Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared

TV Warikandwa*

Online ISSN
1727-3781

P·E·R
Pioneer in peer-reviewed, open access online law publications

Author

Tapiwa Warikandwa

Affiliation

University of Namibia, Namibia

Email

twarikandwa@unam.na

Date Submission

31 October 2020

Date Revised

23 April 2021

Date Accepted

23 April 2021

Date published

21 May 2021

Editor Prof H Chitimira

How to cite this article

Warikandwa TV "Personal Data Security in South Africa's Financial Services Market: The *Protection of Personal Information Act* 4 of 2013 and the European Union General Data Protection Regulation Compared" *PER / PELJ* 2021(24) - DOI http://dx.doi.org/10.17159/1727-3781/2021/v24i0a10727

DOI
http://dx.doi.org/10.17159/1727-3781/2021/v24i0a10727

Abstract

The contemporary global financial services market has witnessed a substantial increase in cybercrime which places consumers' personal data at risk. Rapid increases in cybercrime linked to the financial services market have driven financial market regulators to pass novel laws and regulations aimed at curbing the rate of occurrence of cybercrimes connected to personal data sharing. To that end, banks and/or financial services companies in Europe have swiftly moved to comply with the European Union's *General Data Protection Regulation*. Whilst personal data protection regulation is not a new concept in Europe, most African countries (with exception of South Africa) do not have laws and regulations on personal data protection. With the financial services market being extremely vulnerable to cyber risks owing to the digitisation of the financial services sector, it is important to assess the suitability of South Africa's current regulatory framework concerning the protection of personal data. This article thus examines South Africa's *Protection of Personal Information Act* 4 of 2013 with a view to ascertaining its suitability and/or adequacy in protecting personal data in the country's financial services market. With the global Covid-19 pandemic bringing about concerns related to rapid increases in cyber-attacks in the financial services market owing to the increased sharing of the sensitive personal data of consumers, there is also need to test the POPIA's conformity with the strict European Union GDPR personal data protection guidelines.

Keywords

Financial services market; cybercrime; financial regulators; data protection; *Protection of Personal Information Act* 4 of 2013; European Union *General Data Protection Regulation*.

.....

1 Introduction

Cyber criminals[1] have become significantly aggressive on the financial services markets in the 21st Century.[2] Financial services companies have become primary targets of sophisticated cyber criminals, who have been aided in pursuit of their objectives by technological advances.[3] The technological and business innovations being adopted by contemporary financial services companies to realise growth, modernisation and the effective use of financial resources have increased cyber risks.[4] Technological innovations such as virtual banking and data sharing have introduced new challenges and susceptibilities into their technology ecosystem.[5] Notable examples of the adoption of new technologies in the financial services market include but are not limited to the adoption of Artificial Intelligence (AI), web, social media, cloud, and mobile technologies, all of which have provided cyber criminals with significant opportunities to realise their objectives.[6] Attempts at realising cost-cutting measures by financial services companies characterised by off-shoring, outsourcing and third-party contracting have significantly compromised such financial services companies' ability to control their Information Technology (IT) access points and systems. This has led to the rise of an increasingly unrestricted ecosystem in which financial services companies conduct business, a development which has enlarged the operating space

---

* Tapiwa V Warikandwa. LLB LLM LLD (University of Fort Hare). Senior Lecturer and Head of Department in the Private and Procedural Law Department, Faculty of Law, University of Namibia. Email: twarikandwa@unam.na. ORCID ID: https://orcid.org/0000-0001-5792-5635. This paper was developed from a keynote address which the author presented as one of the Guest Speakers at the North-West University (NWU) Virtual Colloquium on Corporate and Financial Markets Law from 29-30 October 2020.

1 The common types of cyber criminals include but are not limited to internet stalkers, identity thieves, cyber terrorists and phishing scammers. See the Council of Europe's *Convention on Cybercrime* (2001). Also see Norwich University Online 2017 https://online.norwich.edu/academic-programs/resources/who-are-cyber-criminals.

2 Dupont 2019 *J Cybersecur* 1-17. Also see Rathi 2020 https://internationalsecurityjournal.com/cybercrime-and-the-financial-system/; Morgan 2021 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

3 Anon 2020 https://www.securitymagazine.com/articles/93534-six-cybersecurity-threats-the-financial-services-sector-faces. Also see De la Riva 2018 https://www.buguroo.com/en/blog/cybercriminals-in-the-financial-sector-understanding-the-culprits-behind-the-keystrokes.

4 Hernandez de Cos "Financial Technology" 3.

5 OECD 2020 http://www.oecd.org/daf/competition/digital-disruption-in-financial-markets.htm.

6 Biallas and O'Neill 2020 https://www.ifc.org/wps/wcm/connect/448601b9-e2bc-4569-8d48-6527c29165e8/EMCompass-Note-85-AI-Innovation-in-Financial-Services.pdf?MOD=AJPERES&CVID=nfuDUlG. Also see Yoon 2020 *Sustainability* 1-2.

for cyber criminals to exploit financial services institutions.[7] The vulnerability of the financial services market to cybercrime has thus prompted legislators in many countries, including South Africa, to adopt regulatory measures to protect personal data. In particular, South Africa's 1996 Constitution recognises the right to privacy, which is entrenched as a human right.[8] The right is accessible to all South African citizens, including juristic persons.

In recognising that cybercrime and personal data sharing have become matters of concern in South Africa, this article evaluates the *Protection of Personal Information Act* 4 of 2013 (POPIA) to ascertain its suitability and/or adequacy in protecting personal data in the country's financial services market. A comparative analysis will be undertaken with the European Union's *General Data Protection Regulation* (GDPR). Such comparative analysis is necessitated by the fact that should the South African financial services companies not be geared up for compliance with financial services market regulatory conditions for doing business with companies registered in European countries, South Africa is likely to be regarded as a high-risk country in so far as personal data protection is concerned. This is so especially if viewed from the perspective of European companies that aim to be compliant with GDPR.[9] Further, the GDPR is regarded as a considerably far-reaching regulatory advancement in personal data protection.[10] More significantly, the GDPR influences personal data usage globally as it brings personal data into a multifaceted and comprehensive regulatory system. In a cybercrime-ravaged global financial services market, it is imperative to protect personal data because it is "the new oil of the internet and the new currency of the digital world".[11] To protect personal data[12] in the financial services market, the GDPR applies constitutional imperatives which are fundamental and play a key role in the self-conception of an emerging data age political body.[13] Personal data protection in Europe is thus a fundamental objective with Rodota, a member of the drafting team of the *European Union Charter of Fundamental Rights*,[14] explaining that personal data protection is a fundamental right which must be considered like a promise.[15] Such a promise must be

---

7 Baur-Yazbeck, Frickenstein and Medine 2019 https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf.

8 Section 14 of the *Constitution of the Republic of South Africa*, 1996 (the Constitution).

9 Rücker and Kugler *New European General Data Protection Regulation* 1-40; Voigt and Von dem Bussche *EU General Data Protection Regulation*; and FRA *Handbook on European Data Protection Law* 1-10.

10 Hoofnagle, Van der Sloot and ZuiderveenBorgesius 2019 *ICTL* 65.

11 Kuneva 2009 http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm.

12 Fuster *Emergence of Personal Data Protection* 164.

13 Rodotà "Data Protection as Fundamental Human Right" 77.

14 *Charter of Fundamental Rights of the European Union* (2012) 2012/C326/02.

