Pineapple Tech Proprietary Limited

POPIA Data Breach Policy and Response Plan

Business unit Human Resources

Policy Effective date: 01 August 2023

Affected areas Pineapple Tech PTY LTD employees

TABLE OF CONTENTS

INTRODUCTION

The Pineapple Policy Manual provides the detail of all policies; guidelines; processes and procedures, which support the employer/employee relationship. These documented policies should increase understanding, eliminate subjective decisions and help to ensure consistency and standardization throughout the organization.

The policy is equally applicable to all employees regardless of race, gender, religion, age, sexual orientation, and/or type of marriage. While every effort has been made to keep the descriptions in this manual as clear and accurate as possible, the statements contained in, or omitted from, the manual confer no contractual rights or benefits and are presented for informational purposes only.

While Pineapple Tech Proprietary Limited (the Company) believes wholeheartedly in the policies described here, they are not conditions of employment. As policies change, you may receive notification of these changes so that you always have ready access to the most accurate and up-to-date information. In keeping with our goal of open communication, we encourage you to provide feedback on ways we can improve. If you should have any questions regarding the plans or policies or require additional information, please contact your line manager or the HR manager. We urge each of you to take the time to carefully review and become familiar with the contents of the policy manual and to use it as a guide during your employment with Pineapple.

Scope

PINEAPPLE is a responsible party as defined in the Protection of Personal Information Act 4 of 2013 (POPIA) and is obliged to comply with the provisions of this Act.

Purpose

POPIA requires the Company to inform data subjects (person(s) whose personal information it has access to) as to how Personal Information is used, disclosed, and destroyed.

This Policy sets out how Pineapple deals with their data subjects' Personal Information and additionally for what purpose the said information is used**.**

Background

Personal Information broadly means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly to a specific natural or juristic person (data subject).

Policy

The Company guarantees its commitment to protecting their data subjects' privacy and ensuring their Personal Information is used appropriately, transparently, securely and in accordance with the applicable laws in place.

The POPIA Principles that we subscribe to:

Obtain and process information fairly.

Keep information only for one or more specified, explicit, and lawful purposes.

Use and disclose information only in ways compatible with these purposes.

Keep information safe and secure.

Keep information accurate, complete, and up to date.

Ensure that information is adequate, relevant, and not excessive.

Retain information for record purposes no longer than is necessary for the required purpose in line with the applicable laws in place.

Provide a copy of personal data kept to the data subject on request.

Procedure

Personal Information Collected

The Company will generally collect some of the following personal information from our data subjects:

- Information relating to their gender, sex, marital status, national, age, physical or mental health, well-being, disability, language, and birth.

- Information relating to the education, financial, criminal or employment history.

- Identifying number, name, symbol, e-mail address, physical address, telephone number, location information.

- Correspondence sent/received that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.

We have agreements in place with all of our products suppliers, and third-party service providers to ensure that there is a mutual understanding with regards to the protection of Personal Information.

We may also supplement the information provided with information we receive from other providers to offer a more consistent and personalised experience in clients' interaction with us.

How Personal Information is used

Personal Information will only be used for the purpose for which it was collected and agreed. This may include:

- Providing a product / service to a data subject.
- As part of employee on-boarding or any other internal human resources function.
- Conducting credit reference searches or verification.
- Confirming, verifying, and updating contact details.
- For the detection and prevention of fraud, crime, money laundering or other malpractice.
- For audit and record keeping purposes.
- In connection with legal proceedings.
- Providing our services to a data subject to carry out the services requested and to maintain and constantly improve the relationship.
- Providing communications in respect of Pineapple and regulatory matters that may affect data subjects; and

- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

- To carry out the transaction(s) requested

- For underwriting purposes

- Assessing and processing claims.

- For purposes of claims history.

- Conducting market or customer satisfaction research.

In terms of the provisions of POPIA, Personal Information may only be processed if certain conditions are met, which are listed below, along with supporting information for Pineapple processing for Personal Information:

- **The d**ata subject consents to the processing – consent only required where the information will be used for something other than the intended use for which the information is supplied.

- The processing is necessary.

- Processing complies with an obligation imposed by law on the Company.

- The processing protects the legitimate interest of the data subject.

- The processing is necessary for pursuing the legitimate interest of the Company or of a third party to whom information is supplied.

Disclosure of Personal Information

We may disclose a data subject's Personal Information for a reason it was not intentionally supplied for where we have a duty or a right to disclose in terms of the law or where it may be necessary to protect our rights.

We have agreements in place to ensure that they comply with confidentiality and privacy conditions.

