

REGULATORY

ARE YOUR CONTRACTS WITH SUPPLIERS / CONTRACTORS SUFFICIENT TO ENSURE COMPLIANCE WITH POPIA?

4 September 2019 3 min read

By Tebogo Sibidla, Director and Kirsten Whitworth, Senior Associate

In anticipation of the coming into operation of the Protection of Personal Information Act, 2013 ("POPIA"), many companies are making changes to various business processes, systems and documents. Key documents under review include contracts with suppliers, contractors or other persons who process personal information on behalf of these companies ("operators").

Here is a handy checklist of key contractual components that you can use to ensure that your contracts with operators are POPIA compliant and to reduce your risks when outsourcing the processing of personal information to third parties.

1. Reduce the contract to writing and have it signed by all parties.
2. Define key terms and concepts in detail, e.g. "personal information", "special personal information".
3. Clearly identify what personal information the operator is authorized to process, how they can access it, the purpose for their processing it, what the operator may or may not do with it and how long the processor may retain it.
4. Require that the operator ensures that personal information is complete, accurate and up to date, and not misleading.
5. Require that the operator undertake to process personal information only with your express written knowledge or permission, to treat all personal information as confidential and not disclose it unless required by law or authorized by you.
6. Require that the operator undertake to only process personal information in accordance with the contract and to comply with POPIA.
7. Require that the operator ensure that each of its employees, agents, representatives is aware of the operators requirements under POPIA and the contract, and have committed themselves to keeping personal information confidential.
8. State clearly what specific technical, administrative and physical security measures the operator must put in place to protect the personal information from loss or damage, or unauthorized access, processing or destruction, including by when these measures must be in place.
9. State clearly how often the operator must assess, review and update the security measures, and the process the operator must follow before making changes to the agreed security measures.
10. Give yourself the right to audit the operator's security measures, assess and verify that the processing is done in accordance with POPIA and your contract.
11. Prevent the operator from outsourcing processing of personal information to third parties without your written permission.
12. If the operator does outsource the processing of personal information, require that they sign a contract with the third party processor that contains similar requirements on processing of personal information.
13. Require that the operator notify you immediately if it suspects or believes that personal information has been accessed or acquired by unauthorized persons or used in a manner inconsistent with the contract or POPIA, identifying the contact person and details that the operator must use to notify you.
14. Hold the operator liable for any claims against you as a result of their breach of POPIA or the contract.

15. Require that the operator assist you to respond to any queries or requests for access to personal information, and/or requests for the correction, destruction or deletion of personal information.
16. Require that the operator, free of charge, return, delete or destroy personal information in their possession if the contract is cancelled or terminated for whatever reason, and clearly indicate by when operator must do this.



Tebogo Sibidla

Director

[View Profile](#)