PRIVACY POLICY

(includes POPI Policy, Privacy Notice & PAIA Manual)

August 2021

Skylaw Legal Pty Ltd
Reg No. 2021/816322/07
www.skylaw.co.za / support@skylaw.co.za

Definitions

Company

SKYLAW LEGAL PTY LTD. Registered in the Republic of South Africa with company number: 2021/816322/07

Mobile Platform

An application that is distributed by the Company through AppStore or Google Play

Website Platform

A website that is operated by the Company and available at https://skylaw.co.za/

Platform(s)

Collective name that can refer to either or both the Mobile and Website Platforms

Skylaw

Collective name that can refer to either or both the Platform and the Company

Privacy Policy

Latest version of the Skylaw Privacy Policy

User

An individual user starting at age 18 or a legal entity that has read and agreed to the Terms and Conditions of Skylaw and uses the services of the Company provided through the Mobile or Website Platforms. May or may not have an account with the company.

GDPR

The General Data Protection Regulations applicable in South Africa

KYC or Due Diligence

Procedure done by Skylaw for User information and identity verification purposes according to applicable laws and Anti-Money Laundering policy of the Company

Biometric information

means the physical, physiological or behavioural identification, including fingerprinting, amongst others.

Processing

The collection, receipt, recording organisation, collation, storage, updating, modification, retrieval, alteration, consultation or use;

- Dissemination by means of transmission, distribution or making available in any form;
- Merging, linking, erasure or destruction of information.

PAIA

means the Promotion of Access to Information Act No. 2 of 2000

POPI

means the Protection of Personal Information Act No 4 of 2013

Regulator

means the Information Regulator established in terms of the POPI Act.

Purpose, Scope and Other Definitions

The Policy is meant for use by Skylaw's Users.

Skylaw represents an entity that has prepared the Platform and allows Users to purchase specially selected legal services which are capable of being provided by Skylaw over-the-counter and without ongoing legal assistance.

Skylaw is a company registered in South Africa that has developed and governs the Platform and services, products and content that is accessible through and offered on the Platform.

The Company is compliant with the applicable South African and international laws for the Prevention of Money Laundering and Terrorist Financing, the General Data Processing Regulations, as well as other legislation applicable in South Africa. The Company has established this Privacy Policy in accordance with General Data Processing Regulation and laws, regulations and/or directives issued pursuant to GDPR and other laws.

This policy aims to provide the Company's Users with information on what type of information the Company collects, how it is used and the circumstances in

which it could be shared with third parties. Throughout this privacy statement, User's data may be called either "personal data" or "personal information". The Company may also sometimes collectively refer to handling, collecting, protecting and storing User's personal data or any such action as "processing" of such personal data.

For the purposes of this statement, personal data shall mean any information relating to the User, which identifies or may identify the User and which includes, for example, User's name, address and identification numbers.

Collection of personal data

The Company shall collect information necessary to fulfil legal obligations for the provision of services and to improve its service to you.

Skylaw will gather information and documentation to identify, contact or locate Users and may gather information from third parties and or other sources, which will help it to offer its services effectively.

As a User, an individual is responsible for providing true and accurate information and for keeping the Company informed of any changes in User's personal information or circumstance by emailing Skylaw's support (support@skylaw.co.za).

Purpose of collecting and processing personal data

Collecting and processing user data is done to enable Skylaw to deliver accurate and quality services to the user and in accordance with South African and International laws for the Prevention of Money Laundering and Terrorist Financing. In addition, user data can be used to enhance User support and User's personal data will be used for specific, explicit and legitimate business purposes only.

Performance of contractual obligations

The personal data collected from Users is used to verify User's identity for Due Diligence purposes, to manage User's account on the Platform, to process User's transactions, to provide Users with post-transaction information, to inform Users of additional products and/or services relevant to the User's profile, to produce analysis and statistical data which will help the Company improve its products and services, and improve the Platform.

Identity Verification purposes

The Company needs to perform its Due Diligence process and apply the principles of KYC before entering some business relationships with any User in order to prevent illegal actions, such as money laundering or terrorist financing, and to perform other duties imposed by law.

The Company may collect from its Users identity verification information (such as copies, images or scans of User's government-issued national ID card or international passport, or other government-issued proof of identification) or other authentication information. Skylaw may also request its Users to provide the Company with a recent utility bill in order to verify the User's residential address. Further to this, the Company can use third parties to carry out identity verification on its behalf.