15 Rodotà "Data Protection as Fundamental Human Right" 77-78.

transformed and moved from the physical body to the electronic body. More significantly, Rodota plausibly argues that, "The inviolability of the person must be reconfirmed in the electronic dimension, according to the new attention paid to the respect for the human body …".[16]

2 The vulnerability of the financial services market to cybercrime

The social and technological revolution places emphasis on a need to adopt a different approach to customer service through the utilisation of new tools in a customer-friendly approach.[17] At the centre of realising such an objective is regulating to ensure cyber security for financial services customers' personal data. Unfortunately, the financial services market has prominently featured in the list of twenty-six different business sectors that cyber criminals have regularly attacked.[18] It has remained as an industry that is significantly vulnerable to malicious electronic message trafficking, with consumers seven times more likely to be susceptible to an attack emanating from a hoax email with a bank logo as opposed to one originating from any other business.[19]

Ordinarily, cybersecurity in the financial services market has placed importance on constraining unlawful access to consumers' personal data.[20] However, the nature of cyber threats in the financial services market has developed to the extent where prevention alone is inadequate.[21] Only an estimated 21 per cent of cyber-attacks can be detected at the point of occurrence with an average breach inside a financial services company remaining undetected for an estimated two hundred and twenty-nine days.[22] In the electronic age, the type and manner of security breaches have advanced and become more sophisticated as well as significantly faster than the traditional prevention mechanisms. As such, it is plausible to contend that cybersecurity must now develop to ensure that response and detection mechanisms in financial services companies become quicker, with each member of staff being a vital component of such response and detection mechanisms. The level of change required in financial services

16 Rodotà "Data Protection as Fundamental Human Right" 78.

17 UNCTAD 2018 https://unctad.org/system/files/official-document/tir2018_en.pdf. Also see Lund 2021 https://www.superoffice.com/blog/digital-transformation/.

18 Intel Team 2013 https://www.cyberdisruption.com/?cat=1687.

19 Marketwired 2013 https://www.yahoo.com/news/agari-q3-trustindex-report-financial-120000057.html.

20 Jang-Jaccard and Nepal 2014 *JCSS* 973.

21 Akinbowale, Klingehofer and Zerihun 2020 *JFC* 945. See also Borghard 2018 https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324 and Lagazio, Sherif and Cushman 2020 https://core.ac.uk/download/pdf/20543077.pdf.

22 Sobers 2021 https://www.varonis.com/blog/cybersecurity-statistics/.

companies to curb cyber-crime and realise personal data protection will need numerous players to move outside their comfort zones.

In a 2012 report published by Deloitte Touche Tohmatsu Limited (DTTL) in the aftermath of a study of global financial services executives, it was established that several financial services companies are struggling to realise a level of cyber-risk maturity required to counter the evolving cyber threats which impact on personal data protection.[23] In a 2015 study conducted by PricewaterhouseCoopers (PwC) among seven hundred and fifty-eight financial services respondents, the average number of personal data violation incidents detected rose by 8 per cent in 2014 to a record-breaking four thousand nine hundred and seventy-eight per financial institution in 2015.[24] Notwithstanding this, only 70 per cent of executives from financial companies believed that cyber-security was a strategic risk for their institutions.[25] This is in spite of the fact that banks in the United Kingdom (UK) spent at least seven hundred million pounds per year on cyber-security.[26] The effectiveness of the net spending on cyber-security in the UK needs to be questioned as 88 per cent of cyber-security attacks on financial services companies succeed in a period not exceeding a day, and only 21 per cent are detected in the same time frame.[27] When it comes to cyber security and/or data protection, two types of companies exist; a company that has been hacked, and a company that has been hacked but is unaware that it has been hacked.[28] This worrying fact has led to the realisation that most mechanisms for cyber defence seek to address past and not only present cyber threats.

Regardless of the foregoing, cyber security is still arguably considered as a temporary function and of minor strategic significance in the financial services market. Generally, the concept of cybersecurity as a source of competitive advantage in a world built progressively on more intricate automated systems (including the use of artificial intelligence in the financial services market) is only now emerging as being superficial. Personal data protection is being undermined with financial losses increasing. It is estimated that cyber-crime will cost the global economy an enormous ten

23 DTTL *2012 DTTL Global Financial Services Industry Security Study*.

24 PwC 2014 https://www.pwc.com/na/en/assets/pdf/global-state-of-information-security-survey-2014-key-findings-report.pdf.

25 PwC 2014 https://www.pwc.com/na/en/assets/pdf/global-state-of-information-security-survey-2014-key-findings-report.pdf 11.

26 PwC 2014 https://www.pwc.com/na/en/assets/pdf/global-state-of-information-security-survey-2014-key-findings-report.pdf 14.

27 PwC 2014 https://www.pwc.com/na/en/assets/pdf/global-state-of-information-security-survey-2014-key-findings-report.pdf 22-23.

28 Barnes 2018 https://dynamicbusiness.com.au/topics/technology/there-are-two-types-of-companies-those-who-know-theyve-been-hacked-those-who-dont.html.

and a half trillion United States Dollars annually by 2025.[29] Financial losses incurred from cyber-attacks are as damaging as the probably greater impact on customer and investor confidence, reputational risk and regulatory impact.

3 The contemporary realities regarding cyber threats

The threat posed by cyber attacks and the resultant impact on the financial services market are rising consistently in the world.[30] As a result, financial services sector authorities are increasingly looking for measures aimed at addressing the cyber risk and cybersecurity in South Africa as well.

An estimated 65 per cent of the financial services sector clients have suffered cyber attacks from 2016, more than clients in any other economic sector, a development which marks a 29 per cent increase since 2015.[31] To this end, enhancing the synchronisation between financial services sector authorities and any other agencies dealing with cyber risk and cybersecurity is crucial. The World Bank Group has published two reports to achieve this objective, namely; the Financial Sector's Cybersecurity Regulatory Digest[32] and the Financial Sector's Cybersecurity Regulation and Supervision report.[33]

The reports place significance on the secret data-sharing of cyber incidents among participants in the financial market. To this end, financial market regulators may build up risk and incident classifications and call for compulsory reporting to approximate the actual or probable impact on the continuity of essential services to facilitate data sharing. Some countries request financial companies to develop an Information and Communication Technology (ICT) strategy and risk management framework, added to incident response plans with a clear chain of command to take the

29 Morgan 2021 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

30 Muncaster 2021 https://www.infosecurity-magazine.com/news/financial-services-suffered-covid/.

31 Boer and Vazquez *Cyber Security and Financial Stability*.

32 The Financial Sector's Cybersecurity Regulatory Digest takes stock of prevailing regulatory and supervisory practices, which include cybersecurity laws, regulations, guidelines and other important documents on cybersecurity for the financial sector. See World Bank Group 2019 https://pubdocs.worldbank.org/en/208271558450284768/CybersecDigest-3rd-Edition-May2019.pdf.

33 The Financial Sector's Cybersecurity Regulation and Supervision paper points the establishing of protocols for coordination between financial sector authorities and agencies involved in regulating and supervising cyber-risk. See World Bank Group 2018 https://openknowledge.worldbank.org/handle/10986/11866.

necessary business decisions.[34] Other countries make provision for the appointment of an information security officer.

4 Current challenges

The financial services markets are currently facing challenges brought about by novel payment technologies that have brought about new risks. The basic method of payment for things, the global mobile wallet market, reached an estimated five trillion United States dollars in 2020.[35] At a time when financial services companies are increasingly accepting mobile wallet payment systems and consumers embracing them, the probability of cyber attackers (in particular hackers) targeting fundamental technologies such as Bluetooth or Near Field Communication (NFC) is very high.[36] This scattered payment ecosystem must regulate expectations to presuppose that infringements will occur and hence the need to build security around the data element. The massive generation of data in novel payment ecosystems furthermore presents the foundation of new cyber-security techniques.[37]

4.1 Big data as a fundamental tool in fighting cyber-crime

Those involved in data security are predisposed to consider big data as an appealing combination of prospects and challenges for fighting cyber-crime. Cybercriminals can use data algorithms maliciously or hide in big data. At the same time, a potentially innovative mechanism of managing cybersecurity can be provided by big data processes and tools. Gartner proposes that cybersecurity informed by big data could provide several benefits.[38] Such benefits include reducing false alerts in existing monitoring systems by improving them by using smarter analytics and contextual data, correlating the resultant urgent alerts across monitoring systems to identify trends of abuse and fraud, and reflecting this picture on the security state of the financial services companies. Systems might then pool their in-house data and applicable external data into a single logical platform and establish common patterns of security infringements or fraud.[39] It is assumed that

---

34 Alshubiri, Jamil and Elheddad 2019 *IJEBM* 1-4.

35 GlobeNewswire 2020 https://www.globenewswire.com/news-release/2020/10/26/2114405/0/en/Global-Mobile-Payment-Technology-Market-Will-Reach-USD-5-500-billion-by-2026-Facts-Factors.html.

