# DATA PRIVACY POLICY

| | | | | |
|---|---|---|---|---|
| **Author:** | Tanya Wingfield | **Designation:** | Information Manager | |
| **Reviewed by Responsible Executive** | Nolufefe Ali | **Designation:** | Corporate Services Executive | |
| **Recommend to HR and Remuneration Committee and Audit and Risk Committee** | Hamish Erskine<br>On behalf of EXCO | **Designation:** | Chief Executive Officer | |
| **Recommended to the Board** | Nokhana Moerane on behalf of HR and Remuneration Committee | **Designation** | Chairperson: HR and Remuneration Committee | |
| **Recommended to the Board** | Zahid Fakey on behalf of the Audit and Risk Committee | **Designation** | Chairperson: Audit and Risk Committee | |
| **Approved By:** | Prof Gasa-Toboti | **Designation:** | Chairperson of the DTPC Board | |
| **Implementation Date:** | 1 December 2021 | **Next Review Date:** | 30 November 2023 | |
| **Document Number** | IM-POL-001 | **Status of Policy** | This is a new policy | |

## 1. Purpose

This is the Data Privacy Policy of Dube Trade Port Corporation (DTPC) and is designed to inform organizational practices which will result in the protection of the personal information of its clients and/or customers, employees, directors, shareholder (The KwaZulu-Natal Provincial Government), contractors, suppliers, consultants, tenants, and all stakeholders.

DTPC is committed to protecting its Data Subjects' privacy of Personal Information and ensuring that their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.

## 2. Scope of Application

The Data Privacy Policy is applicable to DTPC's clients and/or customers, employees, directors, shareholder (The KwaZulu-Natal Provincial Government), contractors, suppliers, consultants, tenants, and all stakeholders.

## 3. Legal Framework and References

The following provides the legal framework and references to this policy:

- Protection of Personal Information Act no 4 of 2013 and related regulations
- ICT Information Security Policy
- Code of Conduct Policy and Forms
- Media Policy
- ICT Incident Response Policy and Plan
- DTPC's Brand Strategy.

## 4. Definitions

| Term/ Abbreviation/ Acronym | Definition |
|---|---|
| Data Subject | means the person to whom Personal Information applies, such as but not limited to, customers, employees, directors, shareholder (The KwaZulu-Natal Provincial |

| | |
|---|---|
| | Government), contractors, suppliers, consultants, tenants, and all stakeholder's personal information. |
| ICT | means Information Communication and Technology |
| Intellectual Property(IP) | is a term that describes the application of the mind to develop something new or original.<br><br>Some IP rights require a formal process of application, examination and registration such as trademarks, patents, designs etc.<br><br>IP rights exist in many forms and in some cases they don't need to be registered in order to be of value. IP provides different competitive advantages for its owners and commercialization opportunities for organizations. IP has many of the same ownership rights a physical property.<br><br>IP can exist in various forms such as Policy documents, Protocol documents, Procedures etc. |
| Information Security | means the practice of preventing unathorised access, use, disclosure, disruption, modification, inspection, recording, or destruction of information. |
| Operator | means a person who processes Personal Information on behalf of DTPC in terms of a contract or mandate, without coming under the direct authority of DTPC. For all intents and purposes, most if not all service providers will fall within the scope of this definition. |
| PAIA | means the Promotion of Access to Information Act, 2000. |
| Person | means a natural person or a juristic person. |
| Personal information | is information that identifies you as an individual, and includes:<br><br>• Information relating to your 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;<br><br>• Information relating to medical (including biometrics), financial, criminal or employment history;<br><br>• Biometric information;<br><br>• Correspondence sent by a person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;<br><br>• Any identifying number symbol, e-mail address, telephone number, location information, or online identifier; |

| | |
|---|---|
| | • The name of a 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. |
| PFMA | means the Public Finance Management Act, 1999; |
| POPIA | means the Protection of Personal Information Act, 2013 read with the Regulations thereto. |
| Processing | means any activity concerning personal information including collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alteration, consultation or use, dissemination by means of transmission, distribution, merging, linking, restriction, degradation, erasure, or destruction of information. |
| Regulator | means the Information Regulator established in terms of POPIA. |

## 5. Responsibility Framework

| Role | Responsibility |
|---|---|
| **Board** | Approving the new Policy for the intended audience. |
| **HR and Remuneration Committee** | Reviewing and recommending the inputs on the new Policy to the Audit and Risk Committee.<br>Approving the annual review of Policy as per delegated authority from the Board |
| **Audit and Risk Committee** | Reviewing and recommending the new Policy to the Board.<br>Approving the annual review of Policy as per delegated authority from the Board |
| **CEO** | Reviewing and Recommending the Policy to the relevant Committee on behalf of EXCO.<br>Acts as the nominated Information Officer<br>Authorise the release of Patented Information to external parties, if requested |
| **Corporate Services Executive** | Regular monitoring, evaluation, and implementation of the Policy.<br>Acts as the nominated Deputy Information Officer. |

| | |
|---|---|
| **Senior Manager ICTG** | Regular monitoring, reporting about information data.<br>Developing and monitoring the data incident responses. |
| **Information Manager** | Developing and updating the Policy.<br>Developing Procedures and Forms to support the Policy.<br>Acts as the nominated Deputy Information Officer. |
| **Employees** | Understanding legislation and acquainting themselves with the aims and objectives of the Policy. |

## 6. Policy

### *6.1. THE 8 CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION*

DTPC commits itself to aligning its processing activities with the POPIA 8 conditions for the lawful processing of personal information. These conditions are as follows:

**Accountability**: all processing activities must align with the 8 conditions.

**Processing limitation**: processing must be lawful, reasonable, and not excessive (where Personal Information is required by DTPC, but not used for any clear purpose, the request for that Personal Information becomes excessive).

