| Policy | General Processing of Personal Information |
|---|---|
| Applicable to | All employees |
| Person responsible | Information Officer |
| Document No. | POL # |

**Dirty Lolli Apparel Pty Ltd Compliance Policy – Protection of Personal Information Act**

**1. Purpose:**

1.1 The purpose of this policy is to establish a Compliance Framework for Dirty Lolli Apparel Pty Ltd to ensure compliance with the Protection of Personal Information Act 4 of 2013.

**2. Definitions:**

2.1. **"automated means":** means any equipment capable of operating automatically in response to instructions given for the purpose of processing information.
2.2. **"automatic calling machine":** means a machine that is able to do automated calls without human intervention.
2.3. **"binding corporate rules":** means personal information processing policies, within a group of undertakings, which are adhered to by the business or operation within that group of undertakings when transferring personal information to a business or operator within that same group of undertakings in a foreign country.
2.4. **"data subject":** means the person to whom personal information relates.
2.5. **"direct marketing":** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

a) Promoting or offering to supply, in the ordinary course of business, any goods or service to the data subject; or
b) Requesting the data subject to make a donation of any kind for any reason.

2.6. **"electronic communication":** means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
2.7. **"filing system":** means any structured set of personal information, whether centralised, decentralised dispersed on a functional or geographical basis, which is accessible according to specific criteria.
2.8. **"group undertakings":** means a controlling undertaking and its controlled undertakings.
2.9. **"information officer":** of, or in relation to, a –

a) Public body means an information officer or deputy information officer as contemplated in terms of Section 1 or 17 of this Act; or
b) Private body means the head of a private body as contemplated in Section 1, of The Promotion of Access to Information Act.

2.10. **"operator":** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
2.11. **"person":** means a natural person or a juristic person.
2.12. **"personal information":** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

a) 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 the person;
b) Information relating to the education or the medical, financial, criminal or employment history of the person;

c) Any identifying number, symbol, e-mail address, telephone number, location information, online identifier or other particular assignment to the person;
d) The biometric information of the person;
e) The personal opinions, views or preferences of the person;
f) Correspondence sent by the person that would reveal the contents of the original correspondence;
g) The views or opinions of another individual about the person; and
h) The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.13**. "private body":** means –
a) A natural person who carries or has carried on any trade, business or profession, but only in such capacity;
b) A partnership which carries or has carried on any trade, business or profession; or
c) Any former or existing juristic person, but excludes a public body.

2.14**. "processing":** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –
a) The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
b) Dissemination by means of transmission, distribution or making available in any other form; or
c) Merging, linking, as well as restriction, degradation, erasure or destruction of information.

2.15**. "Promotion of Access to Information Act":** means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).

2.16**. "public body":** means –
a) Any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
b) Any other functionary or institution when –
    I. Exercising a power or performing a duty in terms of the Constitution or a Provincial Constitution; or
    II. Exercising a public power or performing a public function in terms of any legislation.

2.17**. "public record":** means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

2.18**. "record":** means any recorded information –
a) Regardless of form or medium, including any of the following:
    I. Writing on any material;
    II. Information produced, recorded or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently divided from information so produced, recorded or stored;
    III. Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
    IV. Book, map, plan, graph, or drawing;

V. Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

b) In the possession or under the control of a responsible party; and

c) Regardless of when it came into existence.

2.19. **"re-identify":** in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that –

a) Identifies the data subject;

b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

c) Can be linked by a reasonably foresee ably method to other information that identifies the data subject.

2.20. **"re-identified":** has a corresponding meaning.

2.21. **"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.

2.22. **"restriction":** means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information.

2.23 **"Dirty Lolli Apparel Pty Ltd":** means Insert if this policy applies to a Group of Companies;

2.24. **"special personal information":** means personal information as referred to in Section 26 of this Act.

2.25. **"terrorist and related activities":** means those activities referred to in Section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004.

2.26. **"this Act":** means the Protection of Personal Information Act, No. 4 of 2013.

2.27. **"unique identifier":** means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

## 3. Policy Statement:

3.1 Dirty Lolli Apparel Pty Ltd recognises its accountability in terms of the Protection of Personal Information Act, together with its Regulations to all its stakeholders. Dirty Lolli Apparel Pty Ltd needs to collect personal information from its employees, clients, suppliers, operators as well as other stakeholders to carry out its business.

To maintain a trust relationship with our stakeholders, we are committed to complying with both the spirit and the letter of this Act and to act with due skill, care, and diligence when dealing with personal information. This is to mitigate the risk, which may include loss of reputation, fines, imprisonment, and exodus of clients.

The responsibility to facilitate compliance throughout Dirty Lolli Apparel Pty Ltd (Pty) Ltd has been delegated to the appointed Information officer and his or her deputies who have the responsibility for supervising, managing, and overseeing the compliance of this Act. However, it must be emphasised that the primary responsibility for complying with this Act lies with all members of staff dealing with personal information. All staff must therefore understand their responsibility in terms of this act as well as with the compliance manual and/or guidance notes and ensure that they are applied when processing personal information.

The compliance policy sets out the approach to managing the compliance risks faced by the organisation.

