DHL SUPPLY CHAIN (SOUTH AFRICA) (PTY) LTD

(Registration Number: 1992/001746/07)

PAIA MANUAL

Published in terms of section 51 of the

Promotion of Access to Information Act 2 of 2000

Incorporating notification in terms of the

Protection of Personal Information Act 4 Of 2013

Contents

1 Introduction

DHL Supply Chain (South Africa) (Pty) Ltd (the "Company") conducts business as a supply chain services provider which includes logistics, warehousing, and distribution. The Company forms part of the Deutsche Post DHL Group, a group of companies which are active worldwide in the markets for mail delivery, express and logistics products with the controlling company being Deutsche Post AG, a German Aktiengesellschaft (Stock Corporation) with its registered offices in Bonn, Germany ("DHL Group") and is ultimately owned or controlled by Deutsche Post AG.

As a private body the Company is required in terms of the Promotion of Access to Information Act 2 of 2000 ("**PAIA**") to make available this Manual in accordance with section 51 of PAIA to ultimately give effect to the right to access of information as contemplated by the aforesaid legislation.

The Company is additionally required, as a responsible party in terms of the Protection of Personal Information Act 4 of 2013 ("**POPIA")**, to take reasonably practicable steps to ensure that data subjects are notified that the Company processes certain information etcetera in ultimately giving effect to the constitutional right to privacy.

The above two pieces of legislation. Being POPIA and PAIA, dovetail in a number of respects - particularly insofar as the requirement to appoint an information officer, the requirement to maintain a record of processing operations, and the manner in which access to records should be governed.

Take note that when exercising a right in terms of POPIA, a data subject request should relate to Personal Information about them or about a third-party data subject on whose behalf the request is made. PAIA requests on the other hand, should relate to access to a record of a private body (in this case, the Company) which is required for the exercise and protection of rights.

The Company has therefore compiled this Manual in complying with its duties in terms of the aforesaid pieces of legislation and the Company believes that this Manual will provide the necessary assistance and information to persons in this regard.

This Manual does not purport to be exhaustive or deal comprehensively with every procedure provided for in PAIA and POPIA respectively.

A reference to a statute, regulation or other legislation will be interpreted as a reference to such statute, regulation of legislation as amended or substituted from time to time.

Please contact the Company's Information Officer or Legal Department should you have any queries relating to this Manual or the Processing of your Personal Information.

Words or terms which are used in POPIA bear the same meaning where used in this Manual. A few words or terms are defined below to assist the reader in utilizing this Manual:

Term	Descriptions
Access control	Access control is a method of restricting access to sensitive data. Only those that have had their identity verified can access company data through an access control gateway.
Biometrics	Means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
Data subject	Means the person to whom personal information relates.
Information Regulator	The regulator who is responsible for enforcement of POPIA through a number of mechanisms. The office if the Information Regulator has been established via POPIA.
Location tracking	Location tracking refers to technologies that physically locate and electronically record and track the movement of people or objects. Location tracking technology is in use every day with GPS navigation, locations located on digital pictures and searching for businesses nearby using common apps.
Metadata	Metadata is a set of data that describes and gives information about other data. Some examples of basic metadata are author, date created, date modified, and file size. Metadata is also used for unstructured data such as images, video, web pages, spreadsheets, etc. Web pages often include metadata in the form of meta tags.

Operator	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.
Person	Means a natural person or a juristic person.
Personal Information	Means information relating to an identifiable, living, natural person, identifiable, existing juristic person, including, but not limited to— a) information relating to the race, gender, sex, national or social origin, language, age disability; b) information relating to the education or medical or financial history of the person; c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; d) the biometric information of the person; e) the personal opinion, views or preferences of the person; f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence 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. In this Manual the term "Personal Information" will include "Special Personal Information" as the context may dictate or as appropriate.
Private body	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.
Processing / processed / process / processes	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.
Responsible Party	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
Regulations	Regulations published in terms of the Protection of Personal Information, 2018 (as amended from time to time)
Special Personal Information	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 the criminal behaviour of a data subject to the extent that such information relates to - - The alleged commission by a data subject of any offence, or - Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings

