COMPLIANCE IS NOT A LEGAL ISSUE: TRUE OR FALSE

Category: Commercial Law,Media and OTT,Privacy Law, Infosec, and POPIA
written by Sasha Beharilal | February 5, 2018

Lawyers interpret legislation and advise accordingly and our advice isn't cheap. We spend hours considering legislation so that we can give you the most precise advice. Most often, we are called in when faeces are propelled in an upward direction. This happens when clients don't follow our advice.

Did you follow our advice? Yes, you say.

But did you really?

Most often, the legal opinion that we have drafted is read by management. Management has no problem understanding their obligations, however our legal opinions aren't made available throughout the organisation. So how has the information been conveyed to staff?

An organisation is made up of every individual that works in the organisation. It is a juristic person and employees are its lifeblood. Considering the critical role that employees play on the success or failure of an organisation, shouldn't they be properly informed on legal and compliance issues? After all, it is their actions that impact whether the organisation is compliant or not.

Take the Protection of Personal Information Act 4 of 2013 ("**POPIA**") for example, there are eight conditions for lawful processing but who is processing vast amounts of information in an organisation? Does the information in the extensive legal opinion, drafted by your lawyers, make its way to every vein of the organisation?

As much as compliance is a legal issue, because you are required to comply with legal rules and regulations, compliance is, at its core, a people issue.

Lets use POPIA as an example. Take condition 7, security safeguards. Section 19 makes provision for security measures on integrity and confidentiality of personal information. This means that an organisation must take appropriate measures to ensure the personal information is safe.

This sounds like an IT issue, and of course you need the appropriate IT infrastructure and security measures like firewalls, anti-viruses and encryption. As a result, management allocates a budget for this and the IT personnel install the reviewed software on the laptops. Legal has drafted a long policy on security and this is given to employees.

But lets look at section 19 closely.

The organisation must

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

Who is responsible for identifying risks?

(b) establish and maintain appropriate safeguards against the risks identified;

Who is responsible for maintaining appropriate safeguards? The IT personnel, with their technical knowledge, are well equipped for this.

(c) regularly verify that the safeguards are effectively implemented; and

Is this an IT issue or a management issue? Is IT required to monitor compliance and ensure that the security software they've installed is being used? Doesn't this sound like a task for a manager?

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

When new risks are identified, the risk department will need to liaise with the IT department.

Is your organisation ready for compliance? Are employees frustrated that they need a new password every month? Do they take it personally that they're not allowed to work off their desktop, do they feel that the organisation is untrusting?

Communicating policies is crucial for compliance. Properly communicated policies lead to good governance which results in improved service delivery. The best way to comply with intimidating legislation is to draft and implement user friendly policies that are in line with the legislation. These policies must be clearly communicated and their purpose clearly defined so that employees understand why it is important. No one, except lawyers maybe, likes to read rules and policies, so find innovate ways to communicate compliance concerns and training on policies.

If employees don't think that the organisation is unnecessarily making life harder by requiring new passwords regularly or discipling them for leaving their laptops unlocked for no reason, then they will happily comply.