

PAIA AND POPIA MANUAL

Version 1.0 – August 2021

INDEX

1. INTRODUCTION	1
2. DEFINITIONS	2
3. SCOPE OF THIS POLICY	3
4. COMPANY DETAILS	3
5. CONTACT DETAILS OF THE INFORMATION OFFICER AND DEPUTY INFORMATION OFFICER	3
6. THE SOUTH AFRICAN HUMAN RIGHTS COMMISSION	4
7. PUBLICATION AND AVAILABILITY OF CERTAIN RECORDS IN TERMS OF PAIA	4
8. LIST OF APPLICABLE LEGISLATION	4
9. THE PURPOSE FOR PROCESSING PERSONAL INFORMATION	4
10. KARGO’S GUIDING PRINCIPLES IN PROCESSING PERSONAL INFORMATION AND RECORDS	4
11. CONSEQUENCES OF WITHHOLDING CONSENT OR PERSONAL INFORMATION	4
12. HOW KARGO STORES AND DESTROYS PERSONAL INFORMATION.	4
13. ACCESS BY OTHERS AND CROSS BORDER TRANSFER	5
14. REQUESTS FOR ACCESS TO PERSONAL INFORMATION IN TERMS OF POPIA	5
15. REQUESTS FOR ACCESS TO INFORMATION IN TERMS OF PAIA	5
16. REFUSAL OF ACCESS TO RECORDS	6
17. RIGHTS	6
18. ACCURACY OF INFORMATION AND ONUS	7
19. AMENDMENTS AND BINDING ON SUCCESSORS IN TITLE	7
20. BREACHES OF PERSONAL INFORMATION	7
21. INFORMED CONSENT TO PROCESS PERSONAL INFORMATION	7
22. AUDITS, CONTROL AND POLICY CHANGES	8
23. ANNEXURE A - CATEGORISATION OF RECORDS HELD	9
24. ANNEXURE A – RECORDS CATEGORISATION ASSIGNMENT	9
25. ANNEXURE B - RECORDS AVAILABLE IN ACCORDANCE WITH OTHER LEGISLATION	10
26. ANNEXURE C1 – INFORMATION PROCESSED PERTAINING TO EMPLOYEES	11
27. ANNEXURE C2 – CUSTOMER INFORMATION PROCESSED	12
28. ANNEXURE C3 – THIRD PARTY SERVICE PROVIDERS AND SUPPLIERS	13
29. ANNEXURE C4 – SHAREHOLDER INFORMATION PROCESSED	14
30. ANNEXURE C4 – VISITORS INFORMATION PROCESSED	14
31. FORM - REQUEST FOR ACCESS TO RECORDS IN TERMS OF PAIA	15
32. PAIA FEES	18

1. INTRODUCTION

This manual serves as the information manual and provides references to the records held by:-

Kargo National (Pty) Ltd
Kargo Long Distance (Pty) Ltd
Kargo Logistics (Pty) Ltd

including their divisions, wholly owned subsidiaries (“**Kargo**”).

Kargo is committed to being a good steward of data and personal information and handling it in a responsible way, and securing it with various administrative, technical, organizational, and physical safeguards in accordance with the following two Acts:-

- **The Promotion of Access to Information Act 2 of 2000 (“PAIA”)** which provides that everyone has the right to access to information held by the State, as well as to information held by another person (or private body) when such privately held information is required to exercise or protect a right; and
- **The Protection of Personal Information Act, No. 4 of 2013 (“POPIA”)** which seeks to give effect to the constitutional right to privacy as contained in section 14 of the Bill of Rights. POPIA seeks to safeguard personal information by regulating the manner in which it may be processed by public and private bodies (such as Kargo).

Accordingly, the principles relating to the processing of any information (including but not limited to the collection, transfer, handling, correction, storage, destruction, and archiving) will be applied to all personal information obtained from:-

- Employees (Including full time salaried staff, wage staff and directors)
- Prospective employees
- Customers
- Suppliers
- Sub-contractors
- Contractors
- Service providers
- Shareholders
- Visitors
- Directors;
- Consultants;
- Associated Companies;

Any requests in terms of **PAIA** and **POPIA** must comply with the procedural requirements laid down in **PAIA** and in this manual.