This Manual may be useful for persons to-

i. check the categories of records held by the Company which are available without a person having to submit a formal PAIA request;
ii. have a sufficient understanding of how to make a request for access to a record of the Company, by providing a description of the subjects on which the Company holds records and the categories of records held on each subject;
iii. know the description of the records of the Company which are available in accordance with any other legislation;
iv. access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access;

v. know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;
vi. know if the Company will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;
vii. know the description of the categories of data subjects and of the information or categories of information relating thereto;
viii. know the recipients or categories of recipients to whom personal information may be supplied;
ix. know that the Company transfers or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and
x. know whether the Company has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

2 How to access records

The Information Regulator published a guide ("**Guide**") which sets out the process of requesting information and generally provides the public with guidance in this regard. The Company has copies of the Guide available in English PAIA-Guide-English_20210905.pdf (inforegulator.org.za), Afrikaans InfoRegSA-PAIA-Manual-2021-Afr.pdf (inforegulator.org.za) and Sesotho InfoRegSA-PAIA-Manual-2021-SeSotho.pdf (inforegulator.org.za) and any member of the public may inspect and obtain copies of the Guide at our office during normal working hours (see address in 2 below). Copies of the Guide in each official language are also available on the website of the Information Regulator https://www.justice.gov.za/inforeg/.

The contact information of the Information Regulator is as follows (please always consult the Information Regulator's website for the most up to date information):

Information Regulator of South Africa
Address: 33 Hoofd Street, Forum III, 3rd Floor Braampark, Braamfontein, Johannesburg, 2017
E-mail: inforeg@justice.gov.za Website: https://inforegulator.org.za/

3 Company contact details

The Company
DHL Supply Chain (South Africa) (Pty) Ltd
PO Box 8166, Elandsfontein, 1406
23 Spier Road, Plumbago Business Park, Glen Erasmia, Kempton Park, 1619
Telephone number: (011) 821-0100
Website : www.dhl.co.za

The Company's Information Officer
Allyn Tasker
ISM Lead Africa | Information Officer | Data Protection Official
E-mail: Allyn.Tasker@dhl.com | dsc.africa.dataprotection@dhl.com

The Company's Legal Department
Melissa Erasmus
Head of Legal for Africa
Telephone number: (011) 821 0100
E-mail: dhl.za.legalnotice@dhl.com

4 Company records

4.1 Description of subjects and categories of records held and processed

Below is a description of different subjects and the categories of records the Company holds in respect of data subjects:

Subject	Categories of records
Human Resource records to recruit new employees (or trainees, learners, volunteers or the like) manage existing employees (or existing trainees, learners, volunteers or the like) and pay their salaries. This may include "deemed employees" as contemplated in the Labour Relations Act, as well as TES employees). Personal and special personal information is also used to comply with legal obligations (including under the Labour Relations Act, Basic Conditions of Employment Act, Employment Equity Act, and Compensation for Occupational Injuries and Diseases Act)	HR policies and procedures; Advertised posts; Employee records (including dependants, family, next-of-kin records); Health & safety records; recruitment records; training records Address, identification number, academic information and qualifications, criminal background, gender, race and/or demographic information, trade union membership; martial status; Income related information Metadata Biometrical data (including fingerprint scanning, location tracking, video footage, CCTV footage and photographs); Photographic and similar images; Bank details, information relating to submissions to the South African Revenue Service, pension funds, provident fund, medical aids Education; training; vehicle identifiers (such as licence plate number) Health and medical information (including where applicable that relating to children of a data subject, for instance, relating to medical aid and/or pension fund where a minor is a dependent or beneficiary) Opinions/views captured via surveys or coaching sessions Employee Contracts, Performance Records Payroll Records, Electronic Access Records, Physical Access Records Surveillance Records, Time & Attendance Records; Conversations (biometrics; voice recordings; transcripts or messages) Information in accordance with Company and DHL and/or DHL Group policies and procedures Criminal Checks; Background Checks
Supplier / service provider records to engage with suppliers and independent contractors to gain access to the goods and/or services they provide; manage such relationships and any developments stemming from such relationships, make payments; monitor services	names, e-mail address, postal address; value added tax registration number; registration number; identity number, and bank details company secretarial information BEE information, certifications; Metadata Conversations (voice recordings; transcripts or messages) Where applicable and in relation to employees, agents, officers etc. of a service provider, information listed under "Human Resources" Biometric data; Access control and surveillance records
Customer/client records (including potential customers/clients) to engage with customers or clients from early stages (such as tenders or request for information); generally to provide services and bill for such services. Includes personal and special personal information of customers'/client's employees or	Company information; Billing details and invoices Contact information; Records provided by clients Advice and records created for clients; Correspondence Biometric data; Access control and surveillance records Where applicable and in relation to employees, agents, officers etc. of a customer, information listed under "Human Resources" (this would, for instance, be relevant where a customer's employee enters a site managed by the Company) Metadata
Company secretarial; Legal	Company memorandum of incorporation; CIPC documents; board meeting minutes; shareholders' meeting minutes; statutory records; legal compliance records; share register Company policies and procedures; intellectual property records; contractual records; immovable property records; legal matters
Marketing	Marketing records; media releases
Compliance	Company policies and procedures and records relating thereto
Finance; Insurance; Risk	Financial statements; accounting and tax records; asset register; insurance records; contracts and mandates; management accounts; supplier records Insurance contracts, claims, and related records Risk registers; audit records BBBEE certificate and records
Visitors Operations; Facilities regulation	Customer records; Performance measurement records; Maintenance records; Property records; Health & Safety records; Certifications

