February 17, 2023

Guidance on reporting of Security Compromises in terms of the POPI Act

In a previous blog, we discussed *the importance of having a data breach incidence response plan within your organisation* to guide you on the correct procedure to follow in the shortest possible time.

Subsequently, during August 2022, the Information Regulator published a prescribed form (the Security Compromise Notification Form, Form SCN1) in terms of section 22 of the Protection of Personal Information Act 2013 (POPIA), together with Guidelines on how to complete it.

In this article, we will discuss the purpose of the Security Compromise Notification Form and the process that should be followed in terms of the accompanying Guidelines.

What is the aim of the Security Compromise Notification (SCN) Form and its Guidelines?

The SCN1 Form and accompanying Guidelines aim to create a mandatory, uniform process to be followed for notifying the Information Regulator of security compromises. Failure to follow this prescribed process may result in the notification being regarded as non-compliant.

The obligation to follow this process is mainly that of the Responsible Party who suffered the security compromise. It is important to note that there is also an obligation on an Operator who suffered a security compromise to notify the Responsible Party immediately where there are reasonable grounds to believe that personal information of a data subject had been accessed by an unauthorised person.

What is the process that should be followed in terms of the Guidelines?

- The Responsible Party must notify the Information Regulator of the security compromise as soon as possible after the incident occurs by completing the prescribed SCN1 Form.
- This form must be emailed to the Regulator at *POPIACompliance@inforegulator.org.za* after which the Information Regulator will register the notification and send an acknowledgement of receipt with a reference number.
- The Responsible Party must also notify the data subject to whom the personal information pertains. This notification must be sent as soon as reasonably possible after detecting the security compromise.

Let's look at the process in more detail.

Notification to the Information Regulator

The SCN1 Form is used to collect information about the security compromise incident that occurred and includes *inter alia*–

- the date and details of the security compromise;
- the date on which the incident was reported to the Regulator;
- an explanation for delay in notifying the Regulator;
- the type of security compromise;
- the type of personal information which was unlawfully accessed;
- the number of affected data subjects;
- the manner in which the affected data subjects were notified; and
- a description of the possible consequences of the security compromise.

Notification to the affected data subjects

Whilst the SCN1 Form is only used to notify the Regulator, it is important that the affected data subject be notified in writing, communicated by way of email or physical mail, or by posting it prominently on the website of the Responsible Party or publishing it in the media. The Regulator may also direct the manner in which the affected data subjects should be notified.

The notification should include enough information to enable the data subjects to take measures to protect themselves against any potential consequences of the security compromise.

In conclusion

Although it is a reality that no one would like to face, it is crucial that the *Information Officers* and Deputy Information Officers of a Responsible Party are aware of the procedure on how to notify the Information Regulator of security compromises in terms of POPIA.

SERR Synergy assists entities to fully comply with procedures as required by the POPI Act by setting up information security management system policies where the physical information and cybersecurity risks of organisations are identified and managed in order to maintain the confidentiality, integrity and legitimate availability of data. Whilst the main focus of POPI is on compliance, our approach at SERR Synergy is to implement information compliance in such a way that it provides business value to our clients and allows for improvement in efficiencies and effectiveness by meeting the compliance requirements.

About the author: Daniele Louw obtained her LLB degree as well as a Post-Graduate Diploma in Financial Planning from the University of the Free State. She also obtained a Certificate in Compliance Management from the University of Cape Town. She is an admitted attorney of the High Court, and after practising at a legal firm for 5 years, she decided to pursue a career in compliance. She joined SERR Synergy in 2021 and currently holds the title of Information Compliance Advisor, specialising in POPI and PAIA compliance.