New way to report security compromises!

All security compromise reports must be submitted via the Information Regulator eServices Portal for a faster, more secure, and POPIA-compliant process.

Fact Sheet on handling of Security Compromises

What is a security compromise?

POPIA does not define a security compromise. In brief, a security compromise, also known as a data breach in other jurisdictions, is a compromise in the security, confidentiality, integrity or availability of personal information, leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, processing or access to personal information. This can lead to harm being suffered by data subjects.

What are some examples of security compromises?

Security compromises can occur in a variety of ways viz.

01 Accidentally

sending an email containing personal information of a data subject to an unintended recipient, losing paperwork or devices which contain unprotected personal information;

02 Deliberately

cyber-security attacks, employee fraud or mischief;

03 Incidentally

theft, rioting, hijacking where personal information is not the target of the activity;

04 Negligently

failing to use appropriate technical and organisational measures to secure personal information such as not using encryption, sharing passwords, leaving personal information unattended.

Do I have to report low risk security compromises?

Yes. POPIA does not have a threshold for reporting of security compromises. All security compromises must be reported by the responsible party irrespective of the deemed level of risk. The reporting requirement is mandatory. Responsible parties do not have a discretion regarding when or if to report a security compromise nor in respect of notifying affected data subjects.

Who should report a security compromise?

The Information Officer or Deputy Information Officer of a responsible party should report the security compromise to both the Information Regulator and to the data subject(s). If a security compromise occurs at an operator of the responsible party, then the operator must notify the responsible party, who in turn must notify the Information Regulator and the data subject(s). However, should a data subject wish to report a security compromise, a complaint should be lodged on a Form 5 and directed to the Complaints & Investigation sub-division.

What is considered a reasonable time within which to report a security compromise?

The responsible party should notify the Regulator and the data subject as soon as it is reasonably sure that a security compromise has occurred. The security compromise does not have to be confirmed before it is reported. Reporting a security compromise as soon as reasonably possible is designed to place the data subject in a position to mitigate against the potential or actual harm that might ensue, as soon as possible. While some delay is allowed for in terms of dealing with law enforcement or stabilising systems, an investigation into a security compromise does not need to be completed before it is reported. If there has been a delay, the responsible party will need to indicate what the reason was for the delay.

What should I do if a security compromise occurs?

1	Identify the security compromise
2	Notify the Information Officer and/or any Deputy Information Officers.
3	Take all necessary measures to mitigate the impact of the security compromise
4	The Information Officer and/or any Deputy Information Officers must notify the data subject in writing of the security compromise. This can be by way of letter, email, notification in the media or on the responsible party's website or any other manner determined by the Regulator.
5	Notify the Regulator by logging the notification via the eServices portal on our website.
6	If you are an operator, you must immediately notify the responsible party of the security compromise.
7	Review your technical and organisational measures to ensure that any weaknesses are addressed.

What if I do not have all the information at hand when notifying the security compromise?

It is advisable to report the security compromise as soon as reasonably practicable based on the information at hand, and then to update the notification as further information comes to light.

What should I write in my notification to the data subject?

The responsible party will need to let the data subject know what has occurred and when, what it plans to do to mitigate against the security compromise, what advice it has for the data subject and where known, who the personal information was exposed to or accessed by. In notifying them of the identity of the unauthorised person, the purpose is to place the data subject in a position where they can guard against any negative impact from the unlawful access to their personal information.

How long should a notice of a security compromise remain on our website?

The determination of how long such notice should remain on your website depends on how likely it is that data subjects will see such notification in the time made available, based on factors such as how often data subjects are likely to visit your website. Thirty to ninety days is a general rule of thumb.

For further information on security compromises, please refer to our FAQs.

INFORMATION REGULATOR (SOUTH AFRICA)

Information Regulator has moved offices.
New address: Woodmead North Office Park, 54 Maxwell Drive Woodmead, Johannesburg 2191, Gauteng Province, South Africa
Tel: +27 10 023 5246 **Toll Free:** +27 80 001 7160
Website: www.inforegulator.org.za