**Purpose specification**: processing must be for a specific and explicitly defined purpose.

**Further processing limitation**: further processing of Personal Information (sharing amongst Divisions and colleagues in different disciplines within DTPC), must be compatible with the purpose which the Personal Information was initially collected for.

**Information quality:** Personal Information must be updated, complete, accurate and not misleading.

**Openness**: DTPC must obtain documentation of all its processing Operations (evidenced by PAIA Manual).

**Security safeguards**: DTPC must secure the confidentiality of Personal Information in its possession by taking reasonable technical and organizational measures to prevent loss of unauthorized destruction of Personal Information.

**Data subject participation**: a Data Subject should at any time be able to make a request to DTPC for it to disclose the Personal Information that it has about that Data Subject, and if applicable, which third parties have had access to that information, for what purpose.

### *6.2. PERSONAL INFORMATION COLLECTED*

a) Subject to a Data Subject's consent (if applicable and no exceptions apply in terms of section 11 of POPIA), DTPC collects Personal Information for purposes which are related to its business functions, or activities, and only when it is necessary for or related to such purposes.

b) Subject to a Data Subject's consent, DTPC also collects and processes information so that it can communicate marketing materials in connection with the various business and business infrastructure related opportunities that it has on offer.

### *6.3. USAGE OF PERSONAL INFORMATION*

a) The Data Subject's personal information will only be used for the purpose for which it was collected and as agreed. As a rule, DTPC only processes Personal Information of Data Subjects to facilitate the rendering of services in the case of customers and clients.

b) In the case of Data Subjects who are employees of DTPC, Personal Information is only collected pursuant to operating and managing an organization of the nature and scope of DTPC (an organization established in terms of the Special Economic Zone Act, 2014 and a Schedule 3C PFMA Provincial Public Entity).

### *6.4. DISCLOSURE OF PERSONAL INFORMATION*

a) DTPC will not share the personal information of a Data Subject with other organisations (including service providers or Operators), or anyone else unless that disclosure:

i. has been consented to by the Data Subject; or
ii. is for a purpose(s) consistent with the purpose for which the Personal Information was initially collected; or
iii. is pursuant to an obligation in terms of the law; or
iv. may be deemed necessary to protect DTPC's rights at law.

b) DTPC will not be responsible for the security of Personal Information shared by Data Subject's on DTPC's social media channels.

c) DTPC will only utilise the information in accordance with this Policy but cannot be responsible for other users collecting and utilising Personal Information made available on these platforms.

### 6.5. *INTELLECTUAL PROPERTY (IP)*

a) IP provides a competitive advantage for DTPC and must not be shared externally without prior written authorisation.

b) Requests to release IP must submitted through to the relevant Executive, and after consultation and approval by the CEO may only be released.

c) DTPC's trademark information is registered with the Company Intellectual Property Commission (CIPC) and monitored in accordance with DTPC's Brand Strategy.

### 6.6. *SAFEGUARDING OF PERSONAL INFORMATION*

a) It is a requirement in terms of POPIA for DTPC to adequately protect Personal Information that DTPC collects. DTPC has measures in place to protect the Personal Information it holds against loss, interference, unauthorised access, use, modification, or disclosure and against other misuse. These measures include but are not limited to, password protection for electronic files, securing paper files, physical access restrictions, technological and organizational measures.

b) DTPC will continuously review its security controls and processes, considering internal and external threats, to ensure that security controls are well aligned with identified security risks, and ensuring as far as possible that personal information is secure. In the event of a data breach, DTPC undertakes to notify the affected Data Subject(s), in accordance with the provisions of section 22 (Notification of security compromises) of POPIA and the DTPC Incident Response Policy and/or Plan, whichever is applicable.

c) DTPC's archived information is stored off site at an offsite storage facility which is also governed by POPIA, and in DTPC's Retention Guide once it is finalized and approved. In both cases access to retrieve personal information is limited to authorised personnel.

d) All electronic files or data are backed up by DTPC's ICT Division, which is also responsible for system security that protects against unauthorized access and any other internal and external threats. The ICT~~G~~ Division is also the custodian of the ICT Information Security Policy, which is relevant to safeguard measures relating to personal information.