36 IMF 2020 https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/.

37 European Commission 2020 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en.

38 Gartner 2013 https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf.

39 European Parliament 2020 https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf. Also see Pan *et al* 2015 https://www.cpaaustralia.com.au

data scientists could then continuously scrutinise and compare security data added to unstructured business data to curb the risk of security infringements.

Through accounts profiling, users or other entities, and identifying irregular transactions against those profiles, big data might allow users to stay alert, and remain ahead of actors and activities that are malicious. Eventually, using potent, real-time analytics across multiple structured and unstructured data sets has the potential to enhance operational efficiency and help faster time-to-remediation.[40]

4.2 Improving staffing competency

Being in possession of data analytics infrastructure aimed at adapting to, reacting to and countering cyber threats is immaterial if staff skills in the financial services market are lacking in order to enable them to utilise outputs from these systems. With the skills gap having grown wider, the current projection by most governments in the world is that the present demand for financial services security professionals may be met only in 2030. The skills gap must be addressed due to the fact that a study conducted by International Business Machines Corporations (IBM) pointed out that 95 per cent of financial services security incidents (cyber-security threat) were attributed to human error.[41] In 2014 PwC observed that insiders (present and former employees) were liable for many security incidents with financial firms being reluctant to manage such risks.[42] Forty-four per cent of the financial services respondents in the PwC study regarded current employees as culprits in security incidents, a figure which is 9 per cent higher than in other global business sectors.[43] Most financial services businesses thus do not have an insider-threat programme. It is therefore in this regard that the personal data protection legal framework of South Africa is examined with regard to its viability in data protection in the financial services market.

/~/media/corporate/allfiles/document/professional-resources/business/analytics-and-cybersecurity.pdf.

40 Senousy, El-Khamisy and Riad 2018 *IJCSIS* 39-45. Also see Vasarhelyi and Kogan 2015 *Account Horiz* 381.

41 IBM 2014 https://www.readkong.com/page/ibm-security-services-2014-cyber-security-intelligence-index-6806866.

42 PwC 2014 https://collabra.email/wp-content/uploads/2015/04/2014-us-state-of-cybercrime.pdf.

43 PwC 2014 https://collabra.email/wp-content/uploads/2015/04/2014-us-state-of-cybercrime.pdf.

5 South Africa's personal data regulatory framework

Changes pertaining to the regulation of personal data control have largely been slower than transformation in the security and technology sectors. However, in the South African context the POPIA and the GDPR have provided a basis for regulatory change that is likely to result in progressive data regulation in South Africa, Africa in general, Europe and the rest of the world. This section of the article will analyse the POPIA and its suitability to ensuring personal data protection in the cyber-crime threatened financial services market of South Africa. In today's market, companies are incentivised to capture and process as much data as possible in order to create a competitive advantage. This approach to business more often than not is prejudicial to consumers. Giving financial services companies unfettered powers to collect personal data may potentially lead to invasive advertising, identity theft and fraud. It is in this regard that the POPIA assumes significance. The POPIA was introduced to ensure the protection of the constitutional right to privacy through the implementation of rules designed to protect private information such as the personal data of financial services consumers. Prior to the introduction of the POPIA, South Africa had no regulation pertaining to how businesses could capture and use the personal data of clients. However, section 14 of the *Constitution of the Republic of South Africa* provides that "Everyone has the right to privacy, which includes the right not to have: a) their person or home searched; b) their property searched; c) their possessions seized; and d) the privacy of their communications infringed". In order to realise the constitutional imperative set out in section 14 of the Constitution, South Africa initially passed the *Electronic Communications and Transactions Act* 25 of 2002 (ECTA). The ECTA regulated the electronic collection of personal information.[44] However, compliance with the ECTA was voluntary.[45] The protection of personal data was expressly dealt with in Chapter VIII of the ECTA, dealing with "Protection of Personal Information". Section 50 of the Act provided for the scope of protection of personal information,[46] while section 51 provided for principles of electronically collecting personal information.[47] Nevertheless, the provisions of the ECTA pertaining to the protection of personal information have been repealed by the POPIA.

---

44 Section 10-11 of the *Electronic Communications and Transactions Act* 25 of 2002 (the ECTA).

45 Section 35 of the ECTA.

46 Section 50(1) of the ECTA provided that Ch VIII applied specifically to personal information obtained through electronic transactions.

47 See s 51(1)-(9) of the ECTA. Key amongst these provisions is the fact that in terms of s 51(1) a data controller should have the express written permission of the data subject for "the collection, collation, processing or disclosure of any personal

The POPIA has a more extensive scope of application and impact than the ECTA. On 26 November 2013 the POPIA was promulgated into law. At the time not all provisions of the POPIA came into effect. Instead, in April 2014 specific sections of the POPIA came into effect. Such provisions related to the definitions section of the POPIA,[48] the provisions dealing with the establishment of the office of the Information Regulator as well as its powers, duties and functions,[49] and the sections pertaining to the procedure for making regulations.[50] The definitions[51] and purpose sections[52] (Chapter 1 of the POPIA) came into effect on 11 April 2014. In October 2016, office bearers of the Information Regulator were officially appointed with effect from 1 December 2016, for a period of five years.

Most of the operative provisions of the POPIA came into effect through the POPIA Commencement Proclamation of 22 June 2020.[53] Therefore, on 1 July 2020 a number of provisions of the POPIA came into force. Chapter 2 dealing with the applications provisions is also now operative. It includes the following provisions: the specific application and interpretation provisions;[54] descriptions of the conditions for the lawful processing of personal information;[55] descriptions of data subjects' rights;[56] and exclusions from the scope of the POPIA, describing those circumstances under which the POPIA does not apply to the processing of personal information.[57] Chapter 3 of the POPIA provides for conditions for the lawful processing of personal information. Such conditions must be complied with by reasonable parties when processing personal information.[58] The POPIA defines personal information as any information that can be used to identify a living person, such as race and gender; contact details; financial details; medical history; employment and criminal history; and educational history. A further classification is provided with regard to personal information. This relates to what is called special personal information. This refers to information that can be used to discriminate against someone. Such information includes the following: criminal history, race and ethnicity, biometric information, medical history, and trade union membership.

---

information on that data subject unless he or she is permitted or required to do so by law".

48 Chapter 1, s 1 of the *Protection of Personal Information Act* 4 of 2013 (POPIA).

49 Section 39 of POPIA.

50 Section 113 of POPIA.

51 Section 1 of POPIA.

52 Section 2 of POPIA.

53 Proc R21 in GG 43461 of 22 June 2020.

54 Section 3 of POPIA.

55 Section 4 of POPIA.

56 Section 5 of POPIA.

57 Sections 6 and 7 of POPIA.

58 Sections 8-35 of POPIA.

Chapter 4 of the POPIA sets out the exemptions from the conditions for the lawful processing of personal information which, if applicable, exempts a responsible party from information processing that is in breach of the conditions for the lawful processing of personal information.[59] The POPIA defines data processing as:

> ... any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –
>
> (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
>
> (b) dissemination by means of transmission or making available in any other form; or
>
> (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

The POPIA covers all forms of personal information, both digital and physical. Such data can be in the form of contact details in a database or a piece of paper with their contact details written down. In principle the POPIA covers matters pertaining to the handling of personal information in either digital or physical formats.

The POPIA further provides for the establishment of the Information Regulator.[60] The Information Regulator works with information officers[61] and is tasked with issuing codes of conduct regarding the collection and processing of personal information.[62] The Information Regulator is also tasked with granting prior authorisation to responsible parties to undertake planned processing activities.[63] Provisions are also made for setting out requirements pertaining to direct marketing, directories, and automated decision making.[64] Furthermore, the POPIA also makes provision for transborder information flows.[65] Administrative fines, offences and penalties are provided for in terms of section 100-109 of the POPIA. Sections 100-106 of the POPIA deal with instances in which parties would be regarded as being guilty of an offence. Such instances include but are not limited to the following: any person who hinders, obstructs or unlawfully influences the Information Regulator; a responsible party which fails to comply with an enforcement notice; offences by witnesses, such as lying under oath or failing to attend hearings; unlawful acts by a responsible party in connection

59 Sections 36-38 of POPIA.
60 Sections 39-54 of POPIA. Sections 39-54 of POPIA came into effect in April 2014.
61 Sections 55-56 of POPIA.
62 Sections 60-68 of POPIA.
63 Sections 57-59 of POPIA.
64 Sections 69-71 of POPIA.
65 Section 72 of POPIA.

with account numbers; and unlawful acts by third parties in connection with account numbers.