Any breach of this compliance policy is considered serious and may result in disciplinary action that could ultimately lead to the dismissal of the offender.

### 3.2 **Breaches of this Policy and Reporting lines**

3.2.1 Any Employee who is part, or becomes aware of a Data breach must report to his or her respective departmental manager/Deputy Information Officer.

3.2.2 The Deputy Information Officer reports to the Information Officer

3.2.3 The Information Officer reports to the Managing Director and the Board of Directors to the Information Regulator.

### 3.3 **Roles and Responsibilities**

3.3.1 The information officer has to ensure this policy is followed by each employee through the support of all management levels who must discharge their responsibilities.

3.3.2 The Deputy Information Officer(s) must support the Information Officer in his duty to ensure data privacy risk management.

The Deputy Information Officer must:

- Ensure the implementation of this policy in all business areas;
- Develop Standard Operating Procedures for their department;
- Monitor whether this policy is implemented in their department or organization.
- Respond to data subject requests and objections subject to paragraph 3.2 above.
- Respond to requests from the Information Regulator and work with the Information Regulator subject to paragraph 3.2 above.

3.3.3 The Head of IT supports the Information Officer and the Deputy Information Officers by:

- Developing IT policies, procedures, standards, and guidelines;
- Provide technical support;
- Support the implementation of this policy through appropriate technology investments which comply with this policy;

## 4. Compliance principles

**A. The Information Officer must ensure that the business adheres to the following conditions for the lawful processing of personal information in terms of the Protection of Personal Information Act:**

4.1 Condition 1: Accountability

4.1.1 The business must ensure that the conditions of lawful processing of personal information and all measures that give effect to such conditions are complied with at all times.

4.2 Condition 2: Processing Limitation

4.2.1 Personal information must be processed in a lawful and reasonable manner that does not infringe the privacy of the data subject.

4.2.2 Personal information may only be processed providing the purpose for which it is processed, it is adequate, relevant, and not excessive;

4.2.3 You may only process and access information as is allowed for in order to perform your duties in terms of your employment function.

4.2.4 Information may not be accessed, stored, or distributed other than is required by your employment function.

4.2.5 You may only process personal in following legal or contractual obligations, to achieve business goals, alternatively with the consent of the data subject after the purpose has been explained to the data subject, who confirmed that the purpose is understood. You may also process information when the processing is in the legitimate interest of the data subject, the business or a third party.

4.2.6 Information must be collected directly from the data subject where possible. If personal information is collected from another source, the data subject must be advised thereof, and the purpose for the collection.

4.3 Condition 3: Purpose Specification

4.3.1 The business may only collect personal information for a specific, explicitly defined, and lawful purpose that relates to the function or activity of the business.

4.3.2 It is the employees' instruction to ensure the data subject is made aware of the purpose for which his/her/its personal information is processed.

4.3.3 Each employee may only destroy and/or de-identify personal information as is allowed for by this policy, as well as the data destruction policy and the data retention policy.

4.4 Condition 4: Further Processing Limits:

4.4.1 If information is processed for any other purpose other than the reason why the information was originally collected, then permission for such further processing must be granted by the Information Officer in writing if the further processing is allowed in terms of the Act.

4.4.2 To assess whether further processing is compatible with the purpose of collection, the business must take account of –

a) The relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

b) The nature of the information concerned;

c) The consequences for the data subject's intended further processing of his, her or its personal information;

d) The manner in which the personal information has been collected from the data subject; and

e) Any contractual rights and obligations bestowed on the parties.

4.5 Condition 5: Information Quality:

4.5.1 Information must be kept complete, accurate, must not be misleading, and must be updated where necessary.

4.5.2 If you become aware that a data subject's details have changed, notice must be sent to (add your procedure) who must advise the relevant department of the changes.

4.6 Condition 6: Openness:

4.6.1 When Dirty Lolli Apparel Pty Ltd collects personal information, reasonable practicable steps must be taken to ensure that the data subject is aware that the personal information is being collected in line with this and other related policies.

4.7 Condition 7: Security Safeguards:

4.7.1 Each employee of Dirty Lolli Apparel Pty Ltd must secure the integrity and confidentiality of all personal information this is in its or under its control to prevent –

a) The loss of, damage to, or unauthorised destruction of personal information; and

b) The unlawful access to or processing of personal information.

4.7.3 When sharing personal information with an operator, the employee must ensure that an Operator's Agreement is entered into with the operator that must make provision for the following:

a) The operator must have sufficient security measures in place;

b) The operator must notify Dirty Lolli Apparel Pty Ltd immediately of any suspected security compromise;

c) Internal responsibility for information security management;

d) Devoting adequate personnel resources to information security;

e) Carrying out verification checks on permanent staff who will have access to the personal information;

f) Requiring employees, vendors, and others with access to personal information to enter into written confidentiality agreements, and

g) Conduct training to make employees and others with access to personal information aware of information security risks presented by the Processing.