Compliance with legal obligations

There are a number of legal obligations arising from the relevant laws to which the Company is subject, as well as other statutory requirements.

Such obligations and requirements may impose on Skylaw the necessity to perform personal data processing activities for credit checks, identity verification, compliance with court orders, tax law or other reporting obligations and anti-money laundering controls.

Purposes of safeguarding legitimate interests

The Company processes personal data to safeguard legitimate interests pursued by Skylaw or by a third party. A legitimate interest is when Skylaw has a business or commercial reason to use the User's information. Even then, it must not unfairly go against what is right and best for the User.

Examples of such processing activities include:

- initiating court proceedings and preparing our defence in litigation procedures;
- measures and processes we undertake to provide the Company's IT and system security, preventing potential crime, asset security, admittance controls and anti-trespassing measures;
- measures to manage business and further develop the Company's products and services;

- the transfer, assignment (whether outright or as security for obligations) and/or sale to one or more persons and/or charge and/or encumbrance over, any or all of the Company's benefits, rights, title or interest under any agreement between the User and the Company.

Marketing Purposes

The Company may use User data, such as location or transaction history to deliver any news, analysis, research, reports, campaigns or training opportunities that may interest the User, to their registered email address. Users always have the right to change this option if they no longer wish to receive such information.

Controlling and processing User's personal data

Skylaw and any agents that it engages for the purpose of collecting, storing or processing personal data and any third parties acting on the Company's behalf may collect, process and store personal data provided by the User.

Authorised Processor

The company may also use authorised external processors for User data processing based on concluded service agreements, which are governed by instructions from the Company for the protection of User-related data. The agreements are important so that both parties understand their responsibilities and liabilities.

The GDPR sets out what needs to be included in the agreement, which the Company has adhered to; the below is not an exhaustive list of the obligations of all relevant parties;

- such third parties must only act on the written instructions of the Company (unless required by law to act without such instructions);
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- the rights of Users will not be impaired in meeting with GDPR requirements;

- the security of processing, the notification of personal data breaches and data protection impact assessments will not be impaired;
- deletion or return of all personal data as requested at the end of the contract.

Such providers will provide various services as agreed upon with the Company.

Skylaw has a regulatory obligation to supervise and effectively oversee the outsourced functions and to act appropriately when it determines that the service provider is not performing the said functions effectively and in accordance with applicable legislation.

Skylaw may use or disclose personal information without User's consent only in certain circumstances:

1. if required by law or by order of a court, administrative agency, or other government entities;
2. if there are reasonable grounds showing disclosure is necessary to protect the rights, privacy, property, or safety of users or others;
3. if the Company believes the information is related to a breach of an agreement or violation of the law, that has been, is being, or is about to be committed;
4. if it is necessary for fraud protection, risk reduction, or the establishment or collection of funds owed to the Company;
5. if it is necessary to enforce or apply the Terms and Conditions and other agreements, to pursue remedies, or to limit damages to the Company;
6. for other reasons allowed or required by law;
7. if the information is public.

When the Company is required or permitted to disclose information without consent, the Company will not disclose more information than necessary to fulfil the disclosure purpose.

Skylaw urges all Users to maintain confidentially and not share with others their usernames or passwords whether private or as provided by the Company. The Company bears no responsibility for any unlawful or unauthorised use of

Users' personal information due to misuse or misplacement of Users' access codes (i.e. passwords /credentials), negligent or malicious, however conducted.

How the Company treats User's personal data for marketing activities

The Company may process User's personal data to inform Users about products, services or offers that may be of interest to them. The personal data that Skylaw processes for this purpose consists of information Users provide to the Company and data Skylaw collects and/or infers when Users use the services on the Platform, such as information on User's transactions. The Company studies all such information to form a view of what is needed or what may be of interest to the Users.

In some cases, profiling may be used. Profiling is a process where User's data is automatically processed with the aim of evaluating certain personal aspects and further providing the User with targeted marketing information on products.

Skylaw can only use User's personal data to promote its products and services if Skylaw has the User's explicit consent to do so – by clicking the check box when filling out the form to open an account or, in certain cases, if the Company considers that it is in the User's legitimate interest to do so.