Section 107 of the POPIA details penalties which apply to specific offences. Ten million Rands or imprisonment for a period not exceeding ten years or both a fine and such imprisonment will be imposed for serious offences. For less serious offences such as hindering an official in executing a search and seizure warrant, a penalty of twelve months' imprisonment or both a fine and such imprisonment will be imposed. The POPIA thus makes provision for the protection of data by responsible parties as follows: entrenching the rights of data subjects, including the right of data subjects to be notified that the data subjects' personal information has been accessed by an authorised person; and placing an obligation on responsible parties to secure the integrity and confidentiality of personal information by taking appropriate, reasonable technical and organisational measures to prevent unlawful access to it. Section 111 then provides for the prescribed fees payable by data subjects to responsible parties in selected circumstances.

However, because the unlawful access of personal information extends to cybercrime and requires legal recourse should there be cyber-attack, there is a need to augment the POPIA with a law that addresses cybercrime and cyber-security. Due to the fact that South Africa's cybercrime laws are not yet up to speed with those in foreign law, the *Cybercrimes and Cybersecurity Bill* [B6-2017] has been tabled before parliament and is just a few steps away from being passed into law. The *Cybercrimes and Cybersecurity Bill* criminalises the following types of crimes: unlawful access;[66] unlawful interception of data;[67] unlawful acts in respect of software and hardware tools;[68] unlawful interference with data, computer

66 Section 2 of the *Cybercrimes and Cybersecurity Bill* [B6-2017]. Unlawful access includes the unlawful and intentional access to data, a computer programme, a computer data storage medium or a computer system (hacking).

67 Section 3 of the *Cybercrimes and Cybersecurity Bill* [B6-2017]. Unlawful interception of data includes the acquisition, viewing, capturing or copying of data of a non-public nature through the use of hardware or software tools.

68 Section 4 of the *Cybercrimes and Cybersecurity Bill* [B6-2017]. This section provides that the unlawful and intentional use or possession of software and hardware tools that are used in the commission of cybercrimes (ie hacking and unlawful interception) is illegal.

programmes, storage mediums and computer systems;[69] cyber fraud;[70] cyber forgery;[71] cyber uttering;[72] and malicious communications.[73]

The *Cybercrimes and Cybersecurity Bill* will create structures such as nodal points and Cybersecurity Hub and Point of Contacts which will be open for 24 hours every day of the week. The Point of Contact will give responsible authorities the ability to investigate offences in terms of the Bill expeditiously. Nodal points reporting cyber incidents, receiving information about cyber incidents from the Cybersecurity Hub and receiving and disseminating information about cyber security incidents will have to be established.

The POPIA and the *Cybercrimes and Cybersecurity Bill* (should it be passed into law) both confer power on the South African Police Services to investigate, search and access or seize any article used in the commission of an offence, and create mechanisms for mutual assistance between foreign states in cross-border investigations. This is done in order to bring South Africa's legislative framework pertaining to data protection and privacy in line with foreign law guidelines such as the GDPR. This approach establishes the minimum requirements for the processing and protection of personal information, thereby promoting the right to privacy enshrined in section 14 of the South African Constitution.

It is important to point out that aside from the POPIA, data privacy must also be considered from the perspective of consumer protection law. In this regard, the *Consumer Protection Act* 68 of 2008 (CPA), which was enacted in 2011, applies to matters pertaining to direct marketing and unsolicited communications. This will depend, however, on whether or not the CPA is applicable to a particular case where the relevant provisions of the POPIA also are applicable.

---

69 Sections 5-7 of the *Cybercrimes and Cybersecurity Bill* [B6-2017]. This section makes reference to the unlawful and intentional interference with data, a computer programme, a computer data storage medium or a computer system.

70 Section 8 of the *Cybercrimes and Cybersecurity Bill* [B6-2017]. This section refers to fraud committed by means of data or a computer programme or through any interference with data, a computer programme, a computer data storage medium or a computer system.

71 Section 9 of the *Cybercrimes and Cybersecurity Bill* [B6-2017]. This section refers to the creation of false data or a false computer programme with the intention to defraud.

72 Section 9 of the *Cybercrimes and Cybersecurity Bill* [B6-2017]. This refers to the passing-off of false data or a false computer programme with the intention to defraud.

73 Sections 10-11 of the *Cybercrimes and Cybersecurity Bill* [B6-2017]. This refers to the distribution of data messages with the intention to incite the causing of damage to any property belonging to, or to incite violence against, or to threaten a person or group or persons.

The next section of this article discusses the GDPR with a view to ascertaining the compliance of South Africa's data protection laws to foreign law standards. As stated in the introduction to this article, the comparative analysis is necessitated by the fact that should South African financial services companies not be geared up for compliance with financial services market regulatory conditions for doing business with companies registered in European countries, South Africa is likely to be regarded as a high-risk country in so far as personal data protection is concerned. This is so especially if viewed from the perspective of European companies that aim to be compliant with the GDPR.

6 The European Commission's general data protection regulation

The GDPR[74] came into effect in 2018.[75] It replaced the *Data Protection Directive* 95/46/EC (DPD) as the primary law regulating European Union registered companies' protection of personal data.[76] To that end, companies that were in compliance with the DPD had to ensure compliance with the GDPR, failing which, stiff penalties and fines would be imposed.[77] The GDPR requirements are applicable to companies registered in all member states of the European Union (EU).[78] The reason behind this blanket approach is that a consistent consumer and personal data protection regulatory framework would be realised across the EU.

The most important requirements for data protection in the GDPR are as follows: consent from subjects for data processing;[79] collected data anonymising to protect privacy; the provision of data breach notifications;

---

74 *General Data Protection Regulation* (EU) 2016/679 (27 April 2016) (the GDPR).

75 Article 99(2) of the GDPR.

76 Rücker and Kugler *New European General Data Protection Regulation* 1-40; Voigt and Von dem Bussche *EU General Data Protection Regulation*; FRA *Handbook on European Data Protection Law* 10.

77 The Data Protection Directive sets out the following grounds for data processing: 1) the data subject has consented to the data processing; 2) the data processing is necessary for a contract with the data subject; 3) there is a law mandating the data processing (for example tax law requires companies to keep certain records); 4) data processing is necessary to protect the life of a data subject (for example the data subject is unconscious after a car accident, and the hospital needs to know from the data subject's family doctor whether the data subject uses certain medication); 5) data processing happens for a public task (for example the tax office gathers certain data, such as people's tax returns, to fulfil its tasks); and 6) when the interests of the data controller prevail over the interests of the data subject. The most important for financial services companies are the following: 1) consent to data processing; 2) contractual necessity; and 3) legitimate interests of the data subject. Also see Article 29 of *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* (9 April 2014).

78 Rodotà "Data Protection as Fundamental Human Right" 77.

79 Hoofnagle 2018 *EuCML* 162.

cross-border data transfer handling; and companies' appointment of data protection officers to oversee GDPR compliance.

The GDPR therefore sets a mandatory baseline of standards for all companies that handle data for EU citizens to protect personal data movement and processing. It is thus important to note that any company (including South African companies) that seeks to market or markets its goods or services (including financial services) in the EU, irrespective of its location, is subject to the GDPR. The GDPR's data protection requirements thus have a global impact.

6.1 The GDPR requirements

The GDPR's most important provisions will be discussed in this section. The GDPR contains ninety-one articles set out in eleven chapters.