2. DEFINITIONS

- 2.1 “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;
- 2.2 “child”** means a natural person under the age of 18 years, who is not legally competent to act without a competent person to take any action or decision in respect of any matter concerning him or her;
- 2.3 “competent person”** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;
- 2.4 “consent”** means the voluntary, specific and informed expression of will;
- 2.5 “data subject”** means the person to whom the personal information processed by Kargo, relates. This will include, but not be limited to personal information obtained from:-
- 2.5.1** Employees (Including full time salaried staff, wage staff and directors);
 - 2.5.2** Prospective employees;
 - 2.5.3** Customers;
 - 2.5.4** Suppliers;
 - 2.5.5** Sub-contractors;
 - 2.5.6** Contractors,
 - 2.5.7** Service providers;
 - 2.5.8** Shareholders;
 - 2.5.9** Directors;
 - 2.5.10** Consultants;
 - 2.5.11** Associated Companies;
 - 2.5.12** Visitors.
- 2.6 “employee”** means any employee of Kargo.
- 2.7 “government”** means the Government of South Africa, it’s affiliates, regulatory bodies and/or subsidiaries and departments.
- 2.8 “Kargo”** shall mean **Kargo National (Pty) Ltd, Kargo Long Distance (Pty) Ltd, Kargo Logistics (Pty) Ltd** or any of it’s subsidiaries or associated companies.
- 2.9 “minimality”** means the principle of only processing information which is necessary or proportionate, but not excessive, in each specific case.
- 2.10 “notice”** means notice in writing and “notify” and “notified” have corresponding meanings.
- 2.11 “operator”** means a natural person or a juristic person who processes a data subject’s personal information on behalf of Kargo in terms of a contract or mandate, without coming under the direct authority of Kargo;
- 2.11.1** Kargo will, in order to pursue and protect its legitimate interests, (and in terms of a written contract) ask operators to process certain categories of data subject’s personal information on Kargo’s behalf.
- 2.12 “PAIA”** means the Promotion of Access to Information Act, No 2 of 2000;
- 2.13 “person”** means a natural person or a juristic person;
- 2.14 “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:-
- 2.14.1** 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 a data subject;
 - 2.14.2** information relating to the education or the medical, financial, criminal or employment history of a data subject;
 - 2.14.3** any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
 - 2.14.4** the biometric information of the person;
 - 2.14.5** the personal opinions, views or preferences of the person;
 - 2.14.6** 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;
 - 2.14.7** the views or opinions of another individual about the person; and
 - 2.14.8** 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.
- 2.15 “policy”** means this this policy;
- 2.16 “POPIA”** shall mean the Protection of Personal Information Act 4 of 2013.
- 2.17 “processing”** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-
- 2.17.1** The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
 - 2.17.2** Dissemination by means of transmission, distribution or making available in any other form; or

2.17.3 Merging, linking, as well as restriction, degradation, erasure or destruction of information.

2.18 “**record**” means any recorded information (regardless of form or medium) including any of the following:

2.18.1 writing on any material;

2.18.2 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 derived from information so produced, recorded or stored;

2.18.3 label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

2.18.4 book, map, plan, graph or drawing;

2.18.5 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;

2.18.6 in the possession or under the control of a responsible party;

2.18.7 whether or not it was created by a responsible party; and

2.18.8 regardless of when it came into existence.

2.19 “**requester**” shall mean any person, including but not limited to a public body or an official thereof, making a request for access to a record held by Kargo.

2.20 “**request for access**” shall mean a request for access to a record held by Kargo in terms of PAIA.

2.21 “**responsible party**” means Kargo including without detracting from the generality thereof, its directors, management, executives, employees, human resources department and consultants who determine the purpose of and means for processing personal information.

