POPIA: WHAT SECURITY COMPROMISES ARE YOU OBLIGED TO REPORT TO THE INFORMATION REGULATOR?

Category: Privacy Law and POPIA,Privacy Law, Infosec, and POPIA,Technology Law
written by Kelly Lekaise | December 1, 2022

The Protection of Personal Information Act 4 of 2013 ("**POPIA**") deals with security compromises and provides guidance on when and how to report them. It also provides some guidance on what constitutes a security compromise. Given the broad definition, there are many situations that will constitute a security compromise. Section 22 of POPIA states that where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the Responsible Party must report this to the Information Regulator, and to the data subject.

POPIA does not define what exactly constitutes a security compromise therefore, it seems section 22

is wide enough to include data breaches from a malicious hacker hacking into your company systems to steal information, to a scenario where a colleague mistakenly views the health information of another employee on a computer. Both are capable of being classified as a security compromise as personal information has been accessed or acquired by an unauthorised person. In light of this, both instances are reportable to the Information Regulator in terms of POPIA.

In contrast, under the General Data Protection Regulation("**GDPR**")[1], organisations are only required to report a data breach (as is referred to under the GDPR) where it is likely that the breach will result in a risk to the rights and freedoms of the data subject.[2] Therefore, when the breach is of such a nature that it poses little to no risk to the rights and freedoms of the data subject, it does not have to be reported. In this regard, the WP29 guidelines on Personal data breach notification under the GDPR recommends that when a breach has occurred, the organisation must undertake a risk assessment that considers:

- the type of breach that occurred – whether this was a confidentiality breach, integrity breach, or availability breach;
- whether sensitive data was breached – this information includes personal information of children, biometrics, racial information, and health information etc;
- the amount of data that was compromised; and
- the number of data subjects that were affected.

Where the breach is likely to be of a high risk to the rights and freedoms of the data subject, this breach must be reported. Where it is determined that the breach is not notifiable, the GDPR requires that the organisation records the breach in a breach register.[3]

The threshold as laid out In the GDPR is not available under POPIA. The consequence of this is that, under POPIA, any kind of unauthorised access to personal information must be reported to the Information Regulator and to the data subject, even where little to no harm may occur. Failure to report a security compromise may attract a hefty penalty from the Information Regulator. We therefore suggest that organisations take their reporting duties seriously and report even the most innocuous security compromises.

Contact us for more good, clear, precise advice.

---

[1] Regulation (EU) 2016/679

[2] Article 33 (1) and 34 (1) GDPR.

[3] Article 33 (5) GDPR.