An important feature of the GDPR is the fact that it provides data subjects with significant control over automatically processed personal data.[80] This affords data subjects the right to portability. The right to portability implies that data subjects can transfer personal data on their own without third parties interfering in the process (as long as the operating software systems are secure). Such data subjects will also be afforded the right to erasure, which allows them to instruct a data controller to erase their personal data should they so wish.[81] The GDPR right to the erasure of personal data (the right to be forgotten) is crucial in the financial markets as it has extra-territorial application. Instances in which a data subject can exercise the right to be forgotten include when:

a) the retention or other processing of personal data of the data subject is unlawful;[82]

b) a legal obligation has been imposed on the controller to erase data;[83]

c) the data subject withdraws consent to personal data processing and the controller has no other legal grounds for processing such data;[84] and

80 Articles 17 and 18 of the GDPR.
81 Article 17(1) and (2) of the GDPR.
82 Article 17(1)(a), (c) and (d) of the GDPR.
83 Article 17(1)(e) of the GDPR.
84 Article 17(1)(b) and (f) read together with Art 8(1) of the GDPR.

d) the application of the opt-out principle from data processing for direct marketing is invoked.[85]

In view of the foregoing, should the processing of personal data be deemed unlawful or an obligation is placed upon a financial institution to erase data, such a financial institution is compelled to act in accordance with the GDPR.[86]

Companies are also obliged to implement rational data protection measures aimed at protecting consumers' personal data and privacy against loss or exposure.[87] Such data protection measures must be augmented by data breach notifications.[88] In instances of single data breaches, data controllers must inform the supervising authorities of any such personal data breach within a period not exceeding seventy-two hours from the point they learnt of such breach.[89] When informing the supervising authorities of a personal data breach, the data controllers should provide exact details of the breach.[90] The data controllers must also promptly notify data subjects as soon as data breaches occur that place their rights and freedoms at high risk.[91] The GDPR mandates companies to conduct Data Protection Impact Assessments as well as Data Protection Compliance Reviews in order to identify and address risks to consumer data.[92]

The GDPR also makes provision for a data protection officer whose key duties centre on ensuring companies' compliance with GDPR and reporting data subjects as well as the supervisory authorities.[93] More significantly, the GDPR extends the scope of data protection to international companies that will collect and process EU citizens' personal data. Such international companies (for example, South African financial services companies doing business with EU financial services institutions) will be subjected to the same GDPR and penalties as EU-based companies.[94] Such penalties as are to be imposed upon non-compliance are set out in Article 79 of the GDPR and can go up to four per cent of the contravening company's global annual revenue.

---

85 Article 17(1)(c) read together with Art 21(2) of the GDPR.
86 Exceptions are set out in Art 95 of the GDPR, however, which refers to the e-Privacy Directive. Also see Article 17(3)(b) of the GDPR.
87 Articles 23 and 30 of the GDPR.
88 Articles 31 and 32 of the GDPR.
89 Article 31 of the GDPR.
90 Article 31 of the GDPR.
91 Article 32 of the GDPR.
92 Articles 33 and 33(a) of the GDPR.
93 Articles 36 and 37 of the GDPR.
94 Article 45 of the GDPR.

Currently the GDPR is regarded as the global standard for protecting the rights of any individual whose personal data enters the digital world.[95] The fundamental user rights contained in the GDPR are seen as an instrument of best practice and Bernstein agrees that since its implementation, the GPDR has significantly increased awareness of these rights.[96] These fundamental rights are the standard that companies and organisations in South Africa and the African continent should aim to comply with. The rights are: the right to transparency and information;[97] the right to be forgotten;[98] the right to restrict data processing;[99] the right to data portability;[100] the right to object;[101] rights in respect of decisions involving automated processing and profiling;[102] and the right to access.[103] Apart from the rights granted to

95 Bernstein 2018 https://techcentral.co.za/sa-firms-at-high-risk-from-europes-gdpr/80801/.

96 Bernstein 2018 https://techcentral.co.za/sa-firms-at-high-risk-from-europes-gdpr/80801/.

97 MacKenzie 2019 https://www.bakermckenzie.com/en/insight/publications/2019/05/general-data-protection-regulation. Companies must provide data subjects with information pertaining to who had access to their personal data, for what purpose and what it will be used for, the identity of the recipients of such data, and the timeframe for which the data will be kept (Art 15 of the GDPR). Such information should be provided to data subjects in a "clear and transparent manner, using intelligible and plain language".

98 Data subjects have the right to demand that their personal data be deleted without unjustifiable deferral, subject to stated grounds. Such grounds include the following: 1) that the use of the personal data is no longer appropriate for the reason for which it was originally collected or processed; 2) that the data subject has withdrawn consent for the processing of the data with such consent being a legal requirement; and 3) that the deletion of the data is a legal duty on the part of the company in terms of local or foreign law (see Art 17 of the GDPR).

99 Data subjects have entitlement to request that a company must stay processing their personal data, subject to stated grounds. Such stay of processing personal data may be prompted by a need to challenge the exactness of the data, or owing to the fact that the processing of the data was illegal and the data subjects request data use restriction as opposed to erasure (see Art 18 of the GDPR).

100 A data subject has the entitlement to obtain their personal data from a specific company and then transfer such data to another company (see the right to data portability in Art 20 of the GDPR). Such entitlement is not applicable in instances where the processing of the data "is for the purpose of the public interest or is done in the exercise of an official authority".

101 Data subjects have the entitlement to object to the processing of their personal data where such data has been initially processed with the consent of the data subjects who later wish to withdraw such consent, or where the data is processed for direct marketing reasons (see Art 21 of the GDPR).

102 The GDPR stipulates that a data subject may not be subject to decisions premised only on automated processing. This includes decisions based on profiling which have the effect of producing legal ramifications regarding a data subject based on such automation (see Art 22 of the GDPR).

103 A data subject has the entitlement to be informed whenever a company processes his or her data, to receive a copy of such data, to be informed of the sources of such data and to be granted the chance to file a complaint against such collection and processing (see Arts 13 and 14 of the GDPR).

data subjects by the GDPR, provision is also made for the international movement of data (cross-border data transfers).[104] The GDPR has set up a framework for the cross-border transfers of data.[105] For internal data transfer to take place, the European Commission (EC) must first evaluate the data-transfer legal regimes of countries where the data is destined to go and be satisfied with the legal regimes thereof.[106] To date, only eleven countries have had their legal regimes approved by the EC (Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay).[107] The aforementioned approval is granted only after protracted negotiations with the targeted data destination (the country) having to update its national data protection regime to a level similar to that of the data protection rules of the EU. Should data be transferred to a non-EU country in the absence of a legal regime adequacy decision, a contractual agreement would have to be entered into by the concerned organisation guaranteeing that it will adhere to the stipulated level of data protection envisaged by the GDPR (this will include all material and procedural safeguards). As a result, data transfer to a non-EU institution will still be regulated by the GDPR and be subject to the same level of protection offered to a data subject that stayed in EU-territory.

7 The POPIA and GDPR compared

The POPIA applies to the processing of personal data in South Africa which has been entered into a record by or for a "responsible party".[108] A responsible party refers to a public or private body or any legal subject, acting alone or in conjunction with others, which regulates the purpose and means for processing the personal data.[109] On the other hand, as a privacy and security law, the GDPR applies to data "controllers" and "processors" that are: established in the EU; and established outside the EU but offering goods or services to data subjects in the EU or monitoring the behaviour of EU data subjects.[110] The POPIA and GDPR are likely to offer African governments a standard by which to measure the efficacy of their data protection regulatory frameworks. The GDPR[111] in particular is likely to offer financial services companies and other organisations in Africa an

104 See Art 44 of the GDPR. Also see Schwartz and Peifer 2017 *Geo LJ* 115.
105 Article 49 of the GDPR.
106 Article 45 of the GDPR.
107 European Commission 2020 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en.
108 See the Preamble of POPIA.
109 Section 1 of POPIA.
110 Article 3 of the GDPR. Also see Art 27 of the GDPR.
111 See for example *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Case C-131/12) [2014] ECLI:EU:C:2014:317 para 71.

international standard to adopt in so far as data protection is concerned, thus maintaining the trust of the international community. The POPIA and GDPR could offer best practices on how to secure personal data in Africa's financial services market and related sectors. This section of the article thus compares the POPIA and GDPR with a view to setting out the best practices in so far as personal data protection is concerned. The section also seeks to point to areas in which the POPIA could be strengthened in comparison to the GDPR, which is internationally oriented.

