INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

S22

GUIDELINES

COMPLETING SECTION 22 SECURITY COMPROMISE NOTIFICATION FORM

PHYSICAL ADDRESS
JD House, 27 Stiemens Street,
Braamfontein,Johannesburg,
South Africa
2001.

POSTAL ADDRESS
PP.O Box 31533,
Braamfontein,
Johannesburg,
2017

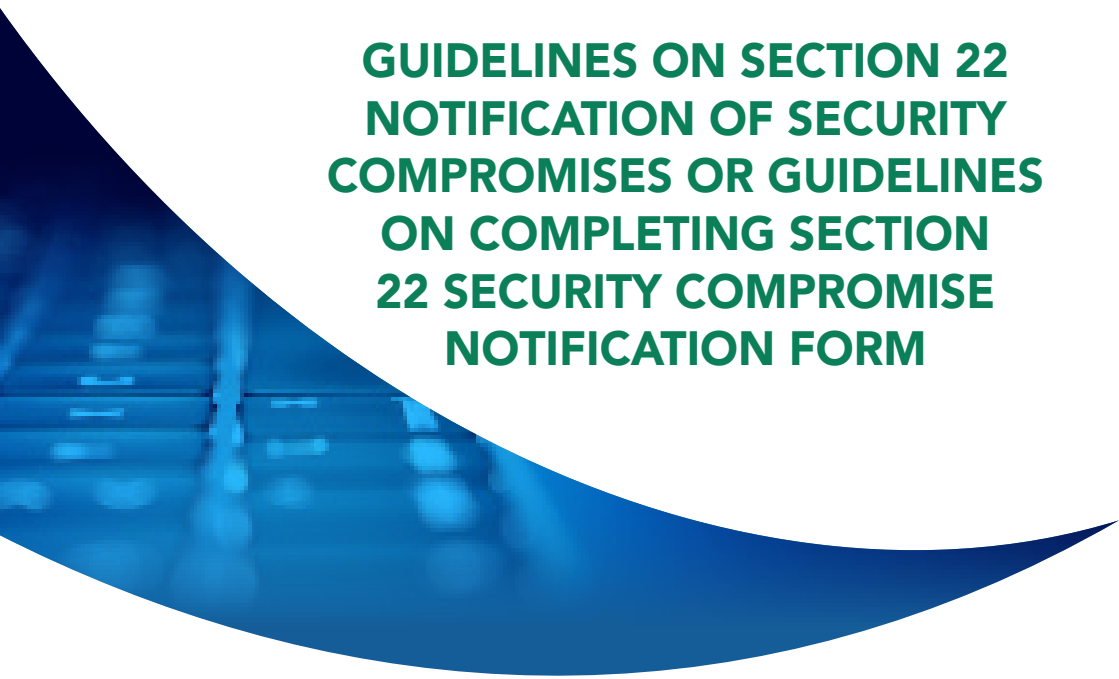
TELEPHONE NUMBER
+27 10 023 5200

EMAIL ADDRESS
enquiries@inforegulator.org.za,

WEBSITE ADDRESS
www.inforegulator.org.za

INFORMATION
REGULATOR
(SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information



GUIDELINES ON SECTION 22 NOTIFICATION OF SECURITY COMPROMISES OR GUIDELINES ON COMPLETING SECTION 22 SECURITY COMPROMISE NOTIFICATION FORM

Guidelines on how the Notification of Security Compromises to the Information Regulator in terms of section 22 of the Proetction of Personal Information Act 4 of 2013 (POPIA) must be completed by Responsible Parties

Introduction

This notification serves as guidance to responsible parties and information officers/deputy information officers on how to complete the Security Compromise Notification Form provided by the Information Regulator (Regulator) in terms of section 22 of POPIA. The use of the form will be effective immediately, upon publication on the Regulator's website. All information officers/deputy information officers will be required to use this pdf fillable Form. Not doing so may result in the notification being regarded as non-compliant.

Process to be followed

1. The responsible party must notify the Regulator of the security compromise as soon as possible after the security compromise occurs using the PDF fillable notification form.

2. Regulator will after registering the notification send an acknowledgement of the notification with a reference number.

3. The notification form is used to collect information about security compromises that occurred under the control of the responsible party and / or of the operator.

4. The responsible party retains the responsibility to report any notification of security compromises as required by section 22 of POPIA.

5. An operator (where applicable) must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of (a) data subject/s has / have been accessed or acquired by any unauthorised person.

6. The responsible party must notify the Regulator and the data subject/s (unless the identity/ties of such data subject cannot be established).

7. The notification must be made as soon as reasonably possible after the discovery of the compromise, unless if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body. The reason for delay of notification to the data subject/s must be included in the notification form.

8. The personal information collected in this notification form (the responsible party's name and contact details) will be handled by the Regulator in accordance with the provisions of POPIA. This information is used to consider and respond to the responsible parties security compromise notification. The Regulator may also use it to contact the responsible party.

Sections of the notification form:

9. **Part A** requires the details of the responsible party.

10. **Part B** requires the details of the information officer unless the details of the information officer are the same as that of the responsible party.

11. **Part C** requires the details of the security compromise in terms of section 22 of POPIA which includes:

a. Notification to the data subject: Details of the security compromise must be provided to the data subject/s to allow them to take protective measures against the potential consequences of the compromise.

b. Date of the security compromise.

c. Date on which the incident was reported to the Regulator.

d. An explanation for delay in notifying the Regulator, if applicable.

e. Type of security compromise.

f. A description of the incident: Should the responsible party / information officer require to add more details about the security compromise, additional information may be provided in a separate annexure.

g. The type of personal information that was unlawfully accessed must be recorded.

h. The number of affected data subjects must be recorded.

i. The method of notification to affected data subjects must be recorded.

j. A description of the possible consequences of the security compromise must be included.

k. A description of the measures that the responsible party intends to take or has taken to address the security compromise must be filled in.

l. A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise must be in the notification.

m. If known, the identity of the unauthorised person who may have accessed or acquired the personal information must be recorded.

12. **Part D** allows a full description of the measures that the responsible party intends to take or has taken to address the security compromise and to protect the personal information of the data subjects from further unauthorised access or use.

13. Should the responsible party / information officer require to add more details about the security compromise, additional information may be provided in a separate annexure.

14. **Part E** is the declaration that the information is accurate, true and correct. This section must be signed by the responsible party / information officer.

End

Ensuring protection of your personal information and effective access to information

PHYSICAL ADDRESS
JD House, 27 Stiemens Street,
Braamfontein,Johannesburg,
South Africa
2001.

EMAIL ADDRESS
enquiries@inforegulator.org.za,

WEBSITE ADDRESS
www.inforegulator.org.za