	Physical Access Records Electronic Access Records & Scans including biometrical data such as fingerprints Surveillance Records (including CCTV footage, photographs) vehicle identifiers (such as licence plate number); Metadata
IT & Security	Security records (visitors, suppliers, contractors, employees etc.) Access records; investigation records Biometrical data (including fingerprint scanning, location tracking, video footage, CCTV footage and photographs); Photographic and similar images; IT – supplier and product contracts and manuals; Licences; IT - Asset & configuration records IT - System account records In respect of children - Access records (if entering any site or facility) including biometrical data, camera surveillance User accounts and activity

4.2 Records may be available in accordance with any other legislation

PAIA provides that any other law that gives a person an avenue for accessing information that is less onerous than PAIA, can be used by a requestor instead. If a requestor is of the opinion that any other law affords such a less onerous avenue to obtain information, then the requestor is advised to enquire from the Company's Information Officer if the desired information can be made available in such manner.

5 Processing of Personal Information

5.1 Purpose of Processing Personal Information

The Company Processes Personal (and Special Personal) Information for a variety of purposes, including but not limited to, the following purposes:

i. to negotiate, enter into and give effect to contracts, including customer and supplier contracts;
ii. vetting and verifying information of customers and suppliers (potential and existing), for instance relating to denied party screening and credit profile screening;
iii. to monitor services being rendered and received; and in general to manage the relationship with relevant parties;
iv. to facilitate physical access to facilities or property, and safeguard premises, vehicles and property which the Company has a duty to protect, including via the use of biometric access control systems and CCTV camera (recording devices);
v. to monitor vehicles and driver behaviour;
vi. to manage employee relationships, including performance monitoring, on-boarding and off-boarding employees on the Company network, facilitation of labour relations, enforcement of policies and procedures, conducting training and awareness, disciplinary action, ensuring a safe and healthy workplace, and other related human resource functions such as payment of salaries, leave applications, recording of trade union affiliation, health/medical evaluations, administration relating to pension and medical fund, and communication with the Department of Employment and Labour (which includes, but is not limited to submitting the annual employment equity report and BBBEE annual report);
vii. to maintain business records;
viii. to comply with customer contractual obligations;
ix. to use certain (appropriate, high-level) customer data in presentations for tenders, request for information or quotations;
x. Due to Company employees often working on customers' sites, customers and suppliers will receive Personal Information (including biometric data for security etcetera) of such employees. When a customer or supplier requests the Company's cooperation where there has been theft or criminal activity (or alleged criminal activity) the Company may share data (including polygraph test results) in order to assist in investigations and the like;
xi. for recruitment purposes;

