Tel: +27 (0)21 976 4930 | Fax: +27 (0)21 976 4909 | Email: info@thembatrans.co.za
Quantico House, Loerie Park, Paul Kruger Street, Durbanville 7550, CAPE TOWN, South Africa
PO Box 3160, Durbanville, 7551, CAPE TOWN, South Africa
www.thembatrans.co.za

DATA BREACH REPORTING PROCEDURE

1. Introduction and Overview

1.1 Themba Trans (Pty) Ltd. (hereinafter referred to as the "Company") is committed to our obligations under the regulatory system and in accordance with the GDPR.

1.2 Every care is taken to protect this personal information from accidental or deliberate misuse, to avoid a data breach that could compromise security and confidentiality.

1.3 However, as the amount of data available grows and technology develops, there are new ways by which data can be breached. We operate a robust and structured system of controls, measures, and processes to help protect data subjects and their personal information from any risks associated with processing information.

2 Purpose

2.1 The purpose of this policy is to provide the Company's intent, objectives and procedures regarding data breaches involving personal information.

2.2 We have a requirement to ensure that the correct procedures, controls and measures are in place and disseminated to all employees, ensuring that they are aware of what the protocols and reporting lines are for personal information breaches.

3. Aim

3.1 The aim of this procedure is to standardize the Company's response to any data breach and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that:

- Incidents are reported swiftly and can be properly investigated.
- Incidents are dealt with in a timely manner and normal operations are restored.
- Incidents are recorded and documented.
- The impact of the incident is understood, and action is taken to prevent further damage.
- The data subjects are informed as required in more serious cases.
- Incidents are reviewed, and lessons learned.

4. Scope

4.1 This policy applies to all persons within the Company (meaning permanent, fixed-term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns, and agents engaged with the Company).

4.2 Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

5. Data security & data breaches

5.1 Article 4 (12) of the General Data Protection Regulation ("GDPR") defines a data breach as: "a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information transmitted, stored or otherwise processed."

5.2 It is important to note that a potential data breach does not always involve technical systems or IT devices. Breaches can also involve paper-based and verbal information.

6. Procedure & guidelines

6.1 Breach monitoring & reporting

6.1.1 The Company has appointed an Information Officer who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact, or containment. All data breaches are reported to this person with immediate effect, whereby the procedures detailed in this policy are followed.

6.1.2 All data breaches will be investigated, even in instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, revision to any such process is recorded.

6.2 Breach incident procedures

6.2.1 Identification of an incident

6.2.1.1 As soon as a data breach has been identified, it is reported to the Information Officer immediately so that breach procedures can be initiated and followed without delay.

6.2.1.2 Reporting incidents in full and with immediate effect is essential to the compliant functioning of the Company. These procedures are for the protection of the Company, its staff, clients, suppliers and third parties, and are of the utmost importance for legal regulatory compliance.

6.2.1.3 As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organization, client, supplier, third-party, system, or data prior to investigation and reporting. The measures taken are noted on the incident record in all cases.

6.2.2 Breach recording

6.2.2.1 The Company utilizes a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder and reviewed against existing records to ascertain patterns or reoccurrences.

6.2.2.2 In cases of data breaches, the Information Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form, and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.

6.2.2.3 A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and record purposes.

6.2.2.4 If applicable, the Information Regulator and the data subject(s) are notified in accordance with the GDPR requirements.

6.3 Breach risk assessment

6.3.1 All data security breaches will be managed according to risk. After the identification of the breach, the risks associated with the breach will be assessed in order to identify an appropriate response.

6.3.2 The investigation will take into account:

- The type of data involved and its sensitivity.
- The protections which are in place.
- What's happened to the data, has it been lost or stolen.
- Whether the data could be put to any illegal or inappropriate use.
- Who the individuals are, the number of individuals involved, and the potential effects on those data subject(s).
- Whether there are wider consequences to the breach.

6.4 Further notification

6.4.1 The Information Officer, Senior Management and/or the IT Management team will determine who needs to be notified of the breach.

6.4.2 Ultimately, the Information Officer will decide whether the Information Regulator should be notified of the breach.

6.4.3 Use of the severity matrix will help determine the risk to people's rights and freedoms, and will aid the decision to notify the Information Regulator (and the data subject(s)).

6.4.4 Every incident will be assessed on a case-by-case basis, considering:

- Whether there are any legal/contractual notification requirements.
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal information?

- Would notification help the Company meet its obligations under the seventh information protection principle?
- The dangers of over notifying. Not every incident warrant notification and over notification may cause disproportionate enquiries and work.

6.4.5 The Information Officer will also consider notifying third parties such as the police, insurers and trade unions. This would be appropriate where illegal activity is known or believed to have occurred, or there is a risk of illegal activity happening in the future.

6.4.6 Notification to the individual(s) whose personal information has been affected by the incident will include a factual description of how and when the breach occurred and the information involved, along with actions taken by the Company.

6.4.7 All decisions and actions will be documented by the Information Officer.

7. Evaluation and response

7.1 Once the initial incident is contained, the Information Officer will carry out a full review of the causes of the breach, the effectiveness of the response and determine whether any changes to systems, policies, or procedures should be made.

