of Directors and management of Pay@ are committed to compliance with POPIA in respect of PI.
- Compliance with the POPIA is described by this policy and other relevant policies such as the Information Security Policies along with connected processes and procedures.
- The POPIA and this policy apply to all of Pay@'s PI processing functions, including those performed on customers, business partners and employees PI, and any other PI the organisation processes from any source.
- The IO is responsible for reviewing the data register of processing annually in the light of any changes to Pay@'s activities and to any additional requirements. This register needs to be available on the Regulator's request.
- Any breach of the POPIA shall be reported to the IR by the office of the IO and will be dealt with the aim of firstly corrective actions and secondly disciplinary, if required.
- Partners and any third parties working with or for Pay@, and who have or may have access to PI, shall be expected to have read, understood and to comply with this policy. No third party may access PI held by Pay@ without having first entered into an information confidentiality agreement which imposes on the third-party obligations.

## 6. Responsibilities and roles under the POPIA

- Pay@ is the Responsible Party, Operator and Data Subject under the POPIA.
- Top Management and all those in managerial or supervisory roles throughout Pay@ are responsible for developing and encouraging good information handling practices within the organisation.
- The IO is accountable to the Board of Directors of Pay@ for the management of PI within the organisation and for ensuring that compliance with POPIA and good practice are demonstrated. The duties and responsibilities can be found in Pay@'s Information Officer Job Description.
- The Board of Directors of Pay@ is responsible for the management of PI within the organisation and for ensuring that compliance with POPIA and good practice are demonstrated.

- Compliance with POPIA is the responsibility of all employees of Pay@ who process PI. Pay@ ensures training and awareness is provided to all staff who process PI.
- Employees of Pay@ are responsible for ensuring that any PI about them and supplied by them to Pay@ is accurate and up to date.

## 7. PI protection conditions

All processing of PI shall be conducted in accordance with the POPIA conditions and Pay@'s related policies and procedures.

### 7.1. Condition 1: Accountability

- Failing to comply with POPIA could potentially damage the organisation's reputation or expose the organisation to a legal claim or penalties. The protection of personal information is therefore everybody's responsibility.
- Pay@ shall demonstrate compliance with this condition by implementing PI protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as PI protection by design, breach notification procedures and incident response plans.

### 7.2. Condition 2: Processing Limitation

#### 7.2.1. *Lawfulness of processing*

✓ Pay@ shall process PI lawfully and in a reasonable manner that does not infringe the privacy of the data subject by first identifying a lawful basis before processing PI.

#### 7.2.2. *Minimality*

✓ Pay@ shall process PI in line with the business purpose, adequacy, relevance and not excessive.

✓ The IO is accountable for ensuring that Pay@ does not collect information that is not strictly necessary for the purpose for which it is obtained and will ensure that, on an annual basis all PI collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant and not excessive.

#### 7.2.3. *Consent, justification and objection*

✓ Pay@ understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of PI relating to him or her.

✓ The data subject can at any time object to the processing of their PI or withdraw their consent at any time and Pay@ will terminate accordingly.

- ✓ Pay@ understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained. under duress or on the basis of misleading information will not be a valid basis for processing.
- ✓ There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. Pay@ shall demonstrate that consent was obtained for the processing operation.
- ✓ For Special PI, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.
- ✓ Pay@ does not process children's information.
- ✓ In most instances, consent to process personal and special information is obtained routinely by Pay@ using standard consent documents e.g. when a new client signs a contract, or during induction for new staff who are intended to work with PI.

#### 7.2.4. *Collection directly from data subject*

- ✓ Pay@ shall ensure the PI is collected directly from the data subject or the business partners has evidence to demonstrate the same, if the PI was received from them.

### 7.3. Condition 3: Purpose specification

#### 7.3.1. *Collection for specific purpose:*

- ✓ PI obtained for specified purposes shall not be used for a purpose that differs from those recorded in the Privacy Notice.

#### 7.3.2. *Retention and restriction of records*

- ✓ Pay@ shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.
- ✓ The organisation may store PI for longer periods if the PI will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.
- ✓ The retention period for each category of PI will be set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations Pay@ has to retain the data.
- ✓ Pay@'s data retention and data disposal procedures will apply in all cases.
- ✓ PI shall be disposed of securely in accordance with this section of the POPIA. Any disposal of data will be done in accordance with the secure disposal procedure.

## 7.4. Condition 4: Further processing Limitation

### 7.4.1. *Further processing to be compatible with purpose of collection*

- ✓ Pay@ may need to disclose PI to staff who require the PI to perform their duties. These include the organisation's responsible management, human resources, accounting, audit, compliance, information technology, or other personnel.
- ✓ Pay@ may need to disclose PI to its operators as per the privacy notice provided to the data subject.
- ✓ Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.
- ✓ Pay@ shall ensure that PI is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and depending on certain circumstances, the South African Police Service (SAPS). In cases where government bodies request information, please refer to the IO.
- ✓ All Employees shall exercise caution when asked to disclose PI held on another individual to a third-party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Pay@'s business.
- ✓ All requests to provide PI to third party shall be supported by appropriate paperwork and authorised by the IO.