xii. to comply with mandatory laws, for example relating to finance and tax, environment, health and safety, road usage, data protection, business administrative, and labour.
xiii. to comply with internal Company policies, procedures, directives and rules, as well as those of the DHL Group;
xiv. to monitor and/or record calls, correspondence for business purposes;
xv. to keep records that an employee or ex-employee was involved with (especially email correspondence) for as long as necessary in the Company's reasonable discretion;
xvi. to monitor compliance with internal policies and procedures;
xvii. to improve the quality of services, conduct analysis for internal reporting and use;
xviii. for the purpose of legal action or proceedings, as well as regulatory type proceedings and correspondence;
xix. for the purposes of the prevention of fraud, loss, bribery or corruption;
xx. to respond to tenders or benchmarking activities;
xxi. allowing access to and use of the Company's electronic and/or online systems and tools;
xxii. shared services or central services being rendered by DHL Group;
xxiii. for purposes of audits (internal and external);
xxiv. for the purposes of facilitating data subject requests;
xxv. to facilitate financial transactions relating to suppliers, customers and employees, this includes but is not limited to banking, payroll reconciliation and maintaining data bases for both customers and suppliers
xxvi. to facilitate employee travel, which includes visa applications;

Please take special note that Personal Information (including Special Personal Information) is transferred outside the borders of South Africa, and the Company will always do its best to make sure that any third country or international organization has the same or similar data protection laws in place as South Africa. The Company is a part of the DHL Group whose headquarters are in Bonn, Germany and as such Personal Information is also hosted on servers outside of South Africa and Personal Information is shared within the DHL Group in line with the DHL privacy policy found at https://www.dpdhl.com/en/data-protection.html.

The Company makes use Microsoft 365 in daily operations and to store information. Microsoft stores content in data centres in various jurisdictions. The Company also makes use of various systems and platforms in its daily operations, including the following: -

Warehousing: warehouse management systems (BlueYonder and Manhattan) (supports the material procurement and order management – picking, replenishment, inventory control, etc.)
Transportation: transport management systems (OTM) (supports the processes required to plan, procure, execute and track transport operations)
Resource management: SmartRem (supports the HR processes including personnel administration, payroll and recruiting; labour planning and management of time & attendance)
Operations Excellence: Smart Ops, LOGICS, etc. (supports the capabilities to manage and improve operational performance. This includes areas such as quality, health, safety and environment and business continuity management, as well as the opportunity lifecycle and project delivery)
Solutions Design: Merlin (supports the capabilities to model a solution and to provide the right costing in line with the customer needs)
Marketing and Sales: MySupplyChain (supports how we manage our internal Sales and Marketing process)
Finance: Oracle and CREST.
Action Content Time Visual (supports our order-to-cash, procure-to-pay and record-to-report financial processes)
Information management: Data Lake and PowerBi (supports the processes to acquire, store, structure, analyze and govern information from any sources and to distribute / make accessible to those who need it, cross-domain)
Integration management: DHL Link (supports the capabilities and tools required to integrate with internal and external customer and trading partner processes and systems including BPM and API solutions).
IT Service management: Request IT (ensures availability and performance of the IT solutions in Supply Chain, and provides industrialize end user support following globally harmonized and data driven processes)

Relevant data may also be shared with authorised DHL divisions; carefully selected business partners who provide products and services under a DHL brand; and service providers and agents who perform services on DHL Group or any of its affiliates' behalf.

5.2 The recipients or categories of recipients to whom the Personal Information may be supplied

Category of Personal Information	Recipients or Categories of Recipients to whom the Personal Information may be supplied
Employee information (including that of prospective employees, temporary employees, independent contractors	South African Qualifications Authority and/or service provider in this regard South African Police Services and/or service provider in this regard Third party requesting confirmation of employment (including length of service and job title) Suppliers such as Uhehluko t/a Ferlio Group of Investigators Professional advisors; Auditors Microsoft 365 Credit Bureaus or service provider in this regard IT service providers Payroll service Providers, Banks Security service providers Medical practitioners, medical service providers, claims or insurance service providers Agents assisting the Company with administration in terms of labour and labour-related legislation such as Compensation of Occupational Injuries and Diseases Act Pension and/or Provident funds (including with agents assisting the Company with admin in this regard) Department of Labour Agents/service providers assisting the Company with BBBEE rating/verifications Operators DHL Group Government departments, Regulators, law enforcement Deloitte (PWC previously) Insurance service providers Time and attendance (current service provider being SmartTime) Electronic signature platforms
Clients, customers, service providers, suppliers information (and their employees or persons corresponding with the Company on their behalf)	Banks Credit Bureaus or service provider in this regard Professional advisors; Auditors Microsoft 365 Government departments, Regulators, law enforcement Operators DHL Group Deloitte (PWC previously) Insurance service providers Electronic signature platforms
Tax and VAT information of clients, employees, and service providers	South African Revenue Services Professional advisors; Auditors Insurance service providers Microsoft 365
Biometrics, Surveillance, Access data	Agents/service providers assisting the Company with security DHL Group Operators South African Police Service IT service providers; OPSI Professional advisors; Auditors Insurance service providers Microsoft 365

