INVENTUM
FINANCIAL PLANNERS CC
CHARTERED ACCOUNTANTS

Tel: 053 244 0986
navra@inventumfinancial.co.za

Reg nr. CK1995/042779/23
FSB nr. 7139

13 Schmidtsdrift Rd
Rhodesdene
Kimberley
8301

# DATA PRIVACY INCIDENT/BREACH RESPONSE PLAN AND BREACH NOTIFICATION AND REPORTING/COMMUNICATION PROTOCOL

## 1. INTRODUCTION

### 1.1 The Rights of Data Subjects

A data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3 of the POPIA, including the right to be notified that his, her or its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22.

### 1.2 Security Measures regarding Information Processed by Operator

The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

### 1.3 Notification of Security Compromises

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Regulator; and the data subject, unless the identity of such data subject cannot be established.

The notification referred to above, must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection, or investigation of offenses or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

## 2. PROCEDURE TO FOLLOW IN THE EVENT OF SECURITY COMPROMISES – NOTIFYING THE DATA SUBJECT

The notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:

(a) Mailed to the data subject's last known physical or postal address;

(b) sent by e-mail to the data subject's last known e-mail address;

(c) placed in a prominent position on the website of the responsible party;

(d) published in the news media; or

(e) as may be directed by the Regulator.

## 3. CONTENTS OF NOTIFICATION

The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

(a) a description of the possible consequences of the security compromise;

(b) a description of the measures that the responsible party intends to take or has taken to address the security compromise;

(c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

(d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

## 4. DIRECTION BY THE INFORMATION REGULATOR

The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

**PROCESS TO BE FOLLOWED WHEN A BREACH IS IDENTIFIED**

STEP 1: REPORT THE SUSPECTED BREACH TO THE INFORMATION OFFICER

As soon as a breach is suspected, it must be reported to the information officer who will then investigate the suspected breach to determine whether there was in fact a breach.

STEP 2: INVESTIGATE

The information officer must obtain as much information as possible. It may be necessary for the information officer to consult legal, Tech or IT specialists during this step.

- What happened?
- When did it happen?
- Where did it happen?
- Who was involve?
- Who was affected?

STEP 3: IDENTIFY SUSPECTED CAUSE

After the investigation into the breach has been concluded, the cause of the breach must be identified:

- Firewall breach
- Malware
- Phishing
- Outdated antivirus
- Employee misconduct
- Unknowingly/Accidentally divulge personal information
- Any other cause

STEP 4: ISOLATE THE AFFECTED SYSTEM

Ensure that the identified causes or systems are isolated and in order to prevent any further data breaches.

STEP 5: OBTAIN LEGAL ADVICE

The information officer must decide whether it would be necessary to obtain legal advice considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

STEP 6: REPORTING

In terms of Section 22, the breach must be reported, as soon as reasonably possible, to the Information Regulator and the affected data subject(s).

STEP 7: IMPLEMENT POLICIES, PROCEDURES, AND TECHNOLOGY TO PREVENT RECURRENCE OF THE BREACH

Policies, procedures, and technology must be implemented to ensure that the identified breach does not occur in the future; or should the breach recur, it will be identified and addressed as soon as possible to mitigate any harm to the data subjects.

STEP 8: PERFORM RISK ASSESSMENT

The effectiveness of the policies, procedures, and technology must be reviewed on a regular basis and be updated whenever a need occur to do so.