## 7.5. Condition 5: Information Quality

### 7.5.1. *Quality of information*

- ✓ PI that is stored by Pay@ shall be reviewed and updated as necessary. No data shall be kept unless it is reasonable to assume that it is accurate.
- ✓ The IO is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.
- ✓ It is also the responsibility of the data subject to ensure that data held by Pay@ is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.
- ✓ Employees/customers/others shall be required to notify Pay@ of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of Pay@ to ensure that any notification regarding change of circumstances is recorded and acted upon.
- ✓ The IO is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, considering the volume of data collected, the speed with which it might change and any other relevant factors.

- ✓ On at least an annual basis, the IO shall review the retention dates of all the PI. processed by Pay@ on its data inventory and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with the Secure Disposal of Storage Media Procedure.
- ✓ The IO is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If Pay@ decides not to comply with the request, the IO shall respond to the data subject to explain its reasoning and inform them of their right to complain to the IR and seek judicial remedy.
- ✓ The IO is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date PI, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the PI to the third party where this is required.

## 7.6. Condition 6: Openness

### 7.6.1. *Documentation*

- ✓ Pay@ shall maintain all documentation of our processing operations as required by PAIA.

### 7.6.2. *Notification to data subject when collecting PI*

The POPIA includes rules on giving privacy information to data subjects in this section of the act. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information shall be communicated to the data subject in an intelligible form using clear and plain language.

Pay@'s Privacy Notice Procedure is followed and recorded.

The specific information that shall be provided to the data subject, as a minimum, include:

- ✓ The identity and the contact details of Pay@.
- ✓ The contact details of the IO.
- ✓ The purposes of the processing for which the PI are intended as well as the legal basis for the processing.
- ✓ The period for which the personal data will be stored.
- ✓ The existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected.
- ✓ The categories of PI concerned.
- ✓ Where applicable, the recipients or categories of recipients of the PI.

- ✓ Where applicable, that Pay@ intends to transfer PI to a recipient in a third country. and the level of protection afforded to the data.
- ✓ Any further information necessary to guarantee fair processing.

## 7.7. Condition 7: Security Safeguards

Security measures on integrity and confidentiality of personal information

Pay@'s security safeguards (Technical implementations) are aligned with its applicable Information Security Policies based on to the guidelines of the International Information Security Management System standard, ISO/IEC 27002:2022 and the requirements of the POPIA.

Pay@ performs risk assessments on a continuous basis to consider the controls on all the processing operations.

In determining appropriateness, the IO shall also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on Pay@ itself, and any likely reputational damage including the possible loss of customer trust.

### 7.7.1. *When assessing appropriate technical measures, the IO shall consider the following:*

- ✓ Password protection.
- ✓ Automatic locking of idle workstations.
- ✓ Classification, labelling and handling of PI.
- ✓ Limiting the copying of PI by unauthorised staff and removal of access rights for USB's and other media devices.
- ✓ Virus checking software and firewalls.
- ✓ Role-based access rights including those assigned to temporary staff.
- ✓ Encryption of devices that leave the organisations premises such as laptops.
- ✓ Security of local and wide area networks. When assessing appropriate organisational measures, the IO shall consider the following:
- ✓ The appropriate training levels throughout Pay@.
- ✓ Measures that consider the reliability of employees (such as references etc.).
- ✓ The inclusion of PI protection and confidentiality clauses in employment contracts.
- ✓ Identification of disciplinary action measures for PI breaches.
- ✓ Monitoring of staff for compliance with Pay@'s security Policies.
- ✓ Physical access controls to electronic and paper-based records.
- ✓ Adoption of a clear desk clear screen policy.

- ✓ Storing of paper-based PI in lockable cabinets.
- ✓ Restricting the use of employee's own personal devices for business.
- ✓ Adopting clear rules about passwords.
- ✓ Making regular backups of PI.
- ✓ These controls have been selected based on identified risks to PI, and the potential for damage
- ✓ or distress to individuals whose PI is being processed.

#### 7.7.2. *Information processed by Pay@'s operator or person acting under authority of Pay@ shall:*

- ✓ Process such information only with the knowledge or authorisation of Pay@.
- ✓ Treat PI as confidential and shall not disclose it.
- ✓ Any request that falls outside the original purpose of disclosing PI shall be authorised by the IO.

#### 7.7.3. *Security measures regarding information processed by operator*

- ✓ Pay@ shall have written contracts with operators to ensure that the operator processes PI and maintains security safeguards as require by the POPIA.