In principle, the main similarities and differences between POPIA and GDPR are summarised in the table below:

Main similarities and differences between the POPIA and GDPR	
POPIA	**GDPR**
Similarities	
Protects data of living and not deceased individuals[112]	GDPR protects only living individuals and not deceased individuals[113]
Section 1 of the POPIA defines a "responsible party" as a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.	The GDPR defines a data controller as a "natural and legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."
Section 1 of the POPIA defines an "operator" as a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.	The GDPR defines a data processor as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

112 Section 1 of POPIA.
113 Articles 2, 4(1); and Recitals 2, 14 and 22-25 of the GDPR.

The POPIA applies to responsible parties that may be public bodies	The GDPR applies to data controllers and data processors who may be public bodies.
Section 3 of the POPIA clarifies that it applies where the responsible party is either domiciled in South Africa; or not domiciled in South Africa but makes use of automated or non-automated means in South Africa, unless those means are used only to forward personal information through South Africa.	The GDPR applies to organisations that have presence in the EU. In particular, under Article 3, the GDPR applies to entities or organisations established in the EU, notably entities that have an "establishment" in the EU, or if the processing of personal data takes place in the context of the activities of that establishment, irrespective of whether the data processing takes place in the EU or not.
Differences	
Section 1 of the POPIA clarifies that a "data subject" means the person to whom the personal information relates. In addition, though, the POPIA also defines a "person" as meaning a natural person or a juristic person.	Article 4(1) of the GDPR clarifies that a data subject is "an identified or identifiable natural person".
The POPIA does not explicitly refer to the nationality or place of residence of data subjects.	The GDPR provides that it "should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data".
The POPIA applies only where either the responsible party is domiciled in South Africa or is using means in South Africa. The POPIA does not refer to the offering of goods or services, or the monitoring of individuals from abroad.	In relation to extraterritorial scope, the GDPR applies to the processing activities of data controllers and data processors that do not have any presence in the EU, where processing activities are related to the offering of goods or services to individuals in the EU, or to the

	monitoring of the behaviour of individuals in the EU.

In scope and content, the POPIA has to be aligned as closely as possible to the GDPR in the best interests of South Africa's trade in goods and services relations. This is attributed to the simple reason that the GDPR is no longer a Europe-specific global data privacy standard but a standard with greater influence around the world. Further, companies in South Africa and the broader African continent that process customer data from the EU must be compliant with the GDPR. South Africa is one of the EU's largest trade partners, so the POPIA must be in line with the GDPR. Since the POPIA was crafted in such a way as to be similar to the EU Directive,[114] it is plausible to conclude that the POPIA and GDPR are more similar than they are different. However, it is pertinent to point out that the GDPR establishes further data protection requirements which the EU Directive did not provide for, and which are currently not required under the POPIA, as will be explained later in this section.

The POPIA and the GDPR contain the same fundamental concepts. For example, the POPIA uses the term "personal information" whereas the GDPR uses the terms "data subject" and "personal data". In the POPIA and the GDPR the concept "personal information/data" refers to information relating to natural persons, ranging from age, gender and race to religious and political views. The term "data subject" refers to any natural person to whom the personal information/data relates.

The POPIA applies to all companies and organisations that collect and process South African consumers' personal information. The POPIA's provisions strictly apply to the extent to which companies are registered and incorporated in South Africa. On the other hand, the GDPR is applicable to companies and organisations, in South Africa and beyond, which process personal data or monitor the online financial activities (or other activities) of EU citizens. This implies that a financial services company which offers its services to EU citizens is mandated to comply with the GDPR. However, a South Africa registered and incorporated company or organisation offering services to South Africans only is not expressly mandated to comply with the GDPR as it does not process data pertaining to EU citizens. In practice this is highly unlikely due to the integrated nature of the financial services sector owing to globalisation and multilateral free market and trade policies which promote cross-border business transactions. As such, companies

114 Bernstein 2018 https://techcentral.co.za/sa-firms-at-high-risk-from-europes-gdpr/80801/.

and organisations registered in South Africa will need to comply with the GDPR.

It is also worth noting that the POPIA places emphasis on where the personal information is processed. For POPIA to apply, the information in question must have been processed in South Africa. POPIA therefore does not have an extra-territorial application. On the other hand, the GDPR can be applied extra-territorially. As such, in terms of the GDPR, regardless of the fact that the data controller or processor of personal information is located outside the EU, the GDPR will still apply should such controller or processor handle personal information of a data subject situated within the EU.

Both the POPIA and the GDPR provide data subjects with broad rights in dealing with their personal information. Such rights include the rights to access data, to object to the processing of personal information for the purpose of direct marketing, or to request the correction, destruction or deletion of the personal information. However, the GDPR provides an additional right to data subjects to access their data in a structured, commonly used, machine-readable format[115] and a right to the transmission of their data directly from one controller to another without hindrance.[116]

8 Conclusion

The financial services market, as a significantly intertwined and increasingly entrepreneurial ecosystem, remains a fundamental driver of socio-economic development in any country. However, as pointed out in this article, the sector has come under severe threats from cyber attacks, with very few financial services providers having established security baselines and standards for external partners, suppliers, and vendors, and only a few complying with their privacy policies. It is in this context that this article discussed the adequacy of the POPIA to protect data subjects' personal information in an era of increased cyber attacks. The analysis undertaken in this article established that the POPIA, once in full operation, is likely to be a key instrument in protecting data subjects' personal data in the financial services market and beyond. The POPIA compares fairly well with the GDPR which is globally applicable. Though South Africa is not yet recognised as being GDPR compliant, the POPIA goes a long way in kick-starting the evolution of personal data protection in South Africa's financial services market. This is essential for the financial services industry as big data can now be analysed from a number of perspectives, such as cyber-security, fraud and physical security, as well as by third parties. As the type,

115 Article 20 of the GDPR.
116 Article 20 of the GDPR.

quantity and complexity of data increases, reorganising business structures to more efficiently combat the shifting threat will increase in importance; enabling improved business intelligence, a more rapid response to threats, reduced costs, and ultimately the better leverage of scarce data and scientific talent. Both the POPIA and the GDPR can help realise this objective.

The POPIA and the GDPR can thus go a long way toward guaranteeing that data is protected in the financial services market. Data protection must advance from a mere IT scheme to being the nucleus of vital financial services companies' decisions, particularly because impactful technology resolutions are being made with amplified regularity. It is therefore imperative for organisational structures to adjust to optimise security procedures. The POPIA and the GDPR offer such an opportunity.

There is increasing recognition in South Africa and the rest of the world that information/personal data must be protected at the database and data element level. Should the premise of protecting data at the micro-level be plausible, then approaches to data security will focus on an in-depth risk-based approach to defence around high-risk and high-value repositories. To that end, despite the differences between the POPIA and the GDPR, there are sufficient similarities between the legal instruments to ensure that the POPIA is brought into compliance with the GDPR and will promote data protection in the financial services market in South Africa.

It is thus possible to conclude that the POPIA will go a long way toward protecting personal data in South Africa's financial services market on account of the progress made in complying with the GDPR. However, to be regarded as fully GDPR compliant the POPIA should be amended to include a few extra requirements for data protection (especially in the financial services market), such as conducting privacy impact assessments and building privacy by design into the fabric of companies, as well as improving records and bodies of evidence to demonstrate compliance.

This article has thus set out the normative foundations, attributes, and strategic approach to regulating personal data advanced by the POPIA. The approach and provisions of the POPIA and the GDPR with regard to data protection have been articulated. The potential implications of the POPIA and its comparability with the GDPR have been outlined. It has been pointed out that the POPIA, whilst being marginally different from the GDPR, can still be useful in protecting personal data in the financial services market due to the similarities between the two instruments. This article has also pointed out that the core of the GDPR as a data protection law is remarkably stable. Hence, the POPIA needs to be in compliance with the GDPR. This would also ensure compliance with the Fair Information Principles. This is because

the GDPR brings personal data into a complex, detailed, and protective regulatory regime, which has profound implications. For example, the GDPR encourages companies to think carefully about their personal data practices and attempts to make companies take privacy seriously. It also encourages companies to vet service providers for their compliance with personal data protection rules and elevates the position of privacy officials in organisations. In addition, the GDPR is sceptical of the legal tool of "informed consent", stresses the significance of accurate data, and grants people the right to access and correct data.

