NPO Legal Issues

Special Volume:
Aug/Sept 2022

NOTIFYING THE INFORMATION REGULATOR

By Ricardo Wyngaard

About NPO Legal Issues:

This is an electronic newsletter published by:
Ricardo Wyngaard Attorneys
which is aimed at updating the non-profit sector on relevant legal issues.

In this edition:

'NOTIFYING THE INFORMATION REGULATOR'

By: Ricardo Wyngaard

Ricardo Wyngaard Attorneys is a law practice that specialises in rendering advice and assistance on non-profit law and governance.

Subscribe:

To subscribe free of charge send an email with NEWSLETTER typed in the subject-line to:
meagon@nonprofitlawyer.co.za

Details:

Postal:
P.O. Box 35131, Menlo Park, 0102

Tel: +27 21 859 1111
Fax: +27 86 538 8435
ricardo@nonprofitlawyer.co.za

The Protection of Personal Information Act (POPIA) imposes important obligations on Organisations in the event of a data breach involving personal information of a data subject.

Section 22 of POPIA (which should be easy to remember in 2022) compels Organisations to notify the Information Regulator if the Organisation has reasonable grounds to be believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

Notifying the Information Regulator

POPIA provides that the Information Regulator must be notified as soon as reasonably possible after the discovery of the compromise, taking into account permissible factors. POPIA does not define the phrase *accessed or acquired by any unauthorised person*, but is clear that the obligation kicks in even if the personal information of *one data subject* has been accessed by an unauthorised person. This could, for example, include the theft of a cellphone containing the personal information of one of the Organisation's data subjects.

The Information Regulator recently published the prescribed form (***FORM SCN1***: *Notification of a Security Compromise*) that must be completed and submitted in the event of a compromise. The notification includes:

a) The type of security compromise;
b) A description of the incident;
c) The number of data subjects affected;
d) The method of notification to affected data subjects; and
e) The measures the organisation has or intend to take to address the security compromise and the protect personal information from further unauthorised access or use.

The Information Regulator also published **Guidelines** to complete the notification form.

Notifying the Data Subject

The Organisation must also notify the data subject in writing and 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) recommended measures the data subject can take to mitigate the potential negative effects of the security compromise; and
c) the identity of the unauthorised person who may have accessed or acquired the personal information, if known to the organisation.

Organisations should ensure that all board members, staff members, volunteers and independent contractors are aware of the obligation to report security compromises and what steps must be taken to minimise the negative effects of such an incident. The Organisation, in turn, must ensure that the obligations under section 22 are complied with.