LITERALLY TAX CONSULTING(Pty) Ltd
2014/036458/07
(Previously: 1989/030876/23)
320/322 Rondebult Rd, Parkdene, Boksburg, 1459
PO Box 9258, Cinda Park, 1463
☎011 892 0286
🖷086 732 0110
www.literallytaxconsulting.com
✉info@literallytc.com

DATA BREACH POLICY

1. Introduction

1.1 This Policy sets out the obligations of Literally Tax Consulting (Pty) Ltd, a company registered in South Africa under number 2014/036458/07, whose registered office is at 71 Black Street Parkdene ("the Company") regarding the handling and reporting of data breaches and personal information breaches in accordance with the Protection of Personal Information Act ("POPIA").

1.2 The Protection of Personal Information Act defines "personal information" as any information relating to an identifiable living natural person or existing juristic person (a "data subject"). A data subject can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.3 For the purposes of this policy, "personal information breach" means the accidental, unlawful or unauthorized access to or acquiring of personal information.

1.4 The Company is under a duty to report personal information breach directly to the Information Regulator's. The Company is also required to inform individual data subjects in the case of breaches.

1.5 All personal information collected, held, and processed by the Company will be handled in accordance with the Company's Personal Information Protection Policy.

1.6 The Company has in place procedures for the detection, investigation, and reporting of data breaches. This Policy applies to all types of data breaches (including personal information breaches) within the Company and is designed to assist in both the handling of such breaches and in determining whether or not they must be reported to the Information Regulator and data subjects.

1.7 The Company's Information Officer and/or appointed Deputy Information Officers, Jacobus J Willemse (011) 892-0286 X228, Charles N Mabokela (011) 892-0286 X203 are responsible for the implementation of this

Policy, for overseeing the handling of all data breaches, and for ensuring that this Policy is adhered to by all staff.

2. Scope of Policy

2.1 This Policy relates to all formats of data (including personal information and special personal information under POPIA, collected, held, and processed by the Company.

2.2 This Policy applies to all staff of the Company, including but not limited to employees, agents, contractors, consultants, temporary staff, casual or agency staff, or other suppliers or personal information processing operators working for or on behalf of the Company.

2.3 This Policy applies to all data breaches, whether suspected or confirmed.

3. Data Breaches

3.1 For the purposes of this Policy, a data breach means any event or action (accidental or deliberate) which presents a threat to the security, integrity, confidentiality, or availability of data.

3.2 Incidents to which this Policy applies may include, but not be limited to:

a) the loss or theft of a physical data record;

b) the loss or theft of computer equipment (e.g. laptop), mobile devices (e.g. smartphone or tablet), portable data storage devices (e.g. USB drive), or other data storage devices;

c) equipment failure;

d) unauthorised access to, use of, or modification of data (or inadequate access controls allowing unauthorised access, use, or modification);

e) unauthorised disclosure of data;

f) human error (e.g., sending data to the wrong recipient);

g) unforeseen circumstances such as fire or flood;

h) hacking, phishing, and other ‘blagging” (tracing) offences whereby information is obtained by deception;

4. Internal Reporting

4.1 If a data breach is discovered or suspected, members of staff should complete a Data Breach Report Form available from HR Office and send the completed form to the Company’s Information Office and/or appointed Deputy Information Officers.

4.2 A completed Data Breach Report Form should include full and accurate details about the incident including, but not limited to (where applicable):

a) the time and date of the breach;

b) the time and date the breach was discovered;

c) the type(s) of data involved;

d) where the breach involves personal information, the categories(s) of data subject to which the personal information relates (e.g. customers, employees etc.);

e) whether or not any special personal information is involved;

f) how many data subjects are likely to be affected (if known);

4.3 Where appropriate, members of staff should liaise with their line Manager when completing a Data Breach Report Form.

4.4 If a data breach occurs or is discovered outside of normal working hours, it should be reported as soon as is reasonably practicable.

4.5 Unless and until instructed to by the Company's Information Officer and/or appointed Deputy Information Officers, members of staff should not take any further action with respect to a data breach. In particular, individual members of staff should not take it upon themselves to notify affected data subjects, the Information Regulator, or any other individuals or organisations.

5. Initial Management and Recording

5.1 Upon receipt of a Data Breach Report Form (or upon being notified of a data breach in any other way), the Company's Information Officer and/or appointed Deputy Information Officers shall begin by determining whether the data breach is still occurring. If this is the case, appropriate steps shall be taken immediately to minimise the effects of the data breach and to stop it.

5.2 Having established the above, the following steps shall then be taken with respect to the data breach:

a) undertake an initial assessment of the data breach, liaising with the relevant staff and departments where appropriate, to establish the severity of the data breach;

b) contain the data breach and, to the extent reasonably practicable, recover, amend, or restrict the availability of (e.g. by changing or revoking access permissions or by temporarily making the data unavailable electronically) the affected data;

c) determine whether anything further can be done to recover the data and/or other losses, and to limit the damage caused by the breach;

d) establish who needs to be notified initially (including, if physical records or equipment have been lost or stolen, the police) as part of the initial containment;

e) determine, in liaison with the relevant staff and departments, the best course of action to resolve and remedy the data breach; and

f) record the breach and the initial steps taken above in the Company's Data Breach Register.

