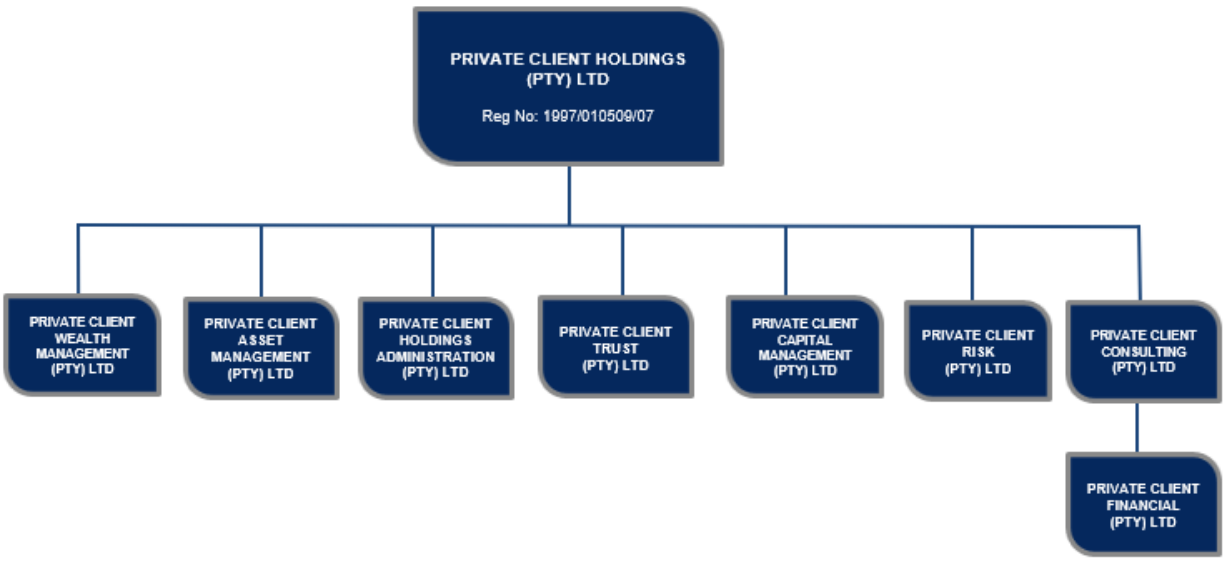
PRIVATE CLIENT HOLDINGS

# POPIA DATA BREACH POLICY



**INTRODUCTION**

The purpose of this policy is to outline the internal breach reporting procedure of Private Client Holdings and its subsidiaries (hereafter "PCH") as outlined on page 1, and our internal and external response plan and it should be read in conjunction with our data protection policy.

Under the Protection of Personal Information Act (POPIA) certain personal data breaches must be notified to the Information Regulator (IR) and affected data subjects need to be told too.

**What constitutes a personal data breach?**
A personal data breach is a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

A breach is therefore a type of security incident and there are three different types of breach that may occur:

1. Confidentiality breach – an accidental or unauthorised disclosure of, or access to, personal data.
2. Availability breach – an accidental or unauthorised loss of access to, or destruction of, personal data.
3. Integrity breach – an accidental or unauthorised alteration of personal data.

A breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these.

A personal data breach would, for example, include:

- Personal data being disclosed to an unauthorised person, e.g. an email containing personal data being sent to the wrong person.
- An unauthorised person accessing personal data, e.g. an employee's personnel file being inappropriately accessed by another member of staff due to a lack of appropriate internal controls.
- a temporary or permanent loss of access to personal data, e.g. where a client's or customer's personal data is unavailable for a certain period of time due to a system shut down, power, hardware or software failure, infection by ransomware or viruses or denial of service attack, where personal data has been deleted either accidentally due to human error or by an unauthorised person or where the decryption key for securely encrypted data has been lost.

**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 PCH 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
- unauthorised reversal of pseudonymisation
- loss of confidentiality
- any other significant economic or social disadvantage.

Where a breach is reportable, PCH's Information Officer must notify the IR without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. If the 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 PCH's Information Officer
- a description of the likely consequences of the breach
- a description of the measures taken, or to be taken, by PCH 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, PCH 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 PCH's Information officer
- 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.

We 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.
We 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, PCH will take into account 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**
PCH 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 were 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 PCH's Information Officer. 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 PCH's Information Officer. You must never attempt to investigate the actual or suspected breach yourself and you must not attempt to notify affected data subjects. The Information Officer 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**

PCH's Information Officer will assemble a team to investigate, manage and respond to the personal data breach. The Information Officer will lead this team and will be supported by the deputy Information Officer.

The data breach team will then:

1. Make an urgent preliminary assessment of what data has been lost, why and how.
2. Take immediate steps to contain the breach and recover any lost data.
3. Undertake a full and detailed assessment of the breach.
4. Record the breach in PCH's data breach register.
5. Notify the IR where the breach is likely to result in a risk to the rights and freedoms of data subjects.
6. Notify affected data subjects where the breach is likely to result in a high risk to their rights and freedoms.
7. 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.