Insurance & Data Privacy

Data Breach Financial Implications of the Protection of Personal Information Act

April 2021

AON
Empower Results®

Table of Contents

4

Introduction

5

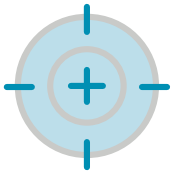
What is the Protection of Personal Information Act?

- Enforcement

6

What are some of the impacts of POPIA for your Company?

7



How can Cyber Insurance assist with POPIA?

11

Case Study

12

What are the next steps?

“The purpose of this publication is to:

Provide an overview of the Protection of Personal Information Act (POPIA).

Highlight the impact that POPIA will have on organisations.

Identify how cyber insurance can assist.”

Introduction

The Protection of Personal Information Act (POPIA), came into effect on 1 July 2020[1] and specifically regulates the processing of information pertaining to natural living persons as well as existing legal persons. This publication seeks to provide some insight as to how organisations can transfer some of the risks arising from this new regulation utilising a cyber insurance policy.

Following the introduction of POPIA, organisations should consider the following:

- How can POPIA impact their business operations and processes?
- What are the financial implications of adhering to POPIA?
- How can a cyber insurance policy assist with transferring financial risks emanating from POPIA?

1 Following the 12-month transition period, organisations must be compliant with POPIA by 1 July 2021

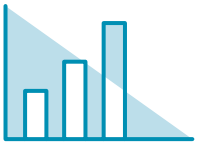
"**Evolving cyber risks** and the Protection of Personal Information Act (POPIA) has created a greater awareness of the **financial impact** of **cyber risks** and emphasised the need for organisations to increase their understanding of **cyber insurance**"

What is the Protection of Personal Information Act?

POPIA was adopted to protect the rights to privacy of natural living persons and in addition, extended to include existing legal persons. It has been introduced to put forth minimum requirements for processing personal information pertaining to these both categories of persons.[2]

The purpose of POPIA is to:

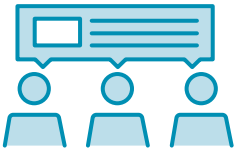
Give effect to the constitutional right of privacy, in particular the safeguarding of personal information;



Regulate the processing of personal information in harmony with international privacy standards;

Prescribe minimum requirements for the lawful processing of personal information;

Provide rights and remedies to protect data subjects against unlawful and illegal uses of their personal information; and



Establish a regulator – i.e. Information Regulator – to promote, enforce and fulfil the rights protected by POPIA.

Within POPIA there are 4 key role players:[3]

Data Subject: Natural living person(s) as well as existing legal person(s) to whom personal information relates to;

Responsible Party: Entity entrusted with personal information who is ultimately responsible for compliance with POPIA;

Operator: A person who processes personal information on behalf of a responsible party in accordance with the terms of the contract or mandate put in place with that responsible party;

Regulator: Information Regulator established pursuant to Section 39 of POPIA

[2] https://www.justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf - Protection of Personal Information Act, 2013

[3] https://www.lssa.org.za/wp-content/uploads/2019/12/Protection-of-Personal-Information-for-South-African-Law-Firms-LSSA-Guidelines-2018.pdf

If you or your organisation are processing personal information, in whatever form or manner, the following key requirements under POPIA must be complied with:[4]

- **Accountability:** The responsible party must comply with all the conditions for lawful processing.
  Purpose specification: Personal information must only be collected for a specific, explicitly defined lawful purpose related to a function or activity of the responsible party.
- **Processing limitation:** Processing must be justified on a ground recognized under POPIA (e.g. consent/legitimate interests of the data subject, responsible party or the third party to whom the information is supplied).
- **Further processing limitation:** Processing must be in accordance with or compatible with the purpose for which it was initially collected.
- **Information quality:** Steps must be taken to ensure that the information is complete, accurate, not misleading and updated where necessary.
- **Openness:** Notification requirements must be complied with when collecting personal information.
- **Security safeguards:** Appropriate, reasonable technical and organisational measures must be implemented and maintained to prevent loss of, damage to or unauthorized destruction of or unlawful access to personal information.
- **Data subject participation:** Data subjects have the right to request details of the personal information that a responsible party holds about them and, in certain circumstances, request access to such information

Enforcement:

Under POPIA, anyone can submit a complaint to the Regulator. If the Regulator deciding to investigate a complaint that they receive, then they are required to notify the complainant and party under investigation as soon as is reasonably possible. In practice, the Regulator can either conduct the investigation or refer the complaint to another regulatory body.

