designhygiene	Quality Management System **Data Privacy Policy**

Document Type	Human Resources Policy
Area of Application	All Employees of Design Hygiene (Pty) Ltd.
Purpose	To provide clarity to anyone who may come into contact with or be responsible for the processing of personal information in any format whatsoever, during the scope of their duties and to detail the actions they should take in order to keep all personal information safe.

DOCUMENT METADATA

Document number:	0001
Document version:	0003
Document approval authority:	INFORMATION OFFICER
Document approval date:	30 JUNE 2021
Document owner:	INFORMATION OFFICER
Document author(s):	INFORMATION OFFICER
Last updated:	30 JUNE 2021
Next review date:	30 JUNE 2022
Visibility (where will it be displayed):	RECEPTION

Data Privacy Policy

Table of Contents

DOCUMENT METADATA 1

1. WHY WE HAVE THIS POLICY 3
2. THE SCOPE OF THIS POLICY 3
3. WHY IT IS IMPORTANT TO COMPLY WITH THIS POLICY 3
4. DEFINITIONS 3
5. OUR POLICY 7
6. ROLES AND RESPONSIBILITIES 12
7. SUPPORTING DOCUMENTS 14
8. REVIEW 14

1. WHY WE HAVE THIS POLICY

Data protection matters, not only to our organisation, but to our stakeholders on a personal level as well. Although compliance is vital, this is not the only motivation that we should consider when ensuring that protection of data is always a priority for all who may have access to or come into contact with personal information of any kind.

At Design Hygiene we value the trust that our stakeholders place in us when they share their personal information with us. Personal information is essential for our business to function effectively, so it is crucial that we protect it in accordance with the guidelines set out in the Protection of Personal Information Act (POPIA) and other relevant privacy regulations.

This policy is intended to provide clarity to anyone who may come into contact with or be responsible for the processing of personal information in any format whatsoever, during the scope of their duties and to detail the actions they should take in order to keep all personal information safe. Not only is it imperative to our reputation to ensure compliance with all data protection legislation, but it is also an ethical requirement to protect the information that our employees, job applicants, customers/clients, prospective customers/clients, contractors, service providers, suppliers, business associates, shareholders, directors, visitors to our premises and members of the public entrust us with.

2. THE SCOPE OF THIS POLICY

This policy applies to:

- any activity where we produce or use personal information (processing activities);
- anybody involved in processing activities where we produce or use personal information; and
- all employees, service providers, contractors, and other individuals who have any form of access to personal information in any format whatsoever.

3. WHY IT IS IMPORTANT TO COMPLY WITH THIS POLICY

Our reputation is our biggest asset. Without our reputation, our relationships with key stakeholders and investors would suffer, and we could lose clients, prospective clients, and top-class candidates. We could also face substantial fines. The ongoing protection of information within the organisation is therefore the responsibility of everyone, given that any negative implications would directly affect all stakeholders.

If the company does not comply:

- Far reaching consequences for our business which will negatively impact our data integrity, and our reputation.
- Financial impact - substantial fines negatively impacting the finances of the organisation which could lead to possible retrenchments.
- More severe penalties i.e. imprisonment, permanent reputational damage and permanent loss of business.

If you do not comply:

- You could face disciplinary action in terms of our Disciplinary Code and Procedure if you do not comply with this policy, or if you discover that we are not complying with the policy and you fail report it to us immediately;
- possible job losses due to loss of business and negative financial impact;

5. DEFINITIONS

POPIA	means The Protection of Personal Information Act 4 of 2013 and its related regulations
POPIA Programme	the POPIA programme is the company's ongoing efforts to comply with the provisions of the POPIA and include: • Stakeholder consultation • Clearly defining roles and responsibilities • Policy development • Policy implementation • Monitoring and audit; and • Continuous improvement
Data Subjects	For the purpose of this policy includes all identifiable natural or juristic persons about whom the Company holds personal information or special personal information including, but not limited to: • Customers / Clients; • Prospective Customers / Clients; • Employees;

- Job applicants;
- Consumers (natural and juristic persons);
- Contractors, Service Providers, Suppliers;
- Business Associates;
- Shareholders and directors; and
- Visitors to our premises and members of the public.

Operator	means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under direct authority of that party.
Responsible Party	means 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.
Information Regulator	means an independent body established in terms of section 39 of the Protection of Personal Information Act 4 of 2013. It is, among others, empowered to monitor and enforce compliance by public and private bodies with the provisions of the POPIA Act.
Personal Information	means personal information relating to an identifiable, living natural person and where it is identifiable, existing juristic persons, including but not limited to.