2.22 “**special personal information**” includes any information relating to a data subjects

2.22.1 Religious or philosophical beliefs;

2.22.2 Race and ethnic origin;

2.22.3 Trade union membership;

2.22.4 Political persuasion;

2.22.5 Criminal information;

2.22.6 Health or sex life;

2.22.7 Biometric information;

2.22.8 Information concerning children.

3. SCOPE OF THIS POLICY

3.1 for the purposes of **PAIA**, this policy details:

3.1.1 the procedure to be followed by a requester; and

3.1.2 the manner in which a request for access to that information will be facilitated; and

3.2 for the purposes of **POPIA**, amongst other things, this policy details:-

3.2.1 the purpose for which personal information may be processed;

3.2.2 a description of the categories of data subjects for whom Kargo processes personal information as well as the categories of personal information relating to such data subjects; and

3.2.3 the recipients to whom personal information may be supplied.

3.3 For added peace of mind and the avoidance of doubt, Kargo does not share personal information of any data subjects with third parties unless Kargo:

3.3.1 is obliged to provide information for regulatory or legal purposes;

3.3.2 is required to do so for ongoing legal proceedings or future legal proceedings;

3.3.3 is involved in the prevention of fraud, loss, bribery or corruption;

3.3.4 is engaged with the third parties to perform services or to process personal information on Kargo’s behalf;

3.3.5 requires the disclosure to third parties to provide or manage any information, products, or services on behalf of Kargo.

3.4 By engaging with Kargo, you acknowledge that you have reviewed the terms of this notice and the consent to use your personal information, and agree that we may collect, use, and transfer your personal information in accordance therewith.

3.5 If you do not agree with these terms, you may choose not to provide any Personal Information but this may impact on our ability to support you as an employee, customer, supplier, service provider or visitor.

4. COMPANY DETAILS

4.1 The details of Kargo is as follows:

4.1.1 Physical address: M2 West Onramp, Denver, Johannesburg, Gauteng

4.1.2 Postal address: Po Box 75100, Gardenview, Johannesburg, Gauteng

4.1.3 Telephone: +27 86 11 52746

4.1.4 Email: paia@kargo.co.za

4.1.5 Website: www.kargo.co.za

5. CONTACT DETAILS OF THE INFORMATION OFFICER AND DEPUTY INFORMATION OFFICER

5.1 Information Officer: M Erasmus

5.2 Email: paia@kargo.co.za

- 5.3 **Deputy Information Officer:** L de Oliveira
- 5.4 **Email:** paia@kargo.co.za
- 5.5 **Physical address:** M2 West Onramp, Denver, Johannesburg, Gauteng
- 5.6 **Telephone number:** +27 86 11 52746
- 5.7 **Website:** www.kargo.co.za
- 5.8 As a security measure the company will require proof of identity before responding to any requests.

6. THE SOUTH AFRICAN HUMAN RIGHTS COMMISSION

- 6.1 The South African Human Rights Commission (“SAHRC”) has compiled a guide which contains all relevant information and steps to assist any person who wishes to exercise any right as contemplated in PAIA.
- 6.2 The guide is available from the PAIA Unit (Promotion of Access to Information) at the SAHRC:

Postal address: Private Bag 2700, Houghton 2041
Website: www.sahrc.org.za
Telephone: 011 877 3600
Email: PAIA@sahrc.org.za

7. PUBLICATION AND AVAILABILITY OF CERTAIN RECORDS IN TERMS OF PAIA

- 7.1 The schedule of records as contained in Annexure “A” of this manual details the records that are held and/or processed by Kargo for the purposes of PAIA and POPIA respectively.
- 7.2 Such access to such records may not be granted if they are subject to the grounds of refusal which are specified in clause 16 below.

8. LIST OF APPLICABLE LEGISLATION

- 8.1 Kargo retains records which are required in terms of legislation other than PAIA.
- 8.2 Certain legislation provides that private bodies such as Kargo shall allow certain persons access to specified records, upon request.
- 8.3 Legislation that may be consulted to establish whether the requester has a right of access to a record other than in terms of the procedure set out in the PAIA are set out in Annexure “B” hereto.

9. THE PURPOSE FOR PROCESSING PERSONAL INFORMATION

- 9.1 The purpose for processing is set out in Annexure “C1 – C4” hereto.
- 9.2 Kargo will comply with the principles of data protection as outlined within POPIA. We will make

every effort possible in everything we do to comply with the POPIA regulations.