Further, Users have the option to choose whether they wish to receive marketing-related emails (Company news, information about campaigns, the Company's newsletter, the Company's strategic report, etc.) sent to the User's provided email address by clicking the relevant check box when filling out the form to open an account.

Users have the right to object at any time to the processing of User's personal data for marketing purposes or unsubscribe from receiving marketing-related emails from the Company, by contacting the Company's User support department at any time by emailing support@skylaw.co.za

Period of keeping User's personal information

The Company will keep User's personal data for:

1. As long as a business relationship exists with the User, either as an individual or a legal entity, which the User is authorised to represent or of which the User is a beneficial owner;

2. Once a business relationship with a User has ended, the Company is required to keep the User's data for a period of five years to meet regulatory and legal requirements. In some cases, this period may be extended.

When the Company no longer needs to keep User's personal data, it will securely delete or destroy it.

User's rights

Users have the right to request copies of their personal data. Information must be provided without delay and within one month of receipt of request at the latest. The Company may extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, it will inform Users within one month of the receipt of request and explain why the extension is necessary.

Skylaw must provide a copy of the information free of charge. However, the Company can charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The fee, if applied, will be based on the administrative cost of providing the information and on delivery expenses if the User requests that the information be delivered in hard copy. If at any time the Company refuses to respond to a request, it will explain why to the User, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and within one month at the latest.

When information is provided:

The Company will first verify the identity of the person making the request, using reasonable means.

When should personal data be rectified?

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

The GDPR provides for a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. Users can make a request for rectification verbally or in writing.

If Skylaw has disclosed the personal data in question to others, it must contact each recipient and inform them of the rectification, unless this proves impossible or involves disproportionate effort. If asked to, the Company must also inform the individuals about these recipients.

How long does the company have to comply with a request for rectification?

The Company must respond within one month.

This can be extended by two months where the request for rectification is complex.

Where the Company does not take action in response to a request for rectification, Skylaw must explain to the individual why this is not done, informing them of their right to complain to the supervisory authority and to a judicial remedy.

User's right to erasure;

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

1. where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;

2. when the individual withdraws consent;

3. when the individual objects to the processing and there is no overriding legitimate interest to continue the processing;

4. when the personal data was unlawfully processed (i.e. otherwise in breach of the GDPR);

5. when the personal data has to be erased in order to comply with a legal obligation;

6. when the personal data is processed in connection with the offer of information society services to a child.

There are some specific circumstances where the right to erasure does not apply and the Company can refuse to execute the request.

When can the Company refuse to comply with a request for erasure?

Skylaw can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

1. to comply with a legal obligation for the performance of a public interest task or exercise of official authority;

2. the exercise or defence of legal claims.

Does the Company have to tell other organisations about erasure of personal data?

If Skylaw has disclosed the personal data in question to others, it must contact each recipient and inform them of the erasure of personal data, unless this proves impossible or involves disproportionate effort. If asked to, the Company must also inform the individuals about these recipients.

User's right to restrict processing

When does the right to restrict processing apply?

The Company will be required to restrict the processing of personal data in the following circumstances:

1. where an individual contests the accuracy of the personal data, the Company should restrict its processing until the individual has verified its accuracy;

2. where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the Company is considering whether the organisation's legitimate grounds override those of the individual;

3. when processing is unlawful, and the individual opposes erasure and requests restriction instead;

4. if the Company no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

The Company may need to review procedures to ensure it is able to determine when it may be required to restrict processing of personal data.

If the Company has disclosed personal data in question to others, it must contact each recipient and inform them of the restriction on processing the personal data, unless this proves impossible or involves disproportionate effort. If asked to, Skylaw must also inform the individuals about these recipients.

User's right to data portability

1. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

2. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

3. It enables consumers to take advantage of applications and services, which can use this data to find them a better deal or help them understand their spending habits.

4. Skylaw will respond without undue delay, and within one month. This can be extended by two months where the request is complex or where the Company may receive a number of requests. Skylaw will inform the individual within one month of receipt of the request and explain why the extension is necessary, if applicable.

5. Where the Company does not take action in response to a request, it will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and within one month at the latest.

User's right to object

Users have the right to object to:

1. processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);

2. direct marketing (including profiling);

3. processing for purposes of scientific/historical research and statistics.

Skylaw will stop processing personal data unless:

1. the Company can demonstrate compelling legitimate grounds for such processing, which override the interests, rights and freedoms of the individual; or

2. the processing is for establishment, exercise or defence of legal claims.