- Information relating to the race, gender, sex, identifiers such as name, identity number, employee number, account number, customer number, company registration number, tax number, photographs, videos, or any other unique information that may be used to identify a person;
- biometric information – this relates to the techniques of identification that are based on physical, physiological, or behavioural characteristics, such as fingerprints, blood-type, DNA analysis, retinal scans, facial and voice recognition;

- demographic information such as race, gender, pregnancy, marital status, age, culture, language and birth;
- Information relating to physical or mental health, well-being or disability;
- background information such as education, financial, employment, medical, criminal or credit history;
- contact details – physical / postal address, telephone number(s), email address(es), online identifier (i.e. twitter handle), or location information;
- an individual's preferences, opinions and views;
- confidential or private correspondence and any correspondence that would reveal the contents of the original correspondence;
- views and opinions about an individual like trade references, job references, performance reviews and interview notes;

Special / Sensitive Personal Information

means information about an individual that pertains to racial or ethnic origins, political, religious, or philosophical beliefs, health or sexual life, trade union membership or political persuasion, biometric information, or criminal behaviour (to the extent that such criminal behaviour relates to the alleged commission by a data subject of an offence or any proceedings in respect of any offense allegedly committed by a data subject).

Sensitive Personal Information may only be processed under strict conditions and will usually require the **express written consent** of the data subject.

Processing:

means any operation or activity, whether or not by automatic means, concerning personal information, including but not limited to:

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

- dissemination by means of transmission, distribution or making available in any other form; or
- merging, linking, as well as restriction, degradation, erasing or destruction of information.

Processing Activities means a collection of interrelated work tasks that achieve a specific result during which personal information is created, collected, used, shared, transformed, stored or deleted / destroyed.

Processing activities are important if stopping or disrupting the process or activity could cause the Company to experience critical or high levels of risk and / or loss.

Incident Means

- non-compliance with this policy and any procedures relating hereto;
- contravention of any data protection legislation such as the POPIA; and
- security incidents such as breaches of confidentiality, failures of integrity or interruptions to the availability of personal information required for business continuity.

6. OUR POLICY

6.1. Everyone has rights regarding how their personal information is handled, processed, stored, shared, protected, and disposed of when its purpose has been fulfilled. In the course of carrying out its business and providing its services the Company may collect, store and process personal information of Data Subjects as detailed in the definitions of this document.

6.2. While all personal information should be protected, we take a risk-based approach to compliance. We prioritise the protection of personal information that is used in our important business activities, and in activities that could have a substantial impact on a data subject's right to privacy.

6.3. Personal information which may be held on paper or in electronic format or other media, is subject to certain legal safeguards specified in the Protection of Personal Information Act ("POPI") and as well as other applicable acts and regulations. The POPI Act imposes restrictions on how the Company may collect and process the information.

6.4. It is our policy to:

6.4.1. Follow all principles of privacy protection as set out in the POPI Act; and

6.4.2. Conduct data protection impact assessments.

THE PRINCIPLE	**WHAT WE DO**
Classify Personal Information:	We identify and classify the personal information we use and produce.
Document Processing Activities:	We document all processing activities to ensure that we can respond to requests from the Information Regulator and from data subjects and other third parties.
Specify the Purpose for Processing:	We both specify and document the purpose for which we process information.
Provide a legal basis for processing activities:	We ensure that: • All processing activities have a legal basis; and • We document the specific legal basis for processing personal information for each activity.
Keep processing to a minimum:	We ensure that: • We process personal information that is adequate, relevant and not excessive, considering the purpose of the activity; and • We de-identify personal information before we start the activity where possible. Where de-identification is not possible, we must consider masking the personal information.

Obtain personal information only from lawful sources:	We obtain personal information from lawful sources only. Lawful sources of personal information include: • The data subject; • Information that the data subject made public deliberately; • Public records; and • A source that the data subject consented to. Other sources may be lawful in special circumstances. If you are unsure always check with the Information / Deputy Information Officer prior to processing.
Process transparently:	We disclose all processing activities to data subjects in our privacy notices
Ensure personal information quality:	We take reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated when necessary.
Limit Information Sharing:	We only share personal information if it is legal to do so and ethically justifiable. We: • Identify all instances when personal information is shared with external individuals or organisations (third parties); • Ensure that sharing personal information complies with all data protection legislation and the Information Sharing Procedure; • Enter into appropriate contracts and take additional steps that may be necessary to reduce the risk created by sharing personal information; • Conduct an information sharing assessment to determine who is responsible to ensure that contracts are concluded, who must review the contracts, and whether we must take additional steps to reduce the risks created by sharing; • Keep records of personal information sharing activities, including the outcome of assessments, a record of additional steps taken, what personal information was shared and when, and the method we used to share the personal information.

Keep personal information secure:	We protect all personal information that we use and produce against breaches or confidentiality, failures of integrity, or interruptions to the availability of that information. All personal information processing must comply with our Information Security Management Policy (ISM).
Manage personal information incidents:	All employees must report incidents in accordance with our Information Security Management Policy and Incident Management Procedure: An incident includes: • Non-compliance with this policy and any procedures that relate to it; • Contraventions of any data protection legislation such as the POPI Act; and • Security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information. Employees must immediately report: • Any known or suspected incidents; or • Any circumstances that increase the risk of an incident occurring. Reports must be sent to: Gray@designhygiene.co.za
Manage retention periods:	We ensure that all records: • Are managed appropriately and in accordance with any operational or legal rules that may apply; and • Comply with our Records Management Policy.
Respect data subjects' rights:	We respect the rights of data subjects to: • Access their records; • Know who their information was shared with • Correct or delete inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or illegally obtained information; • Withdraw consent; and • Object to the processing of their information when it is not necessary for the conclusion or performance

	of a contract or to comply with an obligation imposed by law. All data subject requests must be made using the "Request for Access Form" (PAIA Form C - Request for Access to Record of a Private Body (Section 53(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)) [Regulation 10]) and all information must be verified prior to any information being released.