In the event of the Regulator decides to investigate a complaint, it may: (i) call witnesses to give evidence; (ii) review information as part of the investigation; (iii) gain access and search any premises of the party being investigated and conduct inquiries; and (iv) issue warrants.

The Regulator can either decide to settle a complaint or issue enforcement notices. Failure to comply with an enforcement notice can result, on conviction, to a fine of R 10million or imprisonment for a period of no longer than ten years or both a fine and imprisonment. In addition, the complainant can bring a civil action against the responsible party.

It is always important to try and resolve a complaint before they become too costly, as well as demonstrate that you have taken steps to comply with POPIA to mitigate any risks of enforcement notices by the Regulator.[5,6]

[4] **https://www.dlapiperdataprotection.com/index.html?t=collection-and-processing&c=ZA** – All notes pertaining to the eight conditions are as described by DLA Piper

[5] Protection of personal information Act 4 of 2013, DLA piper handbook

[6] https://www.mondaq.com/southafrica/privacy-protection/981326/beware-the-enforcer-enforcement-and-liability-under-popia

What are some of the impacts of POPIA for your company?

As organisations seek to comply with the requirements set out in POPIA, it will become increasingly important for their businesses to make operational changes to the way they process personal information.

In addition to this, organisations will be required to appoint an independent member of their organisation who will be required to perform the function of a data protection officer (referred in POPIA as "information officer").

The function will be to ensure that the principles of POPIA are adhered to and form part of the overall organisational culture. This will include reviewing both new and existing operating procedures to ensure that business complies with strict requirements imposed by POPIA.

This function can be performed by an individual or a group of individuals, who are familiar with the organisation's operations and processes.

The act also requires that the responsible party of data, notify the regulator and data subject of any incident, that may compromise the data subject's information. The notification should describe the consequences of the security incident, measures that are being taken to address the incident, recommendations to effected data subjects to protect against further exploitation of their information and lastly, if it is known, the unauthorised party who may have accessed the information.[7]

Adapting to this legal change comes with its challenges, and the management of your organisation needs to be aware of, and co-ordinate the appropriate steps to mitigate the impact of such a new piece of legislation.

[7] https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=ZA

How can Cyber Insurance assist with POPIA?

Cyber insurance and POPIA

The scope of POPIA is broader than most cyber insurance policies which are often triggered by privacy or security incidents, whereas POPIA violations can also be triggered by non-compliance separate and apart from a privacy or security incident.

The current insurance market does allow for some expansion of cover to specifically address certain instances of non-compliance as it relates to POPIA, but the language of such insurance policy must be carefully drafted and reviewed. Where a cyber insurance policy is intended to cover such fines, a key issue for organisations is the extent to which those fines are insurable.

Typical cyber insurance policies only insure fines when insurable by applicable laws, and generally stipulate that the insurability of fines or penalties shall be determined by the "laws of any applicable jurisdiction that most favours coverage for such monetary fines or penalties."[8]

Regulatory fines are generally not insurable in South Africa. It is not possible to insure against criminal fines as a matter of law and public policy. Insuring administrative fines is not expressly prohibited but such fines are likely to be found uninsurable as a matter of public policy.

In addition, organisations should also consider other costs and liabilities that could result from non-compliance with POPIA.

To the extent individuals and entities are subject to POPIA, as a general rule, intentional and/or gross negligence resulting in a breach of non-compliance with POPIA will not be covered under an insurance policy.

[8] Aon GDPR Insurability of Fines white paper, 3rd Edition. May 2020"

Cyber insurance policies can play a central role in how an organisation manages and mitigates cyber related risks. It may protect an organisation by not only providing financial indemnification after a cyber incident has gone wrong, but also offering other term consultancy to help improve security and on-the-ground incident response support during a period of crisis following a cyber incident.

