DIRECTORS AND OFFICERS (D&O) & CYBER RISK LIABILITY

FOR SMES (SMALL & MEDIUM ENTERPRISES)

Insurer: Western National Insurance Company Ltd. **FSP No**. 9465

western
Rethink Insurance

This brochure is an informative document and is always superseded by the specific Policy Wording

PREMIUM & UNDERWRITING

What will this cost a small to medium sized business?

- R85 per month for a Limit of Indemnity of R2,5 million (R2,5m D&O / R2,5m Cyber)
- R125 per month for a Limit of Indemnity of R5 million (R5m D&O / R2,5m Cyber)
- Subject to further information detailed in the schedule and policy wording
- This offering is further limited to companies with a turnover of less than R50 million
- The company's assets must also exceed their liabilities

How do I apply for this insurance?

→ Complete the **Application Form and Debit-Order Authority Mandate**

→ If a higher than R5 million limit of indemnity is required, complete a full **Proposal Form**

WHAT IS DIRECTORS & OFFICERS LIABILITY?

Directors & Officers Liability (often referred to as "D&O") is a commercial insurance policy which provides financial protection for the Directors and Officers of a company in the event they are sued in conjunction with the performance of their duties as they relate to the company.

Since a director can be held personally responsible for acts of the company, most Directors and Officers will demand to be protected rather than put their personal assets at stake.

The D&O cover offered by Genlib is aligned with the Companies Act 71 of 2008. Section 78 (3) of the new Companies Act allows for the indemnification of Directors and the purchase of D&O Liability insurance.

King IV and the introduction of the Companies Act in 2008 has rendered Directors and Officers Liability insurance crucial for all companies regardless of size and incorporation.

Directors and Officers now find themselves in a far more onerous position than ever before, with legislation holding them more accountable for any wrongful or negligent actions, as well as breaches of their fiduciary duties.

In addition, other sources of responsibility include:

- The Company's Memorandum of Incorporation;
- Sector –specific legislation (e.g., in the mining sector, or in healthcare);
- Tax legislation;
- Employment and labour laws;
- Data protection and Privacy legislation (e.g. POPIA);
- Environmental legislation

What are the responsibilities of Directors and Officers?

- ✓ To act in good faith and for a proper purpose;
- ✓ Exercise independent and unfettered judgement and discretion;
- ✓ Exercise one's powers in good faith and for a proper purpose;
- ✓ Not exceed one's powers (acting ultra vires)
- ✓ Account for profits, and not make secret or undisclosed profits
- ✓ Not place oneself in a position of conflict with the company, and not to act on behalf of the company in any matter where such conflict exists
- ✓ To act with the degree of care, skill and diligence that may reasonably be expected of a person carrying out the same functions in relation to the company as those carried out by the director having the general knowledge, same skill and experience of that director – a reasonable man/women test.

WHO NEEDS THE COVER?

- ✓ Past, present and future executive directors AND non-executive directors
- ✓ Employees and volunteers in a managerial / supervisory capacity, audit committee or risk committee, as examples: CEO / CFO / Company Secretary / Information Officer (POPIA / PAIA)
- ✓ Non-Profit organisations : CEO / Treasurer / Secretary

WHO IS THE INSURED?

- ➢ Any person or persons as listed as Insured in the Schedule while acting in their capacity as a director, member, partner or principal of the business including their predecessors in that specific business as director, member, partner or principal and;
- ➢ Any person who becomes a director, member, partner or principal during the period of insurance, but limited to the extent that liability only attaches to the Insured acting in this capacity and;
- ➢ The company or organisation named in the Schedule or any Subsidiary of the named company or organisation;
- ➢ Any employee of the company other than as described above named as co-defendant in an action with any of the above mentioned.

WHAT IS AT RISK?

- → The company itself in terms of its Memorandum of Incorporation or Articles of Association
- → Personal liability: property, cars, assets, savings & pension funds are at risk
- → Spouse, heirs and estates (may be named in a suit)
- → Financial implications of defence costs could be catastrophic
- → Should your personal assets be frozen, are you able to cover the costs of schooling, housing, utilities and personal insurance?

WHAT IS THE FUNCTION OF THIS POLICY?

Protect the decision makers against **ALLEGATIONS** of

- Wilful misconduct and breach of trust
- Breach of Authority
- Illegal acts (if found guilty, insured would have to reimburse insurer)
- Discrimination
- Sexual harassment

Or to **INDEMNIFY** the Insured (Director or officer or the company itself) against

- Wrongful acts – including Breach of duty, Misstatement, Misleading statement, Errors in judgement
- Legal defence costs – it's not just about damages / liabilities
- Fines and penalties, maximum limit R100,000

Where could claims come from?

