

26 August 2022

TECHNOLOGY & COMMUNICATIONS

NEWSLETTER

Information Regulator issues data breach notification guidelines and template

In order for responsible parties to comply with their notification obligations under section 22 of the Protection of Personal Information Act (POPIA), the Information Regulator (IR) has published a set of [guidelines](#) along with a prescribed notification [template](#) which is to be used when reporting a data breach to the IR. The template and guidelines can be found on the IR's [website](#).

Should personal information be compromised, such that the notification obligations under section 22 are triggered, the notification template provides for specific information to be furnished to the IR including:

- Details of the responsible party and the Information Officer
- Details of the breach incident, including:
 - The date of the incident;
 - The date that the incident is reported to the IR; and
 - An explanation for any delay in reporting the incident to the IR (if applicable).



INCORPORATING
KIETI LAW LLP, KENYA

- The type of security compromise (e.g. loss, damage, destruction and/or unlawful access or processing of personal information)
- A description of the incident
- The type of personal information compromised
- The number of data subjects affected by the incident
- The method of communication used to notify the affected data subjects
- Status of the compromise (either confirmed or alleged)
- Whether the notification of the data breach to the affected data subjects provides sufficient information to the data subject to allow them to implement measures against the potential consequences of the data breach

Additionally, the template requires responsible parties and information officers to sign the notification form making a declaration that the information presented in the notification is accurate and true.

The guidelines provide an explanation on the use of the notification template and a step-by-step process to be followed when completing and submitting the notification.

The critical question to consider is, would a data breach be notifiable under section 22 of POPIA, with this section providing for the standard to be applied in making this determination. The incident must have

resulted in there being “*reasonable grounds*” for the responsible party to believe that personal information for which it is responsible was either accessed or acquired by an unauthorised person. These terms are not specifically defined under POPIA and therefore their ordinary meanings apply. Whether personal information was accessed or acquired by a person who is ‘unauthorised’ will depend on the specific facts and circumstances of each breach incident.

Data breaches can occur in many ways including unauthorised use of or access to personal information or due to accidental loss, hacking or theft. Data breaches can also occur either by physical or electronic means and includes many instances of negligence or erroneous data processing, such as where an employee accidentally forwards an email which contains personal information to unintended recipients

outside of the organisation who should not receive such data. It would also include breaches which may occur outside of South Africa, but which involve personal information protected under POPIA.

It is also worth emphasising that if a data breach is notifiable under POPIA, then the responsible party is obliged to notify all affected data subjects in accordance with the requirements set out in section 22 of POPIA.

Non-compliance with section 22 is considered an “*interference with the protection of personal information*” under section 73 of POPIA. As a result, this may prompt an investigation by the IR and could ultimately attract penalties or administrative fines.

**PREETA BHAGATTJEE AND
PRESHANTA POONAN**