The discussion advanced in this article must be construed from the point of view that rules for the fair processing of personal data (in general and in particular with regard to data protection in the financial services market) will never be exhausted. As is the case in consumer protection law, personal data protection rules will have to be updated and amended frequently to adjust to novel conditions. In conclusion, the POPIA signals the advent of a new chapter in privacy law and personal data protection in South Africa and the rest of Africa. It is likely to improve personal data protection in the financial services market and probably to reduce the prevalence of cyber attacks, especially if it is brought into compliance with the GDPR and the *Cybersecurity Bill* is passed into law to augment the role played by the POPIA in personal data protection.

Bibliography

Literature

Akinbowale, Klingehofer and Zerihun 2020 *JFC*
Akinbowale OE, Klingehofer, HE and Zerihun MF "Analysis of Cyber-crime Effects on the Banking Sector Using the Balanced Score Card: A Survey of Literature" 2020 *JFC* 945-958

Alshubiri, Jamil and Elheddad 2019 *IJEBM*
Alshubiri F, Jamil SA and Elheddad M "The Impact of ICT on Financial Development: Empirical Evidence from the Gulf Cooperation Council Countries" 2019 *IJEBM* 1-14

Boer and Vazquez *Cyber Security and Financial Stability*
Boer M and Vazquez J *Cyber Security and Financial Stability: How Cyber-attacks could Materially Impact the Global Financial System* (Institute of International Finance Washington DC 2017)

DTTL *2012 DTTL Global Financial Services Industry Security Study*
Deloitte Touche Tohmatsu Limited *2012 DTTL Global Financial Services Industry Security Study* (Deloitte Global Services Limited New York 2012)

Dupont 2019 *J Cybersecur*
Dupont B "The Cyber-resilience of Financial Institutions: Significance and Applicability" 2019 *J Cybersecur* 1-17

FRA *Handbook on European Data Protection Law*
European Union Agency for Fundamental Rights *Handbook on European Data Protection Law* (Publications Office of the European Union Luxembourg 2018)

Fuster *Emergence of Personal Data Protection*
Fuster GG *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer Cham 2014)

Hernandez de Cos "Financial Technology"
Hernandez de Cos P "Financial Technology: The 150-year Revolution" Keynote address delivered at the *22nd Euro Finance Week* (19 November 2019 Frankfurt) 1-11

Hoofnagle 2018 *EuCML*
Hoofnagle C "Designing for Consent" 2018 *EuCML* 162-171

Hoofnagle, Van der Sloot and ZuiderveenBorgesius 2019 *ICTL*
Hoofnagle CJ, Van der Sloot B and ZuiderveenBorgesius F "The European Union General Data Protection Regulation: What it is and What it Means" 2019 *ICTL* 65-98

Jang-Jaccard and Nepal 2014 *JCSS*
Jang-Jaccard J and Nepal S "A Survey of Emerging Threats in Cybersecurity" 2014 *JCSS* 973-993

Rodotà "Data Protection as Fundamental Human Right"
Rodotà S "Data Protection as Fundamental Human Right" in Gutwirth S *et al* (eds) *Reinventing Data Protection?* (Springer Dordrecht 2009) 77-82

Rücker and Kugler *New European General Data Protection Regulation*
Rücker D and Kugler T *New European General Data Protection Regulation: A Practitioner's Guide* (Baden-Baden Nomos 2018)

Schwartz and Peifer 2017 *Geo LJ*
Schwartz PM and Peifer KN "Transatlantic Data Privacy Law" 2017 *Geo LJ* 115-179

Senousy, El-Khamisy and Riad 2018 *IJCSIS*
Senousy Y, El-Khamisy N and Riad AEM "Recent Trends in Big Data Analytics towards More Enhanced Insurance Business Models" 2018 *IJCSIS* 39-45

Vasarhelyi and Kogan 2015 *Account Horiz*
Vasarhelyi MA and Kogan A "Big Data in Accounting: An Overview" 2015 *Account Horiz* 381-396

Voigt and Von dem Bussche *EU General Data Protection Regulation*
Voigt P and Von dem Bussche A *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer Cham 2017)

Yoon 2020 *Sustainability*
Yoon S "A Study on the Transformation of Accounting Based on New Technologies: Evidence from Korea" 2020 *Sustainability* 1-22

Case law

Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (Case C-131/12) [2014] ECLI:EU:C:2014:317

Legislation

Europe

Charter of Fundamental Rights of the European Union (2012) 2012/C326/02

Convention on Cybercrime (2001)

Directive 95/46/EC (Data Protection Directive) (24 October 1995)

*General Data Protection Regulation (EU) 2016/679 (*27 April 2016)

Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (9 April 2014)

South Africa

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Electronic Communications and Transactions Act 25 of 2002

Protection of Personal Information Act 4 of 2013

Government publications

Cybercrimes and Cybersecurity Bill [B6-2017]

Proc R21 in GG 43461 of 22 June 2020

Internet sources

Anon 2020 https://www.securitymagazine.com/articles/93534-six-cybersecurity-threats-the-financial-services-sector-faces
Anon 2020 *Six Cybersecurity Threats the Financial Services Sector Faces* https://www.securitymagazine.com/articles/93534-six-cybersecurity-threats-the-financial-services-sector-faces accessed 3 February 2021

Barnes 2018 https://dynamicbusiness.com.au/topics/technology/there-are-two-types-of-companies-those-who-know-theyve-been-hacked-those-who-dont.html
Barnes S 2018 *There are Two Types of Companies: Those Who Know They've been Hacked and Those Who Do Not* https://dynamicbusiness.com.au/topics/technology/there-are-two-types-of-companies-those-who-know-theyve-been-hacked-those-who-dont.html accessed 2 March 2021

Baur-Yazbeck, Frickenstein and Medine 2019 https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf
Baur-Yazbeck S, Frickenstein J and Medine D 2019 *Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion* https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf accessed 22 February 2021

Bernstein 2018 https://techcentral.co.za/sa-firms-at-high-risk-from-europes-gdpr/80801/
Bernstein D 2018 *SA Firms at High Risk from Europe's GDPR* https://techcentral.co.za/sa-firms-at-high-risk-from-europes-gdpr/80801/ accessed 2 April 2021

Biallas and O'Neill 2020 https://www.ifc.org/wps/wcm/connect/448601b9-e2bc-4569-8d48-6527c29165e8/EMCompass-Note-85-AI-Innovation-in-Financial-Services.pdf?MOD=AJPERES&CVID=nfuDUlG
Biallas M and O'Neill F 2020 *Artificial Intelligence Innovation in Financial Services* https://www.ifc.org/wps/wcm/connect/448601b9-e2bc-4569-8d48-6527c29165e8/EMCompass-Note-85-AI-Innovation-in-Financial-Services.pdf?MOD=AJPERES&CVID=nfuDUlG accessed 2 March 2021

Borghard 2018 https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324

Borghard E 2018 *Protecting Financial Institutions against Cyber Threats: A National Security Issue* https://carnegieendowment.org/2018/09/24/protecting-financial-institutions-against-cyber-threats-national-security-issue-pub-77324 accessed 16 February 2021

De la Riva 2018 https://www.buguroo.com/en/blog/cybercriminals-in-the-financial-sector-understanding-the-culprits-behind-the-keystrokes
De la Riva P 2018 *Cybercriminals in Financial Sector: The Culprits Behind the Keystrokes* https://www.buguroo.com/en/blog/cybercriminals-in-the-financial-sector-understanding-the-culprits-behind-the-keystrokes accessed 5 February 2021

European Commission 2020 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en
European Commission 2020 *Data Transfers Outside the EU* https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en accessed 8 February 2021

European Parliament 2020 https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf
European Parliament 2020 *The Ethics of Artificial Intelligence: Issues and Initiatives*
https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf accessed 12 February 2021