From a financial perspective, typically, a cyber insurance policy will assist in incident response costs associated with a cyber incident and subsequent financial liability that may arise such as:[9]

Operational Risk

Network Business Interruption: Reimbursement coverage for the insured for lost net income caused by a network security failure, as well as associated extra expense. Retention and waiting periods are negotiable

System Failure: Expands coverage trigger for business interruption beyond computer network security failure to include any system failure

Dependent Business Interruption/Dependent System Failure: Reimbursement coverage for the insured for lost income caused by a network security failure of a business on which the insured is dependent, as well as associated extra expense. Retentions and waiting periods are negotiable.

Cyber Extortion: It should be noted that there will be no reimbursement cover if payment is not made according to the applicable law.

Digital Asset Restoration: Reimbursement coverage for the insured for costs incurred to restore, recollect, or recreate intangible, non-physical assets (software or data) that are corrupted, destroyed or deleted due to a network security failure.

Privacy Liability: Liability coverage for defence costs and damages suffered by others for any failure to protect personally identifiable or confidential third-party corporate information, whether or not due to a failure of network security. Coverage may include: unintentional violations of the insured's privacy policy, actions of rogue employees, and alleged wrongful collection of confidential information.

[9] Please refer to actual policy as coverage can vary.

Privacy and Network Security Risk

Network Security Liability

Liability coverage for defence costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or disclosure of confidential information, unauthorized access, unauthorized use, denial of service attack or transmission of a computer virus.

Privacy Regulatory Fines and Penalties

Liability coverage for defence costs for proceedings brought by a governmental agency in connection with a failure to protect private information and/or a failure of network security. Coverage includes fines and penalties where insurable by law. Compensatory damages, i.e. amounts the insured is required by a regulator to deposit into a consumer redress fund, may be covered.

Media Liability

Liability coverage for defence costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy. The scope of covered media is variable and can range from the insured's website only to all content in any medium.

PCI Fines and Penalties

Coverage for a monetary assessment (including a contractual fine or penalty) from a Payment Card Association (e.g., MasterCard, Visa, American Express) or bank processing payment card transactions (i.e., an "Acquiring Bank") in connection with an Insured's non-compliance with PCI Data Security Standards.

Breach Event Expenses

Reimbursement coverage for the insured's costs to respond to a data privacy or security incident. Policy triggers vary but are typically based on discovery of an event, or a statutory obligation to notify consumers of an event. Covered expenses include computer forensics expenses, legal expenses, costs for a public relations firm and related advertising to restore your reputation, consumer notification, call centres, and consumer credit monitoring services.

NB:

Please note that each individual insurance policy contains specific terms and conditions which are subject to certain exclusions.

Case Study[10]

The below case study illustrates how a standard ransomware attack[11] could materialise and the expenses incurred to deal with both the incident as well as the subsequent liability.

The table below has been split between (i) the hypothetical expenses incurred by a common ransomware attack on the left and (ii) references of documented real-life examples on the right:

Scenario: Standard ransomware attack	
A retail company suffers a ransomware attack, resulting in a data breach of 100,000 account information records.	
Hypothetical expenses	Real-life examples
Event Management	
Incident response and forensic investigators are required to remediate the incident. Ransomware payment is to recover information that is stolen.	A South African municipality suffered a ransomware attack, as a result, it costs the municipality R50 million[12] to resolve this incident.
Business Interruption	
The company experiences business interruption for a period of up to 3 weeks whilst incident responders and the internal information security team works tirelessly to restore business operations. Subsequently, they phase back operations over a period.	Co-President of Aon's Stroz Friedberg, Eric Friedberg discussing ransomware remediation post breach, stated some breaches can take up to 3 weeks to effectively resolve.[13]
Notification & Credit Monitoring	
Call centre is set up to handle queries by account holders with the retail company. Credit monitoring is offered to the affected data subjects for a period of 6-12 months.	Consideration for credit monitoring services for affected data subjects, as criminal hackers may use the stolen information to open new accounts.[14] All damages flowing from a data breach of the data holder will be considered consequential damages.[15]
Liability Defence & Regulatory Investigation	
Defence costs for possible third-party liability claims. Costs for regulatory investigation and potential fines imposed by the regulator. Regulatory investigation may lead to suspension of processing personal information for a sustained period – this may lead to additional business interruption expenses.	As POPIA is not yet fully in effect, limited information is known on regulatory and liability related defence costs however, examples of fines imposed by regulators following data breaches can be found around the world: • An international hotel chain was fined £20.45m by the UK Information Commissioner's Office (the "ICO") [16] • A UK based airline company was fined £22m by the ICO.