Automated decision-making

In establishing and carrying out a business relationship, the Company generally does not use any automated decision-making. Skylaw may process

some of the User's data automatically, with the goal of assessing certain personal aspects (profiling), in order to enter into or perform a contract with Users for data assessments (including on payment transactions), which are carried out in the context of combating money laundering and fraud. An account may be detected as being used in a way that is unusual for a User or User's business. These measures may also serve to protect Users and their assets or private data.

Geographical area of processing

As a general rule, User data is processed within South Africa.

The transfer and processing of User data outside of South Africa can take place, provided there are appropriate safeguards in place and the actions are made based on a legal basis only.

Upon request, the User may receive further details on User data transfers to countries outside of South Africa.

Other related information

Skylaw uses appropriate technical, organisational and administrative security measures to protect any information it holds in its records from loss, misuse, unauthorised access, disclosure, alteration or destruction. Unfortunately, no company or service can guarantee complete security. Unauthorised entry or use, hardware or software failure and other factors may compromise the security of User information at any time.

Among other practices, User's account is protected by a password for User's privacy and security. Users must prevent unauthorised access to User's account and Personal Information by selecting and protecting User's password carefully and limiting access to User's computer or device and browser by signing off after finishing accessing the User's account.

Transmission of information via regular email exchange is not always completely secure. The Company, however, exercises all possible means to protect Users' personal data; yet it cannot guarantee the security of User data that is transmitted via email; any transmission is at the Users' own risk. Once the Company has received User information it will use procedures and security features in an attempt to prevent unauthorised access.

When Users email the Company (via the "Contact Us" page or by using the Live Chat feature) a person may be requested to provide some additional personal data, like their name or email address. Such data will be used to respond to their query and verify their identity. Emails are stored in the Company's standard internal contact systems which are secure and cannot be accessed by unauthorised external parties.

Raising a concern

Users can be confident that Skylaw handles User's personal information responsibly and in line with good practices.

Users can contact support@skylaw.co.za If a User has a concern about the way the Company handles User's information, or if a User feels the Company may, for example;

- not keep User's information secure;
- hold inaccurate information about the User;
- have disclosed information about the User;
- keep information about the User for longer than is necessary; or
- collect information for one reason and use it for something else.

The Company takes all concerns seriously and will work with the User to resolve any such concerns.

Any concerns and/or requests may be raised with the appointed Data Protection Officer whose contact information is below:

Email: support@skylaw.co.za

The User has the right go to court or to escalate their complaint to the data protection regulator in their jurisdiction for the protection of rights, unless applicable laws prescribe a different procedure for handling such claims.

Changes to this privacy statement

The Company reserves the right to modify or amend this Privacy Statement unilaterally at any time in accordance with this provision.

If any changes are made to this privacy statement, the Company shall notify the Users accordingly. The revision date shown at the end of this page will also be amended. The Company does, however, encourage the Users to review this privacy statement occasionally so as to always be informed about how the Company processes and protects the User's personal information.

Cookies

The Company's website uses small files known as cookies to enhance its functionality and improve User's experience.

A cookie is a small text file that is stored on a User's computer for record-keeping purposes. The Company uses cookies on the Platform(s). Skylaw links the information it stores in cookies to any personally identifiable information the User submits while on the Platform. Skylaw uses both session ID cookies and persistent cookies. A session ID cookie does not expire when the User closes the browser. A persistent cookie remains on User's hard drive for an extended period of time. A User can remove persistent cookies by following directions provided in the User's Internet browser's "help" file.

The Company sets persistent cookies for statistical purposes. Persistent cookies also enable the Company to track and target the location and interests of the Users and to enhance the experience of Company's services on the Platform. If a User rejects cookies, the User may still use the Platform

Some of Company's business partners use cookies on the Platform. The Company has no access to or control over these cookies.

Monitoring and Review

The Company will monitor the effectiveness of this Policy on a regular basis and, in particular, the quality of execution of the procedures explained in the Policy and, where appropriate, it reserves the right to correct any deficiencies.

In addition, the Company will review the Policy at least annually. A review will also be carried out whenever a material change occurs that affects the ability of the Company to continue to the best possible result for the execution of its Users' orders on a consistent basis using the venues included in this Policy.

The Company will inform its Users of any material changes to this Policy by posting an updated version of this Policy on its Website(s).