Note: The Company has many contracts in place with various vendors, suppliers and/or service providers and this may change regularly based on contract length, service levels, market fluctuations and the like. It is therefore not possible for the Company to update this Manual every time such a party changes. For this reason, the names or identity of most of these parties are not mentioned in this Manual, but a data subject is welcome to contract the Company's Information Officer at any time if they would like to request information in this regard.

5.3 Planned transborder flows of Personal Information

The Company makes use of servers or cloud storage located outside the borders of South Africa, with three major data centres being located in Czech Republic, Malaysia and the United States of America. The Company also makes use of service providers and Operators who may Process Personal Information outside the borders of South Africa, such as Microsoft 365 (which generally stores data in the European Union,Austria, Finland, France, Ireland, Netherlands, and Sweden). The Company also services customers who are domiciled or registered in countries other than South Africa.

5.4 General description of Information security measures implemented to ensure the confidentiality, integrity and availability of the information

The Company (largely via DHL Group efforts) has taken reasonable steps to protect the integrity and confidentiality of Personal Information. The Company continuously implements and monitors technical and organisational security measures to protect and safeguard data. These measures include data encryption; internet security software such as anti-virus and anti-malware solutions to scan for and protect against malicious content, malware, network attacks etcetera.

The Company also runs regular awareness campaigns in this regard (including to test our employees' reactions relating to phishing).

Personal Information is stored via cloud services or other technology, by third parties contracted to the Company and/or DHL Group, to support the Company's business operations.

The Company is committed to safeguarding Personal Information and the Company's security measures are regularly reviewed and updated where necessary.

The Company's third-party service providers., including data storage and processing providers (Operators) may from time to time have access to a Data Subject's Personal Information. The Company will ensure that such providers employ comparable safeguarding measures to that of the Company.

5.5 Data subject rights

Most of the rights of data subjects are set out in section 5 of POPIA. Below are a few of these rights that the Company would like to highlight: -

Where found in POPIA	You have a right -
Section 23	of access to and the right to rectify the information collected;
Section 24	to request, where necessary, the correction, destruction or deletion of your information
Section 11	to object, on reasonable grounds relating to your particular situation to the processing of your information
Section 74	to submit a complaint to the Regulator regarding the alleged interference with the protection of your information of or to submit a complaint to the Regulator in respect of a determination of an adjudicator

6 Forms

The following forms are available on the website of the Information Regulator for use by data subjects when asserting their rights:

- Form 02: Request for Access to Record [Regulation 7] - InfoRegSA-PAIA-Form02-Reg7.pdf (SECURED) (inforegulator.org.za)
- Form 03: Outcome of request and of fees payable [Regulation 8] - Form-3-PAIA.pdf (inforegulator.org.za)

Copies of the forms are attached below. Kindly note that it is recommended to always verify that the forms are the latest versions as published by the Information Regulator by checking the Information Regulator's website.

FORM 2

REQUEST FOR ACCESS TO RECORD

[Regulation 7]

NOTE:

1. *Proof of identity must be attached by the requester.*
2. *If requests made on behalf of another person, proof of such authorisation, must be attached to this form.*

TO: The Information Officer

_____

_____

_____

_____

(Address)

E-mail address: _____

Fax number: _____

Mark with an "X"

☐ Request is made in my own name ☐ Request is made on behalf of another person.