New research from the Ponemon Institute shows that a data breach costs South African companies on average $3.06 million – nearly R50 million.[17]

[10] For informational purposes only. Each ransomware attack is a unique situation and may not follow the scenario noted above.

[11] Ransomware attack: Malware which suspends access to service and/or encrypts information (usually with the threat to publish information publicly), the impact of which may be remedied upon payment of a specified ransom

[12] https://m-net.dstv.com/show/carte-blanche/videos/your-money-or-your-data-the-rise-of-ransomware/video - City of Johannesburg CIO, quoted within the video

[13] https://players.brightcove.net/5968919803001/default_default/index.html?videoId=6140639141001 – Eric Friedberg shares insights on battling ransomware attacks

[14] https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

[15] https://legal.thomsonreuters.com/en/insights/articles/data-breach-liability

[16] https://www.lexology.com/library/detail.aspx?g=de721448-2173-4267-b703-9523f0b0194e

[17] https://businesstech.co.za/news/enterprise/339763/the-average-cost-of-a-data-breach-in-south-africa/

Recommended next steps

Risk Governance

- Carry out a security audit to check personal information is secure against unauthorised access or processing.
- Put in place a plan for ensuring continuous monitoring and follow up of data compliance efforts.
- Ensure contracts with all third-party processors contain at least the minimum terms stipulated by POPIA.

Insurance Review

- Ensure adequate cyber insurance coverage is in place.
- Review your existing cyber insurance policy with assistance from qualified coverage counsel and your broker regarding coverage for non-compliance with POPIA, especially fines and liability post data breach.

Incident Response

- Ensure you have an incident response plan in place, including data security breach notification procedures which is aligned to the requirements of POPIA.
- Review your existing companywide incident response plan to ensure that it incorporates escalation plans and nominated advisors covering all required stakeholders. This includes, business operations,legal, public relation, human resources and key third-parties such as IT service providers.
- Test your incident response plans on a regular basis to ensure they remain effective.

Understanding the threat environment imposed by the introduction of POPIA should be an organisation wide initiative. It is imperative that principles of Risk Governance described above are appropriately applied by organisations, within the context of POPIA pre-breach, whilst also factoring what implications may arise post-breach.

Risk managers and C-Suite level executives within your organisation, should assess how POPIA changes their business requirements in processes such as, incident response and business continuity, whilst making considerations of the value that can be unlocked from the insurance market via forensic consultants, experience in handling claims and incidents that may be somewhat unfamiliar to the business.

This consolidation of enterprise wide risk governance, can help leave organisations in good stead to face adversity from the unforeseen landscape that cyber risks offer, and the subsequent liability that can now be enforced via POPIA.