× **The Company itself**

× **Shareholders:** accounting fraud, dividend declaration, financial performance (or lack thereof), breach of fiduciary duties, inadequate disclosure, insider trading, investment / loan decisions, bankruptcy, mergers & acquisitions

× **Employees:** breach of contract, compensation duties, defamation, discrimination, employee benefits, employee conditions, failure to hire or promote, harassment, whistle blowing, wrongful termination

× **Competitors:** anti-competitive violations, business interference, contract disputes, copyright / patent / trademark infringements

× **Business rescue practitioners or Liquidators**

× **Creditors**

× **Regulators:** such as the FSCA and, in the case of POPIA, the Information Regulator

× **Government:** If a director or officer is found to have breached a duty or obligation, he/she may have a liability to pay compensation (damages), a fine or a penalty. This amount is in addition to bearing their own legal defence costs and the legal costs of the regulator or the party that brought the claim.

ENTITIES EXCLUDED FROM COVER

× Trustees

× Governmental Organisations

× Asset Managers

× Pension Fund Managers

GENERAL EXCLUSIONS (NOT LIMITED TO THIS LIST)

- × Illegal / criminal acts
- × In-fighting where one director sues another
- × Where shareholders holding 25% or more of a shareholding, influence decisions of a director then sue the director for making the decision
- × Where another policy is in force
- × Basic investment performance
- × Where bribes have been paid
- × Environmental impairment
- × Wilful misconduct
- × Wilful breach of trust
- × Claims known to the insured prior to inception of the policy
- × Claims prior to the retroactive date
- × Secret profits
- × Professional indemnity
- × Instigation
- × Insider trading
- × Failure to procure or maintain the relevant insurances

HOW MUCH COVER IS REQUIRED?

- ✓ Our limits are up to R5 million
- ✓ As much as is affordable to the company
- ✓ Remember to buy more cover as the company grows
- ✓ Higher limits are available subject to a completed Proposal Form

A SOUND KNOWLEDGE OF CORPORATE GOVERNANCE IS NECESSARY IN ORDER TO UNDERSTAND THE OBLIGATIONS AND DUTIES OF A POSITION OF AUTHORITY. THE KING COMISSION PROVIDES FOR A SOUND UNDERSTANDING OF CORPORATE GOVERNANCE.

EXTENSIONS

#	Specific Extensions of Cover
1	Corporate Manslaughter
2	Emergency costs
3	Fines and Penalties Extension
4	General Counsel Liability
5	Outside Directorships
6	Protection for Non-Executive Directors
7	Public Relations Consultants
8	Reasonable Costs and Expenses
9	Reputation Protection Expenses
10	Tax, COID and UIF Extension

CYBER LIABILITY

What is covered?

- Operational risks such as not frequently changing passwords which result in a security breach or privacy breach or breach of privacy regulations.
- Legal defence costs
- Fines and penalties
- Maximum Limit of Indemnity is R2,5 million

What you need to know about this cover provided

The cover provided is limited and is not intended to replace a bespoke Cyber Risk policy of insurance.

FREQUENTLY ASKED QUESTIONS

1) Are a company's subsidiaries covered under the D&O policy?

No, this product is designed for SMME's only

2) The D&O policy does not cover fraudulent acts, how will a director defend a fictitious claim?

The D&O policy provides defence costs. The Insurers will decide whether to defend the director in court. Therefore, the director will not have to pay for expensive legal battles which may be drawn out for many years. Should the case be defended successfully, the director would not sustain any personal loss. However, if it is found that the director acted fraudulently, the Insurers will subrogate.

3) Why should private companies purchase D&O insurance?

The costs of defending legal actions may exceed the new worth of the company's assets. A judgement against a director of a private company could lead to major financial losses. Complicated conflicts of interest could arise due to the intertwined responsibilities which exist in private companies.

4) What are some of the main exclusions on the D&O policy?

Dishonesty or fraud, questionable payments, copyright, professional indemnity, illegal profits or gains, pensions, injury, sickness, damage to property and bodily injury, and deliberate acts.

5) Does the D&O policy cover privacy regulations?

Yes, it does, under breach of statutes, where for example the requirements of the act are ignored and providing there is no intentional or wilful transgression of such regulations.

6) What are some examples of privacy regulations (Listed below but not limited to the list)

- Promotion of Access to Information Act, 2000 (PAIA)
- Protection of Personal Information Act, 2021 (POPIA)
- Electronic Communications and Transactions Act, 25 of 2002

7) What are some typical claims examples on a D&O & Cyber Liability policy?