7.2 The review will consider:

- Where and how personal information is held and where and how it is stored.
- Where the biggest risks lie and will identify any further potential weak points within its existing measures.
- Whether methods of transmission are secure; sharing minimum amount of information necessary.
- Identifying weak points within existing security measures.
- Staff awareness.
- If deemed necessary, a report recommending any changes to systems, policies, and procedures will be considered by the Company's Senior Management Team.

8. Record keeping

8.1 All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorised by the Information Officer and are retained for a period of six years from the date of the incident.

8.2 Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

9. Disciplinary

9.1 Employees, contractors, visitors, or partner organisations who act in breach of the Company's policy and procedure may be subject to disciplinary procedures or other appropriate sanctions.

ANNEXURE A – DATA INCIDENT REPORTING FORM

Section 1	Details of person reporting the incident
Name	
Job title	
Department	
Date of report	

Section 2	Details of incident
Date and time incident was discovered	
Brief description of event and circumstances – time, date, location, how it occurred, etc.	
Has there been any delay in reporting this? If yes, please explain the reason(s)	Yes / No
Did the incident involve personal information? If no, submit the form now If yes, complete the rest of this section	Yes / No
Describe the type of personal information compromised.	
Was any sensitive information compromised? (eg race, ethnic origin, religious or political beliefs)	Yes / No
Described the type of sensitive personal information compromised.	
Is the breach contained or ongoing?	Yes / No
What steps were/will be taken to contain the breach?	
When was the breach contained?	
If information is lost or stolen, what steps are being taken to recover the information? If recovered, what steps were taken?	

Section 3	Personal information compromised
Number of individuals whose personal information has been compromised	
Types of individual(s) whose information has been compromised – employee, job applicant, client, supplier, etc	
Are the affected individuals aware of the incident?	Yes / No
Have any of the individuals affected complained about the incident?	Yes / No

Section 4	Containment and recovery
Details of any measures in place to prevent an incident like this occurring, e.g. encryption, back-up, training, policy, etc.	
Details of any 3rd party service providers involved in the breach	

Section 5	Assessment of risks
Is the information unique? Can it be restored or is it lost completely? Will its loss have an adverse effect on the Company?	

Section 6	Further notification
Has Senior Management been informed?	Yes / No
Does the Information Regulator require to be informed?	Yes / No
Does the data subject(s) require to be informed?	Yes / No
Do the Police or other regulatory authority need to be informed?	Yes / No

Section 7	Evaluations and response
Description of action taken in response to the incident	
Has the person(s) responsible for or involved in the incident undertaken information protection training?	Yes / No
What steps/actions can be taken to minimise the possibility of a repeat of such an incident?	

Section 8	Overall assessment
Incident reference	
Incident severity (using severity matrix)	
Overall assessment – likely to result in: A – no risk to the data subject B – risk to the data subject C – high risk to the data subject Provide explanation for decision	

ANNEXURE B – MATRIX FOR ASSESSING SEVERITY OF INCIDENT

Data subjects affected

Description	Scenario	Code letter	Risk rating
Very high	1000+	VH	5
High	500 – 999	H	4
Medium	100 – 499	M	3
Low	10 – 99	L	2
Very low	0 - 9	VL	1

Impact

Description	Score	Code letter	Risk rating
Very high	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.)	VH	5
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.)	H	4
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.)	M	3
Low	Individuals may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.)	L	2
Very low	No evidence that individuals will be materially affected	VL	1

Severity

Score = Data subjects affected x impact score

Description	Score	Notify Information Regulator	Notify data subjects
Very high	20+	Yes	Yes
High	16 - 19	Yes	Yes
Medium	11 - 15	Consider	Yes
Low	6 - 10	No	Consider
Very low	0 - 5	No	No

A final decision about notification to the Information Regulator, and whether to inform the data subject(s) will be made by the Information Officer.

ANNEXURE C – DATA BREACH INCIDENT FORM

INFORMATION OFFICER OR INVESTIGATOR DETAILS:	
Name	
Date	
Position	
Time	
Email	

INCIDENT INFORMATION:			
Date or period of breach			
Description & nature of breach			
Type of breach			
Categories of data subjects affected			
Categories of personal information records concerned			
Number of data subjects affected		Number of records involved	
Immediate action taken to contain/mitigate breach			
Employee(s) involved in breach			
Procedures involved in breach			
Third parties involved in breach			

BREACH NOTIFICATIONS:		
Was the Information Regulator notified?	Yes / No	
If no to the above, provide reason(s)		
If applicable, was the below information provided:	Yes	No
A description of the nature of the personal data breach		
The categories and approximate number of data subjects affected		
The categories and approximate number of personal information records concerned		

The name and contact details of the Information Officer and/or any other relevant point of contact		
A description of the likely consequences of the personal data breach		
A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)		
Was notification provide to data subject?	Yes / No	

INVESTIGATION INFORMATION & OUTCOME ACTIONS:	
Details of incident investigation	
Procedure(s) revised due to breach	
Employee training provided	Yes / No
Details of actions taken and investigation outcomes	
Have the mitigating actions prevented the breach from occurring again? (Describe)	
Were appropriate technical protection measures in place?	Yes / No
If yes to the above, describe measures	

Investigator Full Name

Date

Investigator Signature