Policy Statement

Skylaw Legal Pty Ltd processes personal information of its employees, members, clients and other data subjects from time to time. As such, it is obliged to comply with the Protection of Personal Information Act No. 4 of 2013 ("POPI") as well as the Promotion of Access to Information Act No. 2 of 2000 ("PAIA").

In line with this, the Company is committed to protecting its members'/ clients'/ supplier's/ employees' and other data subjects' privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

This Policy sets out the manner in which the Company deals with such personal information and provides clarity on the general purpose for which the information is used, as well as how data subjects can participate in this process in relation to their personal information.

In addition to this policy, the company has also developed a manual and made it available as prescribed under the PAIA Act. Where parties/requesters submit requests for information disclosure in terms of this manual, internal measures have been developed together with adequate systems to process requests for information or access thereto.

Objectives

To ensure legislative compliance (POPI and PAIA Acts) in respect of all personal information that the Company collects and processes.

To inform employees and clients as to how their personal information is used, disclosed and destroyed.

To ensure that personal information is only used for the purpose for which it was collected.

To prevent unauthorised access and use of personal information.

Collection of Personal Information

The Company collects and processes various information pertaining to its employees, members, clients and suppliers. The information collected is based on need and it will be processed for that need/purpose only. Whenever

possible, the Company will inform the relevant party of the information required (mandatory) and which information is deemed optional.

The employee, member or client will be informed of the consequence/s of failing to provide such personal information and any prejudice which may be incurred due to non-disclosure. For example, the Company may not be able to employ an individual without certain personal information relating to that individual or the organisation may not be in a position to render services to a client in the absence of certain information which is required.

The Company will process information in a manner that is lawful and reasonable (i.e., will not infringe the privacy of the individual or company).

Where consent is required for the processing of information, such consent will be obtained.

Information will be processed under the following circumstances:

- When carrying out actions for the conclusion or performance of a contract
- When complying with an obligation imposed by law on the company
- For the protection of a legitimate interest of the data subject
- Where necessary, for pursuing the legitimate interests of the company or of an authorised third party to whom the information is supplied.

Examples of the personal information the Company collects includes, but is not limited to:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of an employee.
- Information relating to the education or the medical, financial, criminal or employment history (this includes disciplinary action) of an employee.
- Banking and account information.
- Contact information.
- Trade union membership and political persuasion.
- Any identifying number, symbol, email address, telephone number, location information, online identifier or other particular assignment to the employee, member or client
- The biometric information of the employee, member, client or data subject
- The personal opinions, views or preferences of an employee (also performance appraisals or correspondence) and the views or opinions of another individual about the person

The Company shall not process special personal information without complying with the specific provisions of the POPI Act. Special information includes personal information concerning:

- the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life or biometric information of a data subject; or
- the criminal behaviour of a data subject, where such information relates to the alleged commission by a data subject of any offence committed or the disposal of such proceedings.

Collection of employee information:

- For the purposes of this Policy, employees include potential, past and existing employees of the Company. Independent contractors are treated on the same basis where the collection of information is concerned.
- When appointing new employees/contractors, the Company requires information, including, but not limited to that listed above, from prospective employees/contractors, in order to process the information on the system/s. Such information is reasonably necessary for the Company's record purposes, as well as to ascertain if the prospective employee/contractor meets the requirements, for the position which he is being appointed/contracted, and is suitable for appointment.
- The Company will use and process such employee information, as set out below for including, but not limited to, its employment records and to make lawful decisions in respect of that employee and its business.
- Use of employee information: Employees' personal information will only be used for the purpose for which it was collected and intended. This includes, but is not limited to:
    - Submissions to the Department of Labour
    - Submissions to the Receiver of Revenue
    - For audit and recordkeeping purposes
    - In connection with legal proceedings
    - In connection with and to comply with legal and regulatory requirements
    - In connection with any administrative functions of the Company
    - Disciplinary action or any other action to address the employee's conduct or capacity.
    - In respect of any employment benefits that the employee is entitled to
    - Pre- and post-employment checks and screening

- Any other relevant purpose to which the employee has been notified.

Should information be processed for any other reason; the employee will be informed accordingly.

Collection of Member / Client/Supplier information:

- For purposes of this Policy, clients include potential, past and existing members and clients. Suppliers include all vendors which contract with the Company, whether once off or recurring, in respect of products and services.