The types of claims against a D&O policy are extensive and continually increasing, some examples are:

- **Minority shareholders** allege that directors have abused their position to favour certain dominant shareholders.
- **Competitor** alleges that the defendant director (former employee) has misappropriated trade secrets and confidential information.
- **Class action complaint** from outside investors stating that directors failed to disclose material information, which could have elucidated that the company would eventually be liquidated.
- **Creditors** allege that directors utilised the plaintiff's services for the company although the said directors were aware that the company was insolvent and would not have the ability to pay.

8) **A specific example of the Cyber Risk Liability responding to a claim:**

XYZ (Pty) Ltd is a small company who deal directly with customers. They store their customers' data for invoicing and also to provide specific reports that are only relevant to each individual client. They obtain and process personal information, some being financial, some being demographic. This is stored on their own server which is located in a dedicated computer room, and they believe that they have all the required protocols and hardware in place to protect their data. However, they did not pay attention to their mobile devices which links into their network.

One day a hacker found his way into their system through a mobile phone and managed to access their database. The hacker actually stumbled by accident into the system and didn't really want to be there but decided he could play around with the data and learn more. (Note: it is immaterial whether the hacker got in intentionally or accidentally). In the process, emails were sent out to recipients with the details of other clients' privileged information. The hacker also managed to print the whole database on the insured's printer, being three reams of paper, and in the end destroyed the database.

The CEO was the first one to get a call from a very irate customer complaining that they had received data which did not make sense and wasn't theirs. The CEO promised to look into it immediately and then discovered that he did not have any access to the database. He sought help from the responsible person who also could not access the information. The outsourced IT service provider was contacted who realised that there was a **security breach** as well as a **privacy breach (Note: Security & Privacy breaches trigger the policy)**. They took the whole day to get access back into the system and managed to get the data restored from a backup. However, to make matters worse, it came to light that the last week's backups hadn't worked, and they now had to recapture all the work of the past week. They hired additional temps and their own staff worked overtime to get the data loaded.

The Insurer was notified by the CEO as soon as he realised what had occurred. **The Insurer would approve the costs for the IT team to restore the data and isolate any potential viruses left behind – in other words, to restore the system to where it should be. The insurer would also allow the overtime costs of the staff to recapture all the work of the past week.**

At some point somebody realised that the database had been printed out on their printer. It had to be destroyed, but the instruction to the cleaner wasn't clear and the docs ended up on an open garbage truck from where the wind blew a lot of these printed docs into the street. A specific page was picked

up and the information printed on that page was sufficient that it could be used to hack into that person's bank account and was able to empty it to the tune of R150 000.

There were two claim demands made for compensation:

The first was for emotional stress **(injury)** on the part of the client who received the wrong information via email and who could not deal with the traumatic news of knowing their data had been hacked.

The second claim was for the R150 000 loss from the person's bank account as it could be pinpointed that the loss of the printed pages lead to the theft **(loss)** of the R150 000.

The insurer would approve both these claims as they are claims for compensation by a third party due to the alleged wrongdoing of the Insured.

- **Information Regulator (POPIA)**

1. I have a POPI plan in place, but for some reason it fails and there is a breach, and we get sued for damages by a third-party.

Q Are these damages covered by the policy?

A Yes, a claim under this policy will respond to the damages as well if is defended or investigated, unless it is found that the incident is not covered in terms of the policy cover.

2. I have a POPI plan in place, but for some reason it fails and there is a breach and fines are imposed by the Information Regulator.

Q Are these fines covered in terms of the policy?

A Yes, fines and penalties are covered in the standard extensions of the policy, as long as these not criminal or fraudulent, intentional of nature, uninsurable under law and for tax infringement.

Q Is there a set sum insured or can the sum insured be increased depending on the clients' requirements?

A The Insurers liability in terms of this extension is sub-limited to R100 000.

3. I have a POPI plan in place and although we do have contracts which ensure that we are not liable for a data-breach incident, I am still concerned that we are exposed – which portions of the policy covers what?

- Cyber Liability: A data breach on your own computer network through electronic means, i.e., a Cyber-attack is firstly a cyber claim and **the Cyber Liability portion** of this policy will cover your costs to stop and remedy the attack as well as the restoring of data. This is applicable even prior to any potential third-party claim because the insured needs to mitigate further loss or damage.
- Cyber Liability: A liability claim where the third party lodging the demand alleges that, due to the attack, their information came into the wrong hands has caused a loss of some kind to them. If the allegation can be proven, **the Cyber Liability portion** of this policy will respond.
- D&O Liability: If it is alleged that the security plan, as required by POPIA, was inadequate, the allegation would imply that the Information Officer failed their statutory of fiduciary duty and is responsible, and therefore the **Directors and Officers cover (D&O)** will respond.