PROTECTION OF PERSONAL INFORMATION ACT (POPI ACT) – DEVELOPMENT OF IMPLEMENTATION AND COMPLIANCE OFFERING PROJECT			
Document:	**BREACH MANAGEMENT CONSIDERATIONS GUIDELINE REFERENCE DOCUMENT**	**Version:**	13.10.20
Purpose:	Guideline considerations relating to addressing data breaches		

1. INTRODUCTION

"South Africa is currently experiencing a high number of data breaches. In the last four months, the Regulator has recorded twenty-five (25) data breaches nineteen (19) of which were self-reported."[1]

Handling data breaches can be extremely time and resource (including cost) intensive. Breaches also have a severe impact on business reputation and trust. Two examples of how the Information Regulator considers data breaches can be accessed in the links below:

- https://www.justice.gov.za/inforeg/docs/ms-20180622-LibertyHoldingsDataBreach.pdf
- https://www.justice.gov.za/inforeg/docs/ms-20200903-ExperianUpdate.pdf

2. DEVELOPING A DATA PRIVACY INCIDENT/BREACH RESPONSE PLAN AND A BREACH NOTIFICATION AND REPORTING/COMMUNICATION (TO AFFECTED PARTIES, THE REGULATOR, CREDIT AGENCIES, LAW ENFORCEMENT) PROTOCOL

Sections 5(a)(ii), 21(2) and 22 of the POPI Act are relevant in this regard and quoted below:

Rights of data subjects
5. *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, including the right—*
(a) to be notified that—
(ii) his, her or its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22;

Security measures regarding information processed by operator
21. *(2) 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.*

Notification of security compromises
22. *(1) 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—*
(a) the Regulator; and
(b) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established

[1] Source: Media statement of the Information Regulator on the Experian security breach – 20 August 2020 [https://www.justice.gov.za/inforeg/docs/ms-20200820-Experian.pdf]

(2) The notification referred to in subsection (1) 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.
(3) 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.
(4) The notification to a data subject referred to in subsection (1) 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.
(5) The notification referred to in subsection (1) 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.
(6) 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.

Section 22 is comprehensive and self-explanatory. The Regulator has however not yet issued Guidelines or templates in this regard, but according to the Regulator's Readiness Plan it will issue the following by 31 March 2021:

"(a) Provide guidance on the manner in which data subjects must be notified of unauthorised access or acquisition of their personal information as provided for in section 22(4)(e);

(b) Provide guidance on the manner in which the responsible party must publicise the fact of any compromise to the integrity or confidentiality of personal information if such compromise would protect a data subject who may be affected by the compromise as provided for in section 22(6)."

An Incident/Breach Response Plan and related communication will be influenced by the above Guidelines and be dependent on the nature and size of each FSP and the nature of the breach. The following considerations can however be shared in this regard, at this stage:

Should a breach occur:

- Notify the Data Subject and regulator in writing as soon as possible.
- Urgently obtain legal advice, if appropriate before the above notification, taking cognisance of section 22(2).
- Do not communicate to / or on (the) media or other parties until advice is obtained on how best to communicate regarding the incident taking cognisance of legal advice obtained.

- Be open and transparent and provide any and all support and cooperation possible to the Data Subject and as may be required by the Regulator.
- Do as much as possible to immediately secure / further secure the Personal Information and to track where the Personal Information could be leaked and take any and all possible further mitigation measures to prevent or limit further leakages or breaches.

More useful tips and considerations in this regard can be accessed in this article: https://digitalguardian.com/blog/data-breach-experts-share-most-important-next-step-you-should-take-after-data-breach-2014-2015.

3. DEVELOPING AND MAINTAINING A LOG TO TRACK DATA PRIVACY INCIDENTS/BREACHES

A mechanism, in any form useful and efficient to the business, to log and track data breaches, should be developed and maintained.

The following elements can be included in the above log:

- Date of Report
- Time of Report
- When did the breach occur (or become known)
- Which staff member was involved in the breach
- Who was the breach reported to
- Notification procedures followed
- Description of Breach
- Initial Containment Activity
- Record what type of data is involved
- Is the data categorised as 'sensitive' or involve children under 18 or account information
- What has happened to the data
- What could the data tell a third party about the individual
- Number of individuals affected by the breach
- Whose data has been breached
- What harm can come to those individuals
- Are there wider consequences to consider e.g. reputational loss
- Action to be taken to recover the data
- Steps needed to prevent the reoccurrence of a breach.

4. INVESTIGATING DATA PRIVACY BREACH INSURANCE COVERAGE

FSPs are obligated by law to have a PI cover and this typically includes cyber liability. Cover to address financial and legal costs and losses as a result of a normal business procedural breach should also be investigated.