The Company collects and processes its members', clients' and suppliers' personal information, such as that mentioned hereunder. The type of information will depend on the need for which it is collected and will be processed for that purpose only. Further examples of personal information collected from clients include, but is not limited to:

- The member/client/supplier's identity number, name, surname, address, postal code
- The member/client/supplier's residential and postal address
- Contact information
- Banking details
- Company registration number
- Full name of the legal entity
- Tax and/or VAT number
- Details of the person responsible for the client's/supplier's account

The Company also collects and processes member/clients personal information for marketing purposes in order to ensure that its products and services remain relevant to our clients and potential clients.

Use of member/client/supplier information:

- The member/client/supplier's personal information will only be used for the purpose for which it was collected and as agreed. This may include, but not be limited to:
- Providing products or services to members/clients
- In connection with sending accounts and communication to a member/client in respect of services rendered.

- Payment of suppliers and communication in respect of services rendered.
- Referral to other service providers
- Confirming, verifying and updating member/client/supplier details
- Conducting market or customer satisfaction research
- For audit and record keeping purposes
- In connection with legal proceedings
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

Disclosure of personal information

- The Company may share employees' and member/clients/suppliers' personal information with authorised third parties as well as obtain information from such third parties for reasons set out above.
- The Company may also disclose employees' or member/clients/suppliers' information where there is a duty or a right to disclose in terms of applicable legislation, the law or where it may be necessary to protect the rights of the organisation or it is in the interests of the data subject.

Safeguarding Personal Information

The Company shall review its security controls and processes on a regular basis to ensure that personal information is secure.

It will take appropriate, reasonable technical and organisational measures to prevent loss or damage or unauthorised destruction of personal information, and unlawful access to or processing of personal information. This will be achieved by –

- Identifying internal and external risks
- Establishing and maintaining appropriate safeguards
- Regularly verifying these safeguards and their implementation
- Updating the safeguards
- Implementing generally accepted information security practices and procedures.

The Company shall appoint an Information Officer and Deputy Information Officer who is/are responsible for compliance with the conditions of the lawful processing of personal information and other provisions of POPI.

Information Officer details:

- Name: Johann Joosten, Director
- Telephone number: On Request Per Email or Contact Us Page
- Postal address: On Request Per Email or Contact Us Page
- Physical address: On Request Per Email or Contact Us Page
- Email address: support@skylaw.co.za

Deputy Information Officer - None

The specific responsibilities of the Information Officer and his/her Deputy include –

- The development, implementation, monitoring and maintenance of a compliance framework.
- The undertaking of a personal information impact assessment to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.
- The development, monitoring and maintenance of a manual, as well as the making available thereof, as prescribed in section 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
- The development of internal measures, together with adequate systems to process requests for information or access thereto; and
- To ensure that company staff awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.

Employment contracts/addendums thereto, containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI are signed by every employee.

On an ongoing basis, all suppliers, insurers and other third-party service providers are required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information.

Consent to process client/member/supplier information is obtained from clients/members/suppliers (or a person who has been given authorisation from

the client/member to provide the member/client's personal information) and suppliers at sign on/appointment/contracting.

Direct Marketing

The company shall ensure that:

- It does not process any personal information for the purpose of direct marketing (by means of any form of electronic communication, including automatic calling machines, SMS's or e-mail) unless the data subject has given his, her or its consent to the processing or is an existing customer.
- It will only approach data subjects, whose consent is required and who have not previously withheld such consent, once in order to request the consent. This will be done in the prescribed manner and form.
- The data subjects will only be approached for the purpose of direct marketing of the Company's own similar products or services. In all instances, the data subject shall be given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details at the time when the information is collected.
- Any communication for the purpose of direct marketing will contain details of the identity of the sender or the person on whose behalf the communication has been sent and an address or other contact details to which the recipient may send a request that such communications cease.

Transfer of Information outside of South Africa

The Company will not transfer personal information about a data subject to a third party who is in a foreign country unless one or more of the following apply:

- the third party is subject to a law, binding corporate rules or a binding agreement which provides an adequate level of protection of personal information and effectively upholds principles for reasonable processing of the information.
- the data subject consents to the transfer
- the transfer is necessary for the performance of a contract between the data subject and
- the company

- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the company and a third party; or
- the transfer is for the benefit of the data subject, and it is not reasonably practicable to obtain the consent of the data subject to that transfer and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

Surveillance Systems

Video footage and/or voice/telephone calls that have been recorded, processed and stored via CCTV camera or other surveillance systems constitute personal information. As such the Company will make all employees, members, clients or data subjects aware as to the use of CCTV/other surveillance on the premises.