### *6.7. THIRD PARTY OPERATORS*

DTPC ensures that the following standards are met by all its Operators:

a) Personal information can only be processed by way of a written agreement entered into by the Operator and DTPC.

b) Operators must treat Personal Information that comes to their knowledge as confidential and must not disclose it to anybody unless required by law and DTPC has provided prior written consent thereto.

c) A written undertaking must be given by the Operator, to the effect that it has systems, processes, and policies in place to ensure that it prevents the unlawful accessing, loss of and/or damage to Personal Information.

d) A warranty must be provided by the Operator that it has the safety and security measures referred to in section 19 (Security measures on integrity and confidentiality of personal information) of POPIA.

e) If there are reasonable grounds to believe that the Personal Information in the control of the Operator has been accessed without authorisation, the Operator must immediately notify DTPC.

### *6.8. ACCESS AND CORRECTION OF PERSONAL INFORMATION*

a) Data Subjects have a right to access the Personal Information DTPC holds about them, and have the right to ask DTPC to update, correct or delete their Personal Information on reasonable grounds. Once a Data Subject objects to the processing of their Personal Information, DTPC may no longer process said Personal Information. DTPC will take all reasonable steps to confirm the Data Subject's identity before providing details of their Personal Information or making changes to their Personal Information.

b) The rights of Data Subjects to access their Personal Information held by DTPC shall always be subject to compliance with PAIA.

### *6.9. USE OF COOKIES*

a) The DTPC website uses "cookies" to help Data Subjects personalize their online experiences. A cookie is a text file that is placed on your hard drive by a web page server. Cookies cannot be used to run programs or deliver viruses to Data Subjects' computers. Cookies are uniquely assigned to each Data Subject and can only be read by a web server in the domain that issued the cookie to that Data Subject.

b) One of the primary purposes of cookies is to provide a convenience feature to save each Data Subject time. Furthermore, the purpose of a cookie is to tell the web server that you have returned to a specific page. For example, if you personalize DTPC pages, or register with DTPC sites or services, a cookie helps DTPC recall your specific information on subsequent visits. This simplifies the process of recording personal information. When a Data Subject returns to the same DTPC website, the information previously provided by the Data Subject can be retrieved without the Data Subject having to complete that same information anew.

c) Data Subjects may accept or decline the use of cookies, using the relevant prompts appearing on the website.

## *6.10. ARCHIVING AND DESTRUCTION OF RECORDS*

a) All archiving and destruction of records containing Personal Information shall be subject to DTPC's operational requirements, applicable legislation, POPIA, PAIA, the National Archives Act, 1996, and the relevant guidance contained in the SAICA Retention Guide. As a rule, records containing Personal Information must not be kept for longer than what is necessary for use.

b) All records which require destruction must be sought via the Information Manager who will facilitate the approval process.

c) Records may be destroyed after the termination of the retention periods prescribed by legislation. Each Division is responsible for initiating the procedure for the destruction of records containing Personal Information, which are no-longer required.

d) Files containing Personal Information must be checked to ensure they may be destroyed.

e) Subject to being authorized, records containing Personal Information may also be stored off site, in storage facilities approved by DTPC.

## *6.11. COMPLAINTS PROCEDURE*

a) A Data Subject may complain about a suspected breach of its Personal Information in terms of POPIA, by submitting the complaint in writing to DTPC's Deputy Information Officer, using the contact details provided in the PAIA Manual. Any complaint must set out in as much detail as possible all the relevant particulars relating to the complaint.

b) DTPC will revert as soon as reasonably possible on whether it will investigate the complaint, and if applicable, any further particulars that the complainant is required to submit to DTPC, to aid the investigation process. DTPC will also provide an estimate on the number of days that it may require to complete the investigation.

c) During the investigation, should it be determined that an employee disclosed personal information unlawfully, the DTPC internal disciplinary process will follow.

d) Upon completion of the investigation, DTPC shall inform the complainant in writing on the outcomes of the investigation, whether there has been a breach of the Data Subject's Personal Information, and actions to be taken (if any).

## 7. Information and Education

Information on the policy may be made accessible to employees in the following ways:

- Uploaded onto the Dube World (electronic version, without signatures);
- Email notification sent to all employees to advise and inform employees off of the new policy; and
- Training on this Policy, POPIA and guidance notes published by the Regulator from time-to-time, will be conducted by DTPC from time-to-time.

## 8. Monitoring and Enforcement

- The Information Officer is ultimately responsible for compliance and enforcement of this Policy.
- The Deputy Information Officer shall assist the Information Officer with their responsibility of ensuring compliance and enforcement of this Policy.
- Management shall monitor compliance with this Policy and the enforcement thereof, as part of their daily responsibilities.

## 9. Annexures

- Complaints Procedure and Form
- User and Access Request Form
- Code of Conduct Form

## 10. Records

The records table shall contain the following information:

| Record Name | Location | Responsibility | Retention Period | Disposal |
|---|---|---|---|---|
| **Privacy Policy** | Board Store Room; and Dube World | Company Secretary | Indefinite | Indefinite |

## 11. Version History

Indicates the major changes that have been made to the document over its lifetime:

| Date | Version No. | Nature of Change |
|---|---|---|
| Nov 2021 | Version 1 | New Policy |