5.3 Having completed the initial steps described above, the Company's Information Officer and/or appointed Deputy Information Officers shall proceed with investigating and assessing the data breach as described in Part 6, below.

6. Investigation and Assessment

6.1 The Company's Information Officer and/or appointed Deputy Information Officers shall begin an investigation of a data breach as soon as is reasonably possible after receiving a Data Breach Report Form (or being notified in any other way) and, in any event, within 24 hours of the data breach being discovered and/or reported.

6.2 Investigations and assessments must take the following into account:

a) the type(s) of data involved (and, in particular, whether the data is personal information or special personal information);

b) the sensitivity of the data (both commercially and personally);

c) what the data breach involved;

d) what organisational and technical measures were in place to protect the data;

e) what might be done with the data as a result of a breach (including unlawful or otherwise inappropriate misuse);

f) where personal information is involved, what that personal information could tell a third party about the data subjects to whom the data relates;

i. the category or categories of data subject to whom any personal information relates;

ii. the number of data subjects (or approximate number if calculating an exact number is not reasonably practicable) likely to be affected by the data breach;

iii. the potential effects on the data subjects involved;

iv. the potential consequences for the Company;

v. the broader consequences of the data breach, both for data subjects and for the Company;

vi. measures that can be taken to prevent similar data breaches.

6.3 The results of the investigation and assessment described above must be recorded in the Company's Data Breach Register.

6.4 Having completed the investigation and assessment described above, the Company's Information Officer and/or appointed Deputy Information Officers shall determine the parties to be notified of the breach as described in Part 7, below.

7. **Notification**

7.1 The Company's Information Officer shall determine whether to notify one or more of the following parties of the breach:

a) affected data subjects;

b) the Information Regulator;

c) the police;

d) the Company's insurers;

e) affected commercial partners.

7.2 When considering whether and how to notify the Information Regulator and individual data subjects in the event of a personal information breach, it must be considered whether such notification will interfere with a criminal investigation. In this regard guidance is to be sought from a public body responsible for the prevention, detection or investigation of offences, relevant to the data breach. Alternatively, it may be determined by the Information Regulator whether notification will impede a criminal investigation by the public body concerned.

7.3 When individual data subjects are to be informed of a data breach, those individuals must be informed of the breach without undue delay. Individuals shall be provided with the following information:

a) a user-friendly description of the data breach, including how and when it occurred, the personal information involved, and the likely consequences;

b) clear and specific advice, where relevant, on the steps individuals can take to protect themselves;

c) a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects;

d) contact details for the Company's Information Officer and/or appointed Deputy Information Officers from whom affected individuals can obtain further information about the data breach.

7.4 If the Information Regulator is to be notified of a breach of personal information within 72 hours, excluding weekends and public holidays, of becoming aware of the breach, where feasible. This time limit applies even if complete details of the data breach are not yet available. The Information Regulator must be provided with the following information:

a) the category or categories and the approximate number of data subjects whose personal information is affected by the data breach;

b) the category or categories and the approximate number of personal information records involved;

c) the name and contact details of the Company's Information Officer from which the Information Regulator can obtain further information about the data breach;

d) a description of the likely consequences of the data breach; and

e) a description of the measures taken (or proposed to be taken) to address the data breach including, where relevant, measures taken to mitigate any possible adverse effects.

7.5 Records must be kept of all data breaches, regardless of whether notification is required to the Information Regulator. The decision-making process surrounding notification should be documented and recorded in the Company's Data Breach Register.

8. Evaluation and Response

8.1 When the steps set out above have been completed, the data breach has been contained, and all necessary parties notified, the Company's Information Officer and appointed deputies, shall conduct a complete review of the causes of the data breach, the effectiveness of the measures taken in response, and whether any systems, policies, or procedures can be changed to prevent data breaches from occurring in the future.

8.2 Such reviews shall, in particular, consider the following with respect to data (and in particular, personal information) collected, held, and processed by the Company:

a) where and how data is held and stored;

b) the current organisational and technical security measures in place to protect data and the risks and possible weaknesses of those measures;

c) the methods of data transmission for both physical and electronic data and whether or not such methods are secure;

d) the level of data sharing that takes place and whether or not that level is necessary;

e) whether any data protection impact assessments need to be conducted or updated;

f) staff awareness and training concerning data protection;

g) whether disciplinary action is to be instituted against any employee whose actions, whether directly or indirectly, resulted in the data breach.

8.3 Where possible improvements and/or other changes are identified, The Company's Information Officer and/or appointed deputies shall liaise with relevant staff and/or departments with respect to the implementation of such improvements and/or changes.

9. **Policy Review and Implementation**

9.1 This Policy will be updated as necessary to reflect current best practice, official guidance, and in line with current legislation.

9.2 This Policy shall be deemed effective as of 1 July 2021. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Mr Anthony James Lubbe
Position:	Chief Executive Officer
Date:	1 July 2021
Due for Review by:	1 July 2022