A STEP TOWARDS POPIA COMPLIANCE – VENDOR MANAGEMENT

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Melody Musoni | July 7, 2021

In terms of the Protection of Personal Information Act, 4 of 2013 ("**POPIA**"), a Responsible Party must comply with POPIA 8 conditions for lawful processing of personal information. As a business, you may engage the services of other service providers and vendors. If such third parties are processing personal information on behalf of your business, they are called Operators. It is important that you take steps to ensure that your vendors are complying with POPIA.

WHAT DOES POPIA REQUIRE FROM A RESPONSIBLE PARTY?

A Responsible Party is required to have written contracts with its Operators to ensure that the Operators have put in place security measures to safeguard personal information.[1] Security measures can either be technical measures or organisational measures. The type and quantity of personal information that vendors process on your behalf can help in determining the reasonable security measures to have in place. I am sure by now you are either reviewing contracts, drafting contracts addenda or new agreements. If you have not yet started on reviewing your current contracts with vendors, now is the time. Vendor contract management is very important for your business. In addition to setting out the expected security safeguards, you can also share your privacy policies which explains to your vendors the level of POPIA compliance that is expected from them.

It is also important to indicate to vendors that they must immediately notify you where there are reasonable grounds to believe that personal information has been accessed by any unauthorised person.[2] If vendors immediately inform you, it gives you an opportunity to take the necessary action before notifying the Information Regulator.

It may also be helpful for you to conduct vendor due diligence. Due diligence exercises can provide you with insight into the compliance culture of a service provider before you engage their services. If a service provider is not taking POPIA compliance seriously, you may need to look for a different service provider to protect yourself. This is because as a Responsible Party, you will be held liable for non-compliance by your Operators.

Even after you are satisfied with the level of POPIA compliance by your vendors, we would advise you to continuously monitor them. Compliance is an on-going process after all. In practice this can be in the form of requesting the vendor to conduct annual privacy compliance self-assessment to evaluate the processes and controls that they have in place to ensure compliance with POPIA. You could also ask your vendors to furnish you with accepted certifications like certifications on information security. Also, this monitoring depends on the nature of the vendor, the volume and type of personal information they are process on your behalf.

WHAT DOES POPIA REQUIRE FROM OPERATORS?

If you are acting as an Operator, POPIA places an obligation on you to only process personal information under the authorisation of a Responsible Party.[3] For example, if a business has requested you to manage its client database, you must only process such information as per the strict instruction of the business and nothing else. As an Operator, you are required to treat personal information which comes to your knowledge as confidential and must not disclose it, unless if required by law or in the course of the proper performance of their duties.[4] This means that even if there is no non-disclosure agreement in place, you must treat personal information it is processing as confidential.

[1] Section 21 (1) POPIA.

[2] Section 21 (2) POPIA.

[3] Section 20 (a) POPIA.

[4] Section 20 (b) POPIA.