BIZCOMMUNITY

Why you need to consider PoPI during M&A deals

By Louella Tindale

16 Mar 2021

With the one-year grace period for compliance with the Protection of Personal Information Act (PoPI) ending on 30 June 2021, it's difficult to think about anything outside of your own organisation's compliance (well, at least for us compliance fanatics, that is). However, if you're considering an M&A deal currently or in the future, PoPI should definitely be at top of the list in terms of due diligence and integration.

Before considering the data protection compliance of the target company, you'll need to consider what information you require from the target for due diligence purposes. No doubt you will be requiring data containing personal information of their staff, potentially their suppliers and their customers. This particularly rings true in South Africa, where PoPI applies to personal information of juristic persons (e.g. companies) as well. One can then only hope that the target has included in their privacy notices to relevant data subjects that their information may be shared in the future for merger or corporate restructuring purposes. Updating the privacy notices could alert persons to the proposed transaction and so it is key to ensure that your target's ducks are in a row. It's also important for post-merger integration purposes to make sure that the target's privacy notices make provision for sharing information amongst group entities.

Apart from the usual due diligence aspects on a target, running a PoPI compliance due diligence will become part and parcel of any acquisition going forward. PoPI due diligence investigations should cover, amongst other things, whether the targets' privacy notices are compliant and cover all personal information of all of their data subjects, whether the target has the correct consent mechanisms in place in instances where consent of the data subject is required (e.g. direct marketing via electronic means), whether the target has in place the required contractual measures with operators processing personal information on their behalf, what policies and procedures they have in place regarding document retention and destruction, IT security as well as data breaches.

Further considerations include the technical measures in place to ensure protection of personal information, particularly around security of your target's systems and whether any breaches have previously occurred. Just ask Marriott Hotels, who last year were fined an impressive GBP18.4million by the UK Information Commissioner Office for failing to keep customer data secure. The breach occurred by way of a cyber-attack of Starwood Hotel and Resorts Worldwide in 2014, which was prior to Marriott Hotels acquiring Starwood, but remained undetected until 2018, hence Marriott being fined. Marriott is also now facing a class action lawsuit by individuals affected.

It is clear that when considering an M&A deal, engaging a data protection specialist at the outset - and even prior to the due diligence phase - is paramount.

ABOUT THE AUTHOR

Louella Tindale has a BA LLB (University of Cape Town) as well as a Certificate in Competition Law (University of the Witwatersrand). She was admitted as an attorney in 2010 after completing her articles at Werksmans Attorneys. In 2012, Louella relocated to the United Kingdom where she worked for two multi-nationals as in-house legal counsel - LSE listed hotel group PPHE Hotel Group (Park Plaza and art'otel) and FTSE 100 travel group TUI Travel. Louella joined Caveat Legal in 2017 focusing on data protection work.

Caveat offer a number of bespoke data protection services to businesses, including those entering into mergers or acquisitions, available to view [[https://www.caveatlegal.com/protection-of-personal-information/ here]].