MEASURES YOUR ORGANISATION CAN TAKE TO COMPLY WITH CONDITION 7 OF POPIA

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Sadia Rizvi | January 26, 2022

As more organisations move towards becoming compliant with the Protection of Personal Information Act ("POPIA"), many organisations are looking for a tailored solution to suit their business needs and to better protect the personal information that they hold. Although condition 7 of POPIA does not stipulate the exact measures that must be taken, it requires that the responsible party must take appropriate and reasonable technical and organisational measures to prevent a loss or compromise of personal information. Some of these reasonable measures may include taking into account the generally accepted information security practices which may apply to the industry or profession in terms of any professional rules or regulations. This has raised the question of what exactly entails generally accepted information security practices.

There are many factors to be considered when a responsible party implements information security measures. The size of the organisation, the amount or type of personal information it holds, cross border flows of data, and the overall cost of the solution will play a role, among other factors, in determining what your organisation requires. For example, if you are a small organisation that handles very little to no personal information, there is no need for your company to implement sophisticated IT measures, or have high tech security equipment. However, if you are a small organisation involved in processing special personal information like health records of many data subjects, you certainly need to have good security safeguards in place.

IT Safeguards

Organisations should ensure that there is a minimum level of IT and technical controls to safeguard their data. For example, implementing multi-factor authentication, access control features, strong passwords, and encrypted network drives are just some of the basic tools one can use to protect their data. For better and further protection, organisations must consider implementing "trusted" and privileged access control features on software, encrypting storage and transmission, firewalls, and security patches. Any security controls used should be kept up to date and reviewed on a regular basis to ensure that any vulnerabilities in the system are addressed. Employees should avoid sending confidential information without encryption in place or using removable storage devices to transfer information. POPIA also states that organisation should not retain records for longer than is necessary.

Physical safeguards

It is sometimes easy to forget that organisations may keep personal information records in the form of hard copies in storage cabinets or filing cabinets in the offices. These physical records also require adequate protection. Filing cabinets should be kept locked and only authorised personnel should be allowed access. Furthermore, it is a good idea to implement a clean desk policy, which requires employees of an organisation to store away paperwork or physical documents and away from the prying eyes of any unauthorised person. Organisations should consider digitising sensitive or confidential records in order to maintain ease of access and prevent any unauthorised access.

Disaster response

In the event of unauthorised access or a security breach, organisations should ensure that a backup plan is provided for and that an appropriate response to the situation is taken. On the IT side, the response plan must ensure that employees have continued access to key systems and data within a reasonable time frame. It is a good idea to maintain an alternate data centre and to annually test the recovery of the organisation's systems. In terms of POPIA, there are additional reporting obligations prescribed, whether it is to the Information Regulator, the data subject, or the responsible party. Data breaches have a huge financial and reputational risk for companies, and it is important to have an appropriate and clear plan of action to minimise the impact of a data breach.

From a risk management perspective, it is important to regularly maintain the security safeguards that have been implemented. This will allow the organisation to identify, prioritise and resolve any new risks that may arise. Considering the number of data breaches and attacks that have been in the media over the past few months, it is a good idea to upgrade your systems and become more involved in safeguarding your organisation's data and to comply with all of the conditions listed in POPIA.

Contact us for more good, clear, precise advice.