Security Breaches

Should the Company detect a security breach on any of its systems that contain personal information, it shall take the required steps to assess the nature and extent of the breach in order to ascertain if any information has been compromised.

The Company shall notify the affected parties should it have reason to believe that their information has been compromised. Such notification shall only be made where the organisation can identify the data subject to which the information relates. Where it is not possible it may be necessary to consider website publication and whatever else the Information Regulator prescribes.

Notification will be provided in writing by means of either:

- email
- registered mail
- the organisation's website

The notification shall provide the following information where possible:

- Description of possible consequences of the breach
- Measures taken to address the breach
- Recommendations to be taken by the data subject to mitigate adverse effects.

- The identity of the party responsible for the breach

In addition to the above, the Company shall notify the Regulator of any breach and/or compromise to personal information in its possession and work closely with and comply with any recommendations issued by the Regulator.

The following will apply in this regard:

- The Information Officer will be responsible for overseeing the investigation.
- The Information Officer will be responsible for reporting to the Information Regulator within 3 working days of a breach/ compromise to personal information.
- The Information Officer will be responsible for reporting to the Data Subject(s) within 3 working days, as far as is reasonable and practicable, of a breach/ compromise to personal information.
- The timeframes above are guidelines and depending on the merits of the situation may require earlier or later reporting.

Access and Correction of Personal Information

Employees and members/clients have the right to request access to any personal information that the Company holds about them.

Employees and members/clients have the right to request the Company to update, correct or delete their personal information on reasonable grounds. Such requests must be made to the Information Officer (see details above).

Where an employee or member/client objects to the processing of their personal information, the Company may no longer process said personal information. The consequences of the failure to give consent to process the personal information must be set out before the employee or client confirms his/her objection.

The member/client or employee must provide reasons for the objection to the processing of his/her personal information.

Head office details:

Name: Skylaw Legal Pty Ltd

10.4.3. Telephone number: available on request

10.4.4. Postal address: available on request

10.4.5. Physical address: available on request

10.4.6. Email address: support@skylaw.co.za

Retention of Records

The Company is obligated to retain certain information, as prescribed by law. This includes but is not limited to the following:

- With regard to the Companies Act, No. 71 of 2008 and the Companies Amendment Act No 3 of 2011, hard copies of the documents mentioned below must be retained for 7 years:
- Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act.
- Notice and minutes of all meetings, including resolutions adopted.
- Copies of reports presented at the annual general meeting.
- Copies of annual financial statements required by the Act and copies of accounting records as required by the Act.

The Basic Conditions of Employment No. 75 of 1997, as amended, requires the organisation to retain records relating to its staff for a period of no less than 3 years.

Requests for Information

In terms of requests to be processed under POPI, the following forms shall be used –

- Objection to the processing of personal information – A data subject who wishes to object to the processing of personal information in terms of section 11(3)(a) of the Act, must submit the objection to the responsible party on Form 1, which form can be requested directly from the information officer listed above.
- Request for correction or deletion of personal information or destruction or deletion of record of personal information – A data subject who wishes to request a correction or deletion of personal information or the destruction or deletion of a record of personal information in terms of section 24(1) of the Act, must submit a request to the responsible party on Form 2, which form can be requested directly from the information officer listed above.

- Request for data subject's consent to process personal information – A responsible party who wishes to process personal information of a data subject for the purpose of direct marketing by electronic communication must submit a request for written consent to that data subject, on Form 3, which form can be requested directly from the information officer listed above.
- Submission of complaint – Any person who wishes to submit a complaint contemplated in section 74(1) of the Act must submit such a complaint to the Regulator on Part I of Form 4. A responsible party or a data subject who wishes to submit a complaint contemplated in section 74(2) of the Act must submit such a complaint to the Regulator on Part II of Form 4, which form can be requested directly from the information officer listed above.

In terms of requests for information under PAIA, the provisions of the PAIA Manual must be complied with and Form 1 of the PAIA Manual forms must be completed, which form can be requested directly from the information officer listed above.

Any requests and/ or advice can be directed to the Information Officer set out in this policy.