We may also share client Personal Information with and obtain information about clients from third parties for the reasons already discussed above.

Safeguarding Personal Information

It is a requirement of POPIA to adequately protect the Personal Information we hold and to avoid unauthorised access and use of your Personal Information. We will continuously review our security controls and processes to ensure that your personal Information is secure.

When we contract with third parties, we impose appropriate security, privacy, and confidentiality obligations on them to ensure that teir Personal Information is kept secure.

We may need to transfer third parties' (electronic) Personal Information to another country for processing or storage. We will ensure that anyone to whom we pass your personal information agrees to treat your information with a similar level of protection as afforded to you by us.

Access and correction of Personal Information

Data subjects have the right to access the Personal Information we hold about them. Data subjects also have the right to request us to update, correct or delete their Personal Information on reasonable grounds. Once a data subject objects to the processing of their

Personal Information, the Company may no longer process said Personal Information. We will take all reasonable steps to confirm our data subject's identity before providing details of their Personal Information or making changes to their Personal Information. THe Company's Information Officer will be responsible for managing this process.

Data Breach and Response Plan

Notification to the IR

Not all personal data breaches have to be notified to the IR. The breach will only need to be notified if it is likely to result in a risk to the rights and freedoms of data subjects, and this needs to be assessed by the Company on a case-by-case basis. A breach is likely to result in a risk to the rights and freedoms of data subjects if, for example, it could result in:

-loss of control over their data
-limitation of their rights
-discrimination
-identity theft
-fraud
-damage to reputation
-financial loss
-unauthorized reversal of pseudonymisation
-loss of confidentiality
-any other significant economic or social disadvantage.

Where a breach is reportable, the Company must notify the IR without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. If our report is submitted late, it must also set out the reasons for our delay.

The notification must at least include:

-a description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records the name and contact details of the Company's CEO.

-a description of the likely consequences of the breach.

-a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

-Awareness of the breach occurs when one has a reasonable degree of certainty that a breach has occurred. In some cases, it will be relatively clear from the outset that there has been a breach.

-Communication to affected data subjects

Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Company also needs to communicate the breach to the affected data subjects without undue delay, i.e., as soon as possible. In clear and plain language, we must provide them with:

-a description of the nature of the breach

-the name and contact details of the Company's CEO

-a description of the likely consequences of the breach

-a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

TheCompany will also endeavour to provide data subjects with practical advice on how they can themselves limit the damage, e.g., cancelling their credit cards or resetting their passwords.

The Company will contact data subjects individually, by e-mail, unless that would involve the Company in disproportionate effort, such as where their contact details have been lost as a result of the breach or were not known in the first place, in which case we will use a public communication, such as a notification on our website.

However, we do not need to report the breach to data subjects if:

-we have implemented appropriate technical and organisational protection measures, and those measures have been applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access them, such as state-of-the-art encryption, or

-we have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.

Assessing “risk” and “high risk”

In assessing whether a personal data breach results in a risk or high risk to the rights and freedoms of data subjects, the Company will consider the following criteria:

-the type of breach

-the nature, sensitivity and volume of personal data affected

-ease of identification of data subjects – properly encrypted data is unlikely to result in a risk if the

-decryption key was not compromised in the breach

-the severity of the consequences for data subjects

-any special characteristics of the data subject

-the number of affected data subjects
-special characteristics of the Company.

-Data breach register

The Company will maintain a register of all personal data breaches, regardless of whether or not they are notifiable to the IR. The register will include a record of:

-the facts relating to the breach, including the cause of the breach, what happened and what personal data was affected

-the effects of the breach

-the remedial action we have taken.

-Data breach reporting procedure

If you know or suspect that a personal data breach has occurred, you must immediately both advise your line manager and contact the Company's CEO. You must ensure you retain any evidence you have in relation to the breach and you must provide a written statement setting out any relevant information relating to the actual or suspected personal data breach, including:

-your name, department and contact details

-the date of the actual or suspected breach

-the date of your discovery of the actual or suspected breach

-the date of your statement

-a summary of the facts relating to the actual or suspected breach, including the types and amount of personal data involved

-what you believe to be the cause of the actual or suspected breach
-whether the actual or suspected breach is ongoing

-who you believe may be affected by the actual or suspected breach.

You must then follow the further advice of the CEO. You must never attempt to investigate the actual or suspected breach yourself and you must not attempt to notify affected data subjects. The Company will investigate and assess the actual or suspected personal data breach in accordance with the response plan set out below and the data breach team will determine who should be notified and how.

Response plan

The Company's CEO will assemble a team to investigate, manage and respond to the personal data breach. They will lead this team and the other members will consist of nominated senior members of the management team. The data breach team will then:

-Make an urgent preliminary assessment of what data has been lost, why and how.