Contact Information

Zamani Ngidi

Client Manager | Cyber Risk

Cyber Solutions

+27 (0) 11 944 7579

zamani.ngidi2@aon.co.za

Jacobus Barnard

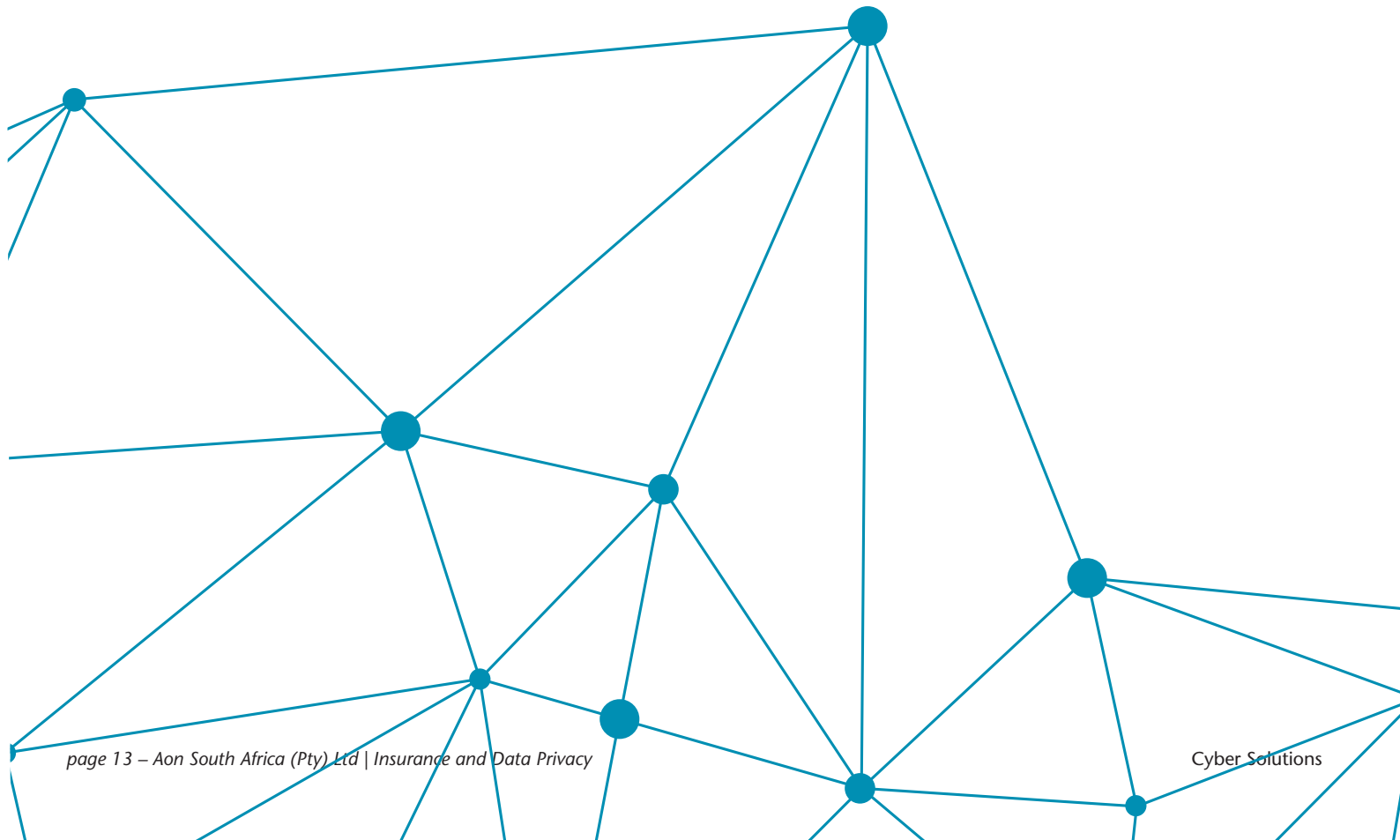
Client Manager | Cyber Insurance

Cyber Solutions

+27 (0) 11 944 7816

jaco.barnard@aon.co.za

Authored by Zamani Ngidi



About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

About Aon South Africa

Aon South Africa is a leading provider of Risk Management Services, Insurance and Reinsurance Broking, Employee Benefits Solutions and Specialty Insurance Underwriting. The company employs more than 700 professionals in its 12 offices in South Africa with its head office in Sandton, Johannesburg.

Aon South Africa (Pty) Ltd, an Authorised Financial Services Provider, FSP # 20555
Aon Re Africa (Pty) Ltd, an Authorised Financial Services Provider, FSP # 20658
Aon Limpopo (Pty) Ltd, an Authorised Financial Services Provider, FSP # 12339

Empower Results®