PERSONAL INFORMATION				
Full Names				
Identity Number				
Capacity in which request is made *(when made on behalf of another person)*				
Postal Address				
Street Address				
E-mail Address				
Contact Numbers	Tel. (B):		Facsimile:	
	Cellular:			
Full names of person on whose behalf request is made *(if applicable)*:				
Identity Number				
Postal Address				

Page 1 of 4

Street Address				
E-mail Address				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			

PARTICULARS OF RECORD REQUESTED

Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)

Description of record or relevant part of the record:	
Reference number, if available	
Any further particulars of record	

TYPE OF RECORD
(Mark the applicable box with an "X")

Record is in written or printed form	
Record comprises virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Record consists of recorded words or information which can be reproduced in sound	
Record is held on a computer or in an electronic, or machine-readable form	

FORM OF ACCESS *(Mark the applicable box with an "X")*	
Printed copy of record *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Transcription of soundtrack *(written or printed document)*	
Copy of record on flash drive *(including virtual images and soundtracks)*	
Copy of record on compact disc drive*(including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	

MANNER OF ACCESS *(Mark the applicable box with an "X")*	
Personal inspection of record at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)*	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format *(including transcriptions)*	
E-mail of information *(including soundtracks if possible)*	
Cloud share/file transfer	
Preferred language *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED *If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.*	
Indicate which right is to be exercised or protected	

Explain why the record requested is required for the exercise or protection of the aforementioned right:	

FEES	
a) A request fee must be paid before the request will be considered. *b) You will be notified of the amount of the access fee to be paid.* *c) The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.* *d) If you qualify for exemption of the payment of any fee, please state the reason for exemption*	
Reason	

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal address	Facsimile	Electronic communication *(Please specify)*

Signed at _____ this _____ day of _____ 20 _____

_____

Signature of Requester / person on whose behalf request is made

---

FOR OFFICIAL USE

Reference number:	
Request received by: (State Rank, Name And Surname of Information Officer)	
Date received:	
Access fees:	
Deposit (if any):	

_____

Signature of Information Officer

FORM 3

OUTCOME OF REQUEST AND OF FEES PAYABLE

[Regulation 8]

Note:

1. *If your request is granted the—*
   - *(a) amount of the deposit, (if any), is payable before your request is processed; and*
   - *(b) requested record/portion of the record will only be released once proof of full payment is received.*
2. *Please use the reference number hereunder in all future correspondence.*

Reference number: _____

TO: _____

Your request dated _____, refers.

1. You requested:

Personal inspection of information at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)* is free of charge. You are required to make an appointment for the inspection of the information and to bring this Form with you. If you then require any form of reproduction of the information, you will be liable for the fees prescribed in Annexure B.	

OR

2. You requested:

Printed copies of the information *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Transcription of soundtrack *(written or printed document)*	
Copy of information on flash drive *(including virtual images and soundtracks)*	
Copy of information on compact disc drive*(including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	

3. To be submitted:

Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format *(including transcriptions)*	
E-mail of information *(including soundtracks if possible)*	
Cloud share/file transfer	
Preferred language: *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

Kindly note that your request has been:

☐ Approved

☐ Denied, for the following reasons:

4. Fees payable with regards to your request:

Item	Cost per A4-size page or part thereof/item	Number of pages/items	Total
Photocopy			
Printed copy			
For a copy in a computer-readable form on: (i) Flash drive • To be provided by requestor (ii) Compact disc • If provided by requestor • If provided to the requestor	 R40.00 R40.00 R60.00		
For a transcription of visual images per A4-size page	Service to be outsourced. Will depend on the quotation of the service provider		
Copy of visual images			
Transcription of an audio record, per A4-size	R24.00		
Copy of an audio record (i) Flash drive • To be provided by requestor (ii) Compact disc • If provided by requestor • If provided to the requestor	 R40.00 R40.00 R60. 00		
Postage, e-mail or any other electronic transfer:	Actual costs		
TOTAL:			

5. Deposit payable (if search exceeds six hours):

☐ Yes ☐ No

Hours of search		Amount of deposit *(calculated on one third of total amount per request)*	

The amount must be paid into the following Bank account:

Name of Bank: _____
Name of account holder: _____
Type of account: _____
Account number: _____
Branch Code: _____
Reference Nr: _____
Submit proof of payment to: _____

Signed at _____ this _____ day of _____ 20 _____

_____
Information officer