Digital transformation in the financial services sector

By Carla Collett et al.

7 Aug 2020

Data protection and cybercrime are becoming more pressing issues for financial services companies to address from a legal perspective, as Covid-19 accelerates digital transformation.

Before Covid-19 landed on South African soil and forced many citizens into the digital, contactless arena, the financial services industry had already started its digital transformation.

South African consumers are increasingly becoming familiar with contactless payment portals and online lending solutions, chat-bots and robo-advisors and obtaining insurance quotes and entering into insurance policies using their mobile devices. However, the shift from brick and mortar stores to a faceless, digital environment opens the door to a new world of legal and commercial risks and issues.

Data protection

A particular legal consideration which should be front of mind for the financial services industry is data protection. In the insurance industry in particular, this is a requirement in terms of the Policyholder Protection Rules issued under the Long-term Insurance Act, 1998 and the Short-term Insurance Act, 1998, and it is mentioned in Prudential Standard GOI3 and GOI5. South African banks are also subject to the cyber security requirements set out in Guidance Note G4 of 2017 and the cloud computing and offshoring of data requirements set out in Guidance Note G5 of 2018 (read with Directive 3 of 2018) which require them to adhere to certain standards on data protection (among other things).

The Protection of Personal Information Act, 2013 (POPIA) has more general application. Financial services businesses will need to ensure that the way they process personal information is POPIA-compliant by 30 June 2021. This means that those businesses that have created novel fintech and insurtech solutions will need to think carefully about whether those solutions have been designed in such a way that on 1 July 2021 they are not deemed unlawful.

POPIA-related questions to ask

For example, if potential insurance customers enter their details on a mobile device to receive an insurance quote, are they aware of all the purposes for which their personal information will be used? How long is that personal information stored?

What technical and organisational measures are built into the solution, and what does the insurer have in place to prevent any loss of damage to or unauthorised destruction of potential customers' personal information, as well as unlawful access to or processing of their personal information when they enter their details onto a mobile device to obtain an insurance quote? These are just some of the POPIA-related questions to ask to check for POPIA compliance.

Risk of cybercrime

Another significant aspect for financial services businesses to consider when moving into the digital environment is the risk posed by cybercrime. On 1 July 2020, the National Council of Provinces passed the Cybercrimes Bill. Once this Bill becomes effective, financial institutions (as this term is defined in the Financial Sector Regulation Act, 2017) have reporting obligations. In terms of the Cybercrimes Bill, if a financial institution is aware or becomes aware that its computer system (which will extend to its fintech or insurtech platform) is involved in committing any offence set out in Part 1 of Chapter 2 of the Cybercrimes Bill, the financial institution must, without undue delay and where feasible, not later than 72 hours after becoming aware of the offence, report it to the South African Police Service.

From a commercial perspective, there are some key considerations for a bank or insurer to consider when embarking on the journey of rolling out a digital solution. For instance, the decision should be made beforehand whether to engage a third-party software developer or to use in-house software developers. Both options have their pros and cons. Should you choose the former, ensuring that your agreement with your selected service provider is drafted correctly from the outset is imperative to:

- secure your ownership of all of the intellectual property rights in the fintech or insurtech solution, as well as any customisations, modifications, updates and upgrades;
- agree appropriate pricing for the solution;
- ensure that your platform is maintained (if required) with appropriate service levels and possible penalties for non-performance; and
- agree other vital provisions, such as, without limitation, data protection, warranties and indemnities.

ABOUT THE AUTHOR

Carla Collett, partner; Peter Grealy, partner; Nozipho Mngomezulu, partner; Dawid de Villiers, partner; Karl Blom, senior associate; and Wendy Tembedza, senior associate from Webber Wentzel