-Take immediate steps to contain the breach and recover any lost data.

-Undertake a full and detailed assessment of the breach.

-Record the breach in the Company's data breach register.

-Notify the IR where the breach is likely to result in a risk to the rights and freedoms of data subjects.

-Notify affected data subjects where the breach is likely to result in a high risk to their rights and freedoms.

-Respond to the breach by putting in place any further measures to address it and mitigate its possible adverse effects, and to prevent future breaches.

Data breach team	
Data breach team lead:	
Other members of data breach team:	
Background	
Name and department of person notifying actual or suspected breach:	
Date of actual or suspected breach:	
Date of discovery of actual or suspected breach:	
Date of internal notification of actual or suspected breach:	
Preliminary assessment	

Summary of the facts relating to the actual or suspected breach, including the types of personal data involved:	
Categories and approximate number of affected data subjects:	
Categories and approximate number of affected records:	
How sensitive is the personal data? Cause of the actual or suspected breach:	
Any other relevant information or comments:	
Containment and recovery	
Is the actual or suspected breach ongoing?	
What steps can be taken to contain the breach, i.e., to stop or minimise further loss, destruction or unauthorised disclosure?	
What steps can be taken to recover any lost personal data?	
Does the breach need to be reported to the police, for example if there is evidence of theft?	
Does any professional regulator or trade body need to be notified of the breach?	
Does the breach need to be reported to any relevant insurers, e.g., professional indemnity?	
Detailed assessment	
What types of personal data are involved, and does the breach involve any	

special categories of personal data or personal data relating to criminal convictions and offences?	
Who is affected by the breach?	
What are the likely consequences of the breach for affected data subjects?	
Where personal data has been lost or stolen, are any protections in place such as encryption?	
What has happened to the personal data? What uses could a third party make of the personal data?	
Are there any other personal data breaches?	
Has the breach been recorded in the data breach register?	
Any other relevant information or comments: ?	
Notifying the IR	
What is the type of breach?	
What is the nature of the personal data affected?	
What is the potential harm to data subjects?	
What is the sensitivity of the personal data affected?	

What is the volume of personal data affected?	
How easy is it to identify data subjects from the personal data?	
What is the number of affected data subjects?	
Any other relevant information or comments:	
Taking the above into account, is there a legal obligation to notify the IR	
Notifying affected data subjects	
Is there a legal or contractual obligation to notify affected data subjects?	
If there is no legal or contractual obligation, should affected data subjects be notified anyway? Consider whether it will help them to know or whether there is a danger of over-notifying.	
What is the best way to notify affected data subjects?	
Do any data subjects, or categories of data subjects, need to be treated with care because of their special characteristics?	
What additional information should be provided to data subjects about what they can do to limit the damage?	

How should affected data subjects contact the Company for further information or advice and how will we manage such responses?	
How will we keep a record of who has been notified?	
Any other relevant information or comments:	
Is there any legal or contractual requirement to notify any other parties?	
Response	
What security measures were in place when the breach occurred?	
What further measures have been, or are to be, put in place to address the breach and mitigate its possible adverse effects?	
Please also outline the timetable for any measures that have not yet been taken.	
What further technical or organisational measures are to be put in place to prevent the breach happening again?	
Does further staff training on data protection awareness need to be conducted?	
Is it necessary to conduct a privacy risk assessment?	

Any other comments:	
Approval of response plan	
Name:	
Job title:	
Date:	
Signature:	

Information Officer and Deputy Information officer

The details of our Information Officer and Deputy Information Officer are as follows:

Information Officer

Sizwe Ndlovu

Deputy Information Officer

Ndabenhle Junior Ngulube

Both our Information Officer and Deputy Information Officer are contactable at our Head Office:

Telephone Number: +27 76 272 8784 / +27 79 890 0606

Physical Address: 4 Sandown Valley Crescent, Sandown

Email Address: sizwe@pineapple.co.za / ndabenhle@pineapple.co.za

Website: https://www.pineapple.co.za/

Consequences of Non-Adherence

Staff members who do not treat the Personal Information of data subjects with the utmost confidentiality will be subject to disciplinary procedures in place .

Training and Awareness

A copy of this employment policy will be provided to each employee. This policy shall be explained to employees who work with data subjects' personal information.

Review

This policy will be reviewed as and when required and will be kept up to date as the applicable laws change and or are amended accordingly.

Policy Review Dates:

Policy review date	Name of reviewer	Role of reviewer
26 October 2023	Timothy MacKeown	Compliance Manager