INFO on Financial Services Sector

POPI challenges for financial services industry

https://www.moonstone.co.za/popi-challenges-for-financial-services-industry/

by **Elizabeth De Stadler** on 21 August 2017

The Protection of Personal Information Act (POPI) applies to all industries, but some industries will be more affected than others. Financial services is one of them. Why? Firstly, FSPs collect very sensitive information. Secondly, when an FSP's security fails, the breach can have dire consequences for customers. Lastly, the Information Regulator has indicated that financial services will be its focus initially, because 85% of the complaints already reported stem from financial services providers.

A real-life example

Want to see a real life example of what can happen when things go wrong at an FSP? Here is an excellent blog about the risk management failures at Wells Fargo, which led to a leak of personal identifiable information of over 50 000 customer records.

However, in my opinion, information security is not the biggest issue for FSPs. Sure, it is important, but it doesn't really change business as usual. There are two issues which will have far larger repercussions:

It will be very difficult post-POPI to buy and sell leads.

The rules about direct marketing is changing.

Buying and selling leads

The practice of buying and selling leads is an established practice in the financial services industry. POPI doesn't make it illegal, but it will be very difficult to do so in future. The main problem is that prospective customers will have to be informed that their information will be shared with third parties. We know, because we tested it, that consumers care deeply about who their information will be shared with and do not trust companies who do share their information.

Direct marketing

The primary reason why businesses purchase leads is to do direct marketing, or 'cold canvassing', as it is also known. POPI contains new rules on direct marketing which will make it compulsory to obtain a person's consent before their details are used for direct marketing. This will definitely apply to sms and e-mail. Whether it applies to telemarketing is unclear. I am of the view that it doesn't, but there are attorneys who disagree with me.

The Information Regulator has indicated to us that this consent will have to be acquired in the form of an 'opt in'. The consent must be voluntary, informed and specific. So, no default consents or statements such us 'by giving us your personal information you consent to us processing it as we deem fit'. It would have to be something like:

'¨ I consent to my information being sold to other FSPs

¨ I consent to direct marketing.'

Not many people who will consent to a company profiting from sharing their personal information. This means that FSPs will have to find ways to convince customers that the buying and selling of their information is in their interest and that they want to receive direct marketing.

Want to read more about this topic? The UK Information Commissioner's Office, who enforces legislation which is very similar to POPI, has written a direct marketing code of conduct. Our Information Regulator is visiting the ICO, so this Code is as close as we can get to a crystal ball.

Training and awareness is a large component of any POPI compliance campaign. Or, in the absence of a campaign, it is a good start. Why? Training raises awareness, exposes risk and changes behaviour.

More so than with many other pieces of legislation, the risks created by POPI can often be cured through small adjustments in behaviour rather than wholesale changes to a business' structure or services.

Digital transformation in the financial services sector

https://www.bizcommunity.com/Article/196/751/207083.html

7 AUG 2020

BY: CARLA COLLETT ET AL.

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.

What about the impact on the insurance industry?

https://www.fanews.co.za/article/front-page-features/25/featured-story/1145/popi-bill-to-significantly-impact-the-financial-services-industry/14263

While there are many people who feel that this legislation is long overdue, its effects will have a significant impact on the insurance industry.

"Companies will need to do significant gap analysis programmes whereby they asses the information that they have already collected and measure it up to whether they comply with the eight areas governed by legislation. You basically need to ask what information you collect, for what purpose the information is being collected, and how the information will be kept. The processing of the information is also a significant area of concern for companies as they will need to get consent from the client in most cases," says De La Harpe.

Companies will also need to be very clear as to what constitutes material information. Material information is the information which is necessary in establishing a policy and its premiums. For example, knowing if a person is a smoker is material when calculating the premiums and exclusion of a life policy. In this instance, a broker or adviser would need to justify why the information is material.

But perhaps the biggest concern is the implementation of systems and processes which are compliant. "Indications are that companies, which have not already started implementing systems and processes which would make them compliant, will take between two to three years to achieve this. This will put them in a tough situation as the act states that companies will only have a year to comply," says De La Harpe.

The legislation will apply to both public and private bodies, including retirement funds and administrators. There will be a transitional period of one year whereafter full compliance with the legislation will be required.

POPIA and financial advisers

https://www.michalsons.com/focus-areas/privacy-and-data-protection/popi-act-training-or-elearning/popi-financial-advisers

The Protection of Personal Information Act (POPI Act) has real significance for the financial and wealth management industry. Financial advisers process a great deal of personal information – the financial history and affairs of their clients, personal information regarding their beneficiaries (often children),

and information regarding their medical health. They also use third parties, such as administrators and other service providers, to process personal information for them.

Securing the integrity and confidentiality of clients' information has always been 'best industry practice'. POPI has made this a legal obligation. Financial advisers need to safeguard their clients' privacy and protect them from identity theft and from their savings and investments being stolen. It is your responsibility to ensure that you (and your administrators and service providers) process personal information lawfully. You also need to ensure that your direct marketing campaigns are compliant with POPI's stricter requirements.

Failure to comply with POPI has serious financial implications (you will get fined). It could also get you imprisoned and irretrievably damage your reputation and the trust clients have placed in you.