4.8 Condition 8: Data Subject Participation:

4.8.1 When a data subject provides sufficient proof of identity (for example copy of an ID document of Driver's License) the data subject is entitled to:

a) Confirmation whether the company holds information of the data subject,

b) access to that information;

c) be advised of his/her/it's right to request the correction or deletion of personal information;

d) confirmation of what action was taken in response to their request.

4.9 To comply with these principles, you must consider the following policies, procedure and management tools:

a) Internal Privacy Notice

b) Privacy Notice

c) Data Mapping

d) PAIA Manual

e) Impact Assessment

f) Standard Operating Procedures

g) Assessment

h) Operators Agreements

i) Incident response Policy

j) Clean Desk Policy

k) Data Retention Policy

l) Data Destruction Policy

**B. <u>The business must adhere to the following provisions of the Protection of Personal Information Act when Special Personal Information is being processed.</u>**

4.10 Prohibition on the processing of personal information

4.10.1 The Business will not process personal information, concerning –

a) The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

b) The criminal behaviour of a data subject to the extent that such information relates to –

I. The alleged commission by a data subject of any offence; or

II. Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings;

unless such processing is justified as follows:

- The Data Subject has consented to process it (in circumstances where we are legally obliged to obtain the data subject's consent); or
- It is necessary to exercise or defend a right or obligation in law; or
- It is necessary to comply with an international legal obligation of public interest; or
- It is for historical, research, or statistical purposes that would not adversely affect your privacy; or
- You have deliberately made your personal information public.

**C. <u>The business must adhere to the following provisions of the Protection of Personal Information Act when processing Personal Information of Children</u>**

4.11 Prohibition on processing personal information of children

4.11.1 It is important to note that the business may not process personal information concerning a child.

4.11.2 In terms of this Act a "child", means a natural person under the age of 18 years who is not legally competent when determining the parameters of the processing of personal information of children.

Unless such processing is:

- Carried out with the prior consent of a competent person;
- Necessary for the establishment, exercise, or defence of a right or obligation in law;
- Necessary to comply with an obligation of international public law;

- For historical, statistical, or research purposes to the extent that –
- the purpose serves a public interest and the processing is necessary for the purpose concerned; or
- it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or
- Of personal information which has deliberately been made public by the child with the consent of a competent person.

**D. <u>The business must adhere to the following provisions of the Protection of Personal Information Act when Marketing Directly to a Data Subject through unsolicited electronic communication</u>**

4.12.1 The processing of personal information of a data subject for the purpose of direct marketing through any form of electronic communication, including automatic calling machines, facsimile machines, SMSs, or e-mail is prohibited unless the data subject –

a) has given his, her or its consent to the processing; or

b) is a customer of the business.

4.12.2 The business may approach a data subject only once to request the consent of that data subject and only if the data subject has not previously withheld such consent.

4.12.3 The data subject's consent must be requested in the prescribed manner and form 4 to the Regulations.

4.12.4 The business may only process the personal information of a data subject who is a customer of the business if –

a) the business has obtained the contact details of the data subject in the context of the sale of a product or service;
b) the purpose of direct marketing is through the business's own similar products or services; and
c) the data subject has been 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 –
    I. at the time when the information was collected; and
    II. on the occasion of each communication with the data subject for the purpose of direct marketing if the data subject has not initially refused such use.

4.12.5 Any communication for the purpose of direct marketing must contain –

a) details of the identity of the sender or the person on whose behalf the communication has been sent; and
b) an address or other contact details to which the recipient may send a request that such communications cease.

**E. <u>The business must adhere to the following provisions of the Protection of Personal Information Act when Transferring Personal Information outside of the Republic of South Africa</u>**

4.13 The business may **not transfer personal information** about a data subject **to a third party who is in a foreign country unless** the personal information that is collected automatically is collected by third parties whose technology we use to provide website functionality and acquire website analytics information. Some of these third parties will be outside of the borders of South Africa and data subject's information will be stored outside the borders of South Africa.

## 5. Training

Staff will receive training as part of the induction process. Further training will be provided at least every year or whenever there is a substantial change in the policies and procedures, or IT Infrastructure.

Training could be provided through information sessions, regular emails to all staff as well as pre-recorded online webinars, and will cover the latest subjects related to the use of *Dirty Lolli Apparel Pty Ltd* IT systems and applications, the applicable laws relating to data protection, and *Dirty Lolli Apparel Pty Ltd*'s data protection, and related policies and procedures. Completion of training is compulsory.

If you have any questions or concerns about anything in this policy, do not hesitate to send your query to **ofentse@dirtylolli.com**

## 6. Enforcement:

We take compliance with this policy very seriously. Failure to comply puts both you and the organization at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, which may result in dismissal.

## 7. Document control

| | |
|---|---|
| **Creation Date** | |
| **Division Name** | *Dirty Lolli Apparel Pty Ltd* Information Technology Department |
| **Author Name** | |
| **Author Position** | |
| **Last Updated** | |
| **This Version** | |
| **Latest version approved by Board of Directors (*Dirty Lolli Apparel Pty Ltd* )** | |

## 8. Change History:

| Date | Author | Version | Change Reference |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## 9. POLICY APPROVAL:

**SIGNED:** _____

**DATE:** _____