CLOUD SERVICES CONTRACTS AND DATA PROTECTION

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Melody Musoni | October 8, 2019

Technology constantly revolves and brings with it new opportunities for economic growth and development. Cloud services are one such technological development that has disrupted how businesses, organisations and private persons manage and store their data. Most people and businesses have migrated data management and IT solutions from the use of USBs, external hard drives, and hardware servers to cloud based services. Cloud based platforms such as Microsoft Azure, Amazon AWS, Dropbox and Google Drive are among the top used cloud services. Where a business decides to adopt a cloud-based service solution to store its information, it is imperative that the business complies with the data protection principles set out in terms of the Protection of Personal Information Act 4 of 2013 (POPIA).

Do you know the location of your data?

One unique feature about cloud computing services is that data may be stored in a cloud that is hosted on a data centre anywhere in the world. It is therefore important before signing that cloud service agreement or service level agreement that you know the location where the data will be hosted. If the data is to be hosted outside South Africa, then the data may be subject to laws of a foreign jurisdiction that you may not be familiar with. This may imply that you may need to consult with legal professionals in that foreign country to establish which foreign laws may be of application to your data hosted on servers in foreign countries.

Do you need to comply with data protection laws?

If the data you store in the cloud contains personal information of your clients, employees, suppliers etc, it is important that you comply with conditions for lawful processing of personal information as set out in POPIA. In addition, where the data centre hosting the cloud services is outside South Africa, then it is expected of a business or organisation as a responsible party to ensure that the POPIA provisions on transborder flow of data have been complied with. Section 72 of POPIA provides that a responsible party is prohibited from transferring personal information about a data subject to a third

party that is in a foreign country unless –

(a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that are substantially like the conditions for the lawful processing of personal information under POPIA and includes provisions that are substantially like those imposed under POPIA data transfer provisions. In the case where the data centre is hosted within the European Union, then it is easier to transfer data into the cloud as the EU has effective data protection laws.

(b) the data subject has consented to the cross-border transfer.

(c) the performance of a contract between the data subject and the responsible party requires the transfer or the transfer is necessary in relation to the implementation of pre-contractual measures to be taken at the data subject's request.

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party.

(e) the transfer is for the benefit of the data subject and where it is not reasonably practicable to obtain the consent of the data subject to the transfer.

In addition, if you are offering goods or services to persons within the European Union or EU citizens and intending to migrate your clients' personal information into a cloud based platform, then you also need to ensure that you also comply with the European Union General Data Protection Regulation (GDPR) data protection principles as well as its principles on transborder transfer of data.

Is your cloud data appropriately secured?

Where you rely on a cloud service provider to store and manage your cloud data (Software as a Service (SaaS)), it is very crucial that your cloud service contract addresses the issues of security. If your cloud data contains personal information, then you must secure the integrity and confidentiality of personal information that is in the cloud by taking appropriate, reasonable technical and organisational measures to prevent the loss of, damage to or unauthorised destruction of personal information and the unlawful access to or processing of personal information. A cloud service provider is generally considered as an operator in terms of POPIA and there is an obligation on the responsible party to ensure that the cloud service provider establishes and maintains these security measures.

Conclusion

If you are running a business and are intending on migrating your data and related personal information into the cloud, you should ensure that you conclude a bespoke cloud services agreement which protects your interests and particularly complies with the data protection laws.

For more good, clear and precise advice, please do not hesitate to contact us.