6.5. We conduct personal information impact assessments

6.5.1. Senior Management must ensure that a personal information impact assessment is done before we start a new processing activity. The data protection impact assessment must include a risk of the activity.

6.5.2. We must conduct a personal information impact assessment before we:

6.5.2.1. continue to process personal information as part of an activity that has not undergone data protection impact assessment before;

6.5.2.2. change an existing processing activity;

6.5.2.3. launch a new product or service;

6.5.2.4. expand into other countries;

6.5.2.5. use new systems or software for processing personal information; or

6.5.2.6. share personal information with third parties.

6.5.3. A personal information impact assessment has three phases:

6.5.3.1. Identify activities in which personal information is processed.

6.5.3.2. Complete the data protection impact assessment questionnaire to document the activity, classify information, and perform a risk-rating for the activity.

6.5.3.3. Complete a further investigation and assessment with assistance from the Deputy Information Officer if the activity had a risk rating

of high or critical after the data protection impact assessment questionnaire was completed.

6.5.4. All activities that are rated as critical or high risk during the data protection impact assessment must undergo an assessment every three years.

7. ROLES AND RESPONSIBILITIES

These are the responsibilities in respect of this policy

The Information Officer (The MD)	The Managing Director (MD) is our Information Officer. The Information Officer has a coordinating function that focuses on the policy-based protection of our information and is the policy owner of this policy. The Information Officer must ensure that this policy receives support from senior management throughout the organisation and that senior management discharges their responsibilities.
Deputy Information Officer(s)	Deputy Information Officer(s) must support the Information Officer and are responsible for strategic guidance to the organisation on data privacy risk management. The Deputy Information Officer(s) must: • oversee the implementation of this policy; • develop procedures and standards to support data- privacy; • provide advice on the identification and management of data privacy risk; • monitor whether personal information impact assessments are performed when required; • develop training on this data privacy; • respond to data subject requests and objections; • respond to requests from the information regulators and working with regulators when there is an investigation; • monitor whether this policy is implemented throughout the organisation.
Manager of IT	The Manager of IT supports the Information Officer and the Deputy Information Officer(s) by: • developing Information Technology policies, procedures, standards and guidelines; • providing technical advice on data privacy; • supporting the implementation of this policy through appropriate technology investments;

	• ensuring that the organisation only invests in information technology that complies with this policy.
Head of Legal	The Head of Legal: • oversees the management of data privacy-related legal obligations; • ensures that the appropriate contracts with third parties concluded; • ensures that employees are aware of contractual obligations and their responsibilities; • provides legal advice on the interpretation of legislation; and • manages legal risks and provides legal advice when an incident occurs.
Head of HR	The Head of HR: • assists the Information Officer and Deputy Information Officer(s) with the ongoing implementation and adherence to the POPIA framework within the context of HR data privacy; • demonstrates an understanding of the impact of the Protection of Personal Information Act on the processing of HR information; • communicates the key aspects of the Protection of Personal Information Act that impact HR to the HR team; • articulates the HR activities that require attention as a result of the Protection of Personal Information Act; • clarifies and monitors the responsibilities of HR personnel involved in the processing of personal information; • develops and implements a compliance framework for the protection of personal information within the HR function; • performs privacy impact assessments as required; • develops a privacy plan for HR information; • monitors the compliance framework for privacy in HR.
Senior Management	Senior Management must implement this policy, create or align other policies and processes in their business areas with this policy, and monitor and advocate for compliance within their business areas. Senior Management must ensure that: • business areas comply with this policy;

	• a register of information assets used in important information processing activities in their business area is created and maintained; • information used in important information processing activities is classified; • personal information impact assessments are conducted before confidential and personal information is processed; • data privacy-related risks in their business area are managed; and • their business area participates in investigations into incidents.
Users of information	All users who have access to the organisations' information or information systems must: • adhere to all policies, procedures and guidelines that relate to the use of information; and • report any actual or suspected incidents.
Internal and external audit	Internal and external audit provides independent assurance that the organisation's risk management, governance and internal control processes are operating effectively, including compliance with this policy.

8. SUPPORTING DOCUMENTS

- Data Subject Request Procedure and Document
- Personal Information Impact Assessment Procedure and assessment

9. REVIEW

This document shall be reviewed annually by the Information Officer, who is the owner of this document, and updated with any new legislation to ensure that it remains fit for purpose.