#### 7.7.4. *Notification of security compromises*

- ✓ The operator shall notify Pay@ immediately where there are reasonable grounds to believe that the PI of a data subject has been accessed or acquired by and unauthorised person.
- ✓ Where there are reasonable grounds to believe that the PI of a data subject has been accessed or acquired by an unauthorised person at Pay@ or its operators, the IO shall notify the IR and data subject.

### 7.8. Condition 8: Data subject participation

#### 7.8.1. *Access to personal information*

- ✓ Data subjects have the following rights regarding data processing, and the data that is recorded about them:
- ✓ To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- ✓ To prevent processing likely to cause damage or distress.
- ✓ To prevent processing for purposes of direct marketing.
- ✓ To be informed about the mechanics of automated decision-taking process. that will significantly affect them.

- ✓ To not have significant decisions that will affect them taken solely by automated process.
- ✓ To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- ✓ To request the IR to assess whether any provision of the POPIA has been contravened.
- ✓ To have PI provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another Responsible Party.
- ✓ To object to any automated profiling that is occurring without consent.

#### 7.8.2. *Pay@ ensures that data subjects may exercise these rights*

- ✓ Data subjects may make data access requests as described in Subject Access Request Procedure. This procedure also describes how Pay@ will ensure that its response to the data access request complies with the requirements of the POPIA.
- ✓ Data subjects have the right to complain to Pay@ related to the processing of their PI, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled.
- ✓ Refer: PP_CPP_008 Complaints Procedure.

#### 7.8.3. *Correction of PI*

- ✓ Data subjects shall be allowed to review, update or delete their PI, only if it was captured on Pay@'s web-based platforms directly by them or provided via email.

#### 7.8.4. *Manner of Access*

- ✓ If the data subject does not have access to his/her PI on Pay@'s system, they, with a proof of Identity, can forward their requests for access to their PI to Pay@'s IO.

## 8. Transfer of PI outside South Africa

Pay@ shall only transfer PI about a DS to a third party who is in a foreign country provided:

- The DS consents to the transfer.
- The third party is subject to a Law, binding corporate rules or binding agreement which provide an adequate level of protection that:
  - Effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of PI relating to a DS who is a natural person and where applicable, a juristic person, and
  - Includes provisions, that are substantially similar to this requirement, relating to the further transfer of PI from the recipient to third parties who are in a foreign country.
- The transfer is necessary for the performance of a contract between the DS and Pay@ or for the implementation of pre-contractual measures taken in response to the DS's request.

- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the DS between Pay@ and the respective third party, or

The transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain such consent of the DS to that transfer and if it were reasonably practicable to obtain such consent, the DS would be likely to give it.

Some of Pay@'s processing facilities shall be hosted in the cloud which may be located inside or outside South Africa. In compliance with POPIA, Pay@ shall, where applicable and possible, ensure the following:

- The notice of the respective hosting is included in the Privacy notice which is shared with the DS during the consent procedure.
- The hosting service provider effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of PI relating to a DS who is a natural person and where applicable, a juristic person.

There are adequate safeguards implemented to protect the confidentiality and integrity of PI in alignment with Pay@'s Cloud security policy.

## 9. Process activity mapping and Risks of particular types of PI

Pay@ shall unpack the details of how Pay@ processes PI by mapping the respective activities to understand the relevant facts; identify who the role players are and discover how Pay@ should go about complying with the conditions of the act. The process shall include but not limited to the documentation of the following activities:

- Business processes that use personal data.
- Source of personal data.
- Volume of data subjects.
- Description of each item of personal data.
- Processing activity.
- Maintains the inventory of data categories of personal data processed.
- Documents the purpose(s) for which each category of personal data is used.
- Recipients, and potential recipients, of the personal data.
- The role of the Pay@ throughout the data flow.
- Key systems and repositories.
- Any data transfers.
- All retention and disposal requirements.

Pay@ is aware of any risks associated with the processing of particular types of PI:

- Pay@ assesses the level of risk to individuals associated with the processing of their PI.

- Pay@ shall manage any risks identified in order to reduce the likelihood of a non-conformance with this policy.
- Where a type of processing, in particular using new technologies and considering the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural and juristic persons, Pay@ shall, prior to the processing, carry out an impact assessment of the envisaged processing operations on the protection of PI.

Where it is clear that Pay@ is about to commence processing of PI that could cause damage and/or distress to the data subjects, the decision as to whether or not Pay@ may proceed shall be escalated for review to the IO.

The IO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the IR.

Appropriate controls shall be selected from either ISO 27001, ISO 27017, ISO 27018, etc., as appropriate and applied to reduce the level of risk associated with processing individual PI to an acceptable level.

Signature
Marlinda de Klerk (CFO)

04 November 2024

Date