Gartner 2013 https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf
Gartner 2013 *Threat Intelligence: What is it, and How can it Protect You from Today's Advanced Cyber-attacks?* https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf accessed 12 February 2021

GlobeNewswire 2020 https://www.globenewswire.com/news-release/2020/10/26/2114405/0/en/Global-Mobile-Payment-Technology-Market-Will-Reach-USD-5-500-billion-by-2026-Facts-Factors.html
GlobeNewswire 2020 *Global Mobile Payment Technology Market will Reach USD 5,500 Billion by 2026: Facts and Factors* https://www.globenewswire.com/news-release/2020/10/26/2114405/0/en/Global-Mobile-Payment-Technology-Market-Will-Reach-USD-5-500-billion-by-2026-Facts-Factors.html accessed 16 February 2021

IBM 2014 https://www.readkong.com/page/ibm-security-services-2014-cyber-security-intelligence-index-6806866

International Business Machines Corporations 2014 *IBM Security Services 2014 Cyber Intelligence Index – Analysis of Cyber Attack and Incident Data from IBM's Worldwide Security Operations* https://www.readkong.com/page/ibm-security-services-2014-cyber-security-intelligence-index-6806866 accessed 18 February 2021

IMF 2020 https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/
International Monetary Fund 2020 *Cyber Risk is the New Threat to Financial Stability* https://blogs.imf.org/2020/12/07/cyber-risk-is-the-new-threat-to-financial-stability/ accessed 17 February 2021

Intel Team 2013 https://www.cyberdisruption.com/?cat=1687
Intel Team 2013 *Not Your Average Cybercriminal: A Look at the Diverse Threats to the Financial Services Industry* https://www.cyberdisruption.com/?cat=1687 18 February 2021

Kuneva 2009 http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm
Kuneva M 2009 *Keynote Speech SPEECH/09/156 (Roundtable on Online Data Collection, Targeting and Profiling March 31, 2009)* http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm accessed 19 February 2021

Lagazio, Sherif and Cushman 2020 https://core.ac.uk/download/pdf/20543077.pdf
Lagazio M, Sherif N and Cushman M 2020 *A Multi-level Approach to Understanding the Impact of Cyber-crime on the Financial Sector* https://core.ac.uk/download/pdf/20543077.pdf accessed 16 February 2021

Lund 2021 https://www.superoffice.com/blog/digital-transformation/
Lund J 2021 *How Customer Experience Drives Digital Transformation* https://www.superoffice.com/blog/digital-transformation/ accessed 20 February 2021

MacKenzie 2019 https://www.bakermckenzie.com/en/insight/publications/2019/05/general-data-protection-regulation
MacKenzie B 2019 *General Data Protection Regulation (GDPR) in Africa: So What?* https://www.bakermckenzie.com/en/insight/publications/2019/05/general-data-protection-regulation accessed 23 February 2021

Marketwired 2013 https://www.yahoo.com/news/agari-q3-trustindex-report-financial-120000057.html
Marketwired 2013 *Agri Q3 TrustIndex Report: Financial and Health Care Most at Risk for Email-Based Cyberattacks*

https://www.yahoo.com/news/agari-q3-trustindex-report-financial-120000057.html accessed 26 April 2021

Morgan 2021 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
Morgan S 2021 *Cybercrime to Cost the World $ 10.5 Trillion Annually by 2025* https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ accessed 3 February 2021

Muncaster 2021 https://www.infosecurity-magazine.com/news/financial-services-suffered-covid/
Muncaster P 2021 *Most Financial Services have Suffered COVID-linked-cyber-attacks* https://www.infosecurity-magazine.com/news/financial-services-suffered-covid/ accessed 22 February 2021

Norwich University Online 2017 https://online.norwich.edu/academic-programs/resources/who-are-cyber-criminals
Norwich University Online 2017 *Who are Cyber Criminals?* https://online.norwich.edu/academic-programs/resources/who-are-cyber-criminals accessed 5 February 2021

OECD 2020 http://www.oecd.org/daf/competition/digital-disruption-in-financial-markets.htm
Organisation for Economic Co-operation and Development 2020 *Digital Disruption in Banking and its Impact on Competition* http://www.oecd.org/daf/competition/digital-disruption-in-financial-markets.htm accessed 21 February 2021

Pan *et al* 2015 https://www.cpaaustralia.com.au/~/media/corporate/allfiles/document/professional-resources/business/analytics-and-cybersecurity.pdf
Pan G *et al* (eds) 2015 *Analytics and Cybersecurity: The Shape of Things to Come* https://www.cpaaustralia.com.au/~/media/corporate/allfiles/document/professional-resources/business/analytics-and-cybersecurity.pdf accessed 12 February 2021

PwC 2014 https://collabra.email/wp-content/uploads/2015/04/2014-us-state-of-cybercrime.pdf
PricewaterhouseCoopers 2014 *US Cybercrime: Rising Risks, Reduced Readiness: Key Findings from the 2014 US State of Cybercrime Survey* https://collabra.email/wp-content/uploads/2015/04/2014-us-state-of-cybercrime.pdf accessed 18 February 2021

PwC 2014 https://www.pwc.com/na/en/assets/pdf/global-state-of-information-security-survey-2014-key-findings-report.pdf

PricewaterhouseCoopers 2014 *Defending yesterday: Key findings from the Global State of Information Security Survey 2014* https://www.pwc.com/na/en/assets/pdf/global-state-of-information-security-survey-2014-key-findings-report.pdf accessed 19 February 2021

Rathi 2020 https://internationalsecurityjournal.com/cybercrime-and-the-financial-system/
Rathi S 2020 *Cybercrime and the Risks to the Financial System* https://internationalsecurityjournal.com/cybercrime-and-the-financial-system/ accessed 3 February 2021

Sobers 2021 https://www.varonis.com/blog/cybersecurity-statistics/
Sobers R 2021 *Cybersecurity Issues are Becoming a Day-to-day Struggle for Businesses* https://www.varonis.com/blog/cybersecurity-statistics/ accessed 15 February 2021

UNCTAD 2018 https://unctad.org/system/files/official-document/tir2018_en.pdf
United Nations Conference on Trade and Development 2018 *Harnessing Frontier Technologies for Sustainable Development Innovation and Technology Report 2018* https://unctad.org/system/files/official-document/tir2018_en.pdf accessed 12 February 2021

World Bank Group 2019 https://pubdocs.worldbank.org/en/208271558450284768/CybersecDigest-3rd-Edition-May2019.pdf
World Bank Group 2019 *Financial Sector's Cybersecurity: A Regulatory Digest* https://pubdocs.worldbank.org/en/208271558450284768/CybersecDigest-3rd-Edition-May2019.pdf accessed 23 April 2021

World Bank Group 2018 https://openknowledge.worldbank.org/handle/10986/11866
World Bank Group 2018 *Financial Sector's Cybersecurity: Regulations and Supervision* https://openknowledge.worldbank.org/handle/10986/11866 accessed 23 April 2021

List of Abbreviations

Account Horiz	Accounting Horizons
AI	Artificial Intelligence
CPA	Consumer Protection Act 68 of 2008
DPD	Data Protection Directive
DTTL	Deloitte Touche Tohmatsu Limited
EC	European Commission

ECTA	Electronic Communications and Transactions Act 25 of 2002
EU	European Union
EuCML	Journal of European Consumer and Market Law
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
Geo LJ	Georgetown Law Journal
IBM	International Business Machines Corporations
ICT	Information and Communication Technology
ICTL	Information and Communication Technology Law
IJCSIS	International Journal of Computer Science and Information Security
IJEBM	International Journal of Engineering Business Management
IMF	International Monetary Fund
IT	Information Technology
J Cybersecur	Journal of Cybersecurity
JCSS	Journal of Computer and System Sciences
JFC	Journal of Financial Crime
NFC	Near Field Communication
OECD	Organisation for Economic Co-operation and Development
OJ	Official Journal of the European Union
POPIA	Protection of Personal Information Act 4 of 2013
PwC	PricewaterhouseCoopers
UK	United Kingdom
UNCTAD	United Nations Conference on Trade and Development