10. KARGO'S GUIDING PRINCIPLES IN PROCESSING PERSONAL INFORMATION AND RECORDS

- 10.1 Kargo will comply with the principles of data protection outlined within the POPIA regulations, and in this regard Kargo will make every possible effort to ensure:

- 10.1.1 the collection and processing of personal data is fair, transparent and lawful. Kargo intends to be transparent as to how data will be used. We will communicate with all data subjects as to what information is being captured, how it is captured, how it will be used and how it will be destroyed upon their request.
- 10.1.2 that the processing of the information will be limited to the purpose for which it is required. We do not hold sensitive personal data.
- 10.1.3 any data collected will be necessary and not excessive for its purpose. Kargo subscribes to the concept of data minimality.
- 10.1.4 the personal information we hold will be accurate and up to date.
- 10.1.5 personal information is not retained for any period longer than is strictly necessary.
- 10.1.6 the integrity and confidentiality of the personal information is secured.

11. CONSEQUENCES OF WITHOLDING CONSENT OR PERSONAL INFORMATION

- 11.1 Should you refuse to provide Kargo with your consent and personal information which is required by us for the purposes indicated in this policy, then we will be unable to engage with you or enter into any agreement or relationship with you. We may further restrict access to any of our premises and/or I.T services.

12. HOW KARGO STORES AND DESTROYS PERSONAL INFORMATION.

- 12.1 Kargo retains personal information for as long as it is necessary to fulfil our legal obligations. Personal data will be deleted or blocked as soon as the purpose for storing it, has ceased to exist. Storage may however take place beyond this point in time if we are legally obliged to do so under law or if there is a necessity for continued storage for a contract conclusion and or contract fulfilment.
- 12.2 In cases where personal information is stored on printed paper, it will be kept in a secure place where unauthorised employees cannot access it.

- 12.3** Printed data will be shredded when it is no longer required by law or when there is no further purposes in retaining such data.
- 12.4** Personal information stored on computers are protected by strong passwords that are changed regularly.
- 12.5** Kargo may store personal information in hardcopy format and/or in electronic format using our own secure on-site servers or other internally hosted technology. Personal Information may also be stored by third parties, via cloud services or other technology, with whom we have contracted with, to support our operations.
- 12.6** These third parties do not use or have access to personal information other than for purposes specified by Kargo, and we require such parties to employ at least the same level of security that we use to protect your personal data.
- 12.7** Data will be regularly backed up in accordance with Kargo's backup procedures.
- 12.8** Kargo has also adopted several policies including:-
- 12.8.1** Acceptable usage of personal information policies;
 - 12.8.2** I.T Security policies;
 - 12.8.3** A clean desk policy, requiring all employees to clear their desks of all personal information when leaving their desks for any length of time at the end of the day;
- 12.9** Information pertaining to data subjects will only ever be accessed through Kargo's VPN which is equipped with:
- 12.9.1** Encryption;
 - 12.9.2** Firewalls;
 - 12.9.3** Verification checks;
- 12.10** Kargo has implemented physical, organisational, contractual and technological security measures to keep all personal information secure, including measures protecting any personal information from loss or theft, and unauthorised access, disclosure, copying, use or modification. Further, Kargo maintains and regularly verifies that the security measures are effective and regularly updates same in response to new risks.
- 12.11** Personal information will be stored electronically in a centralised data base which will be accessible to all within Kargo on a need to know and business basis.

13. ACCESS BY OTHERS AND CROSS BORDER TRANSFER

- 13.1** Kargo does not sell or share personal data with third parties for direct marketing. In order to make

certain services available to our customers, we may need to share associated personal data with some of our service partners.

- 13.2** Personal information may be shared between the companies in the group for the purposes listed in this policy.
- 13.3** Personal information may be passed and/or submitted or acquired by third parties for the prevention of crime, fraud, money laundering and for the tracing of debtors.
- 13.4** Where Personal Information and related data is transferred to a country which is situated outside the borders of South Africa, Kargo will ensure compliance with section 72 of Chapter 9 of **POPIA**, and ensure that the data subjects personal Information will only be transferred to those countries which have similar data privacy laws in place or where the recipient of the Personal Information is bound contractually to a no lesser set of obligations that those imposed by **POPIA**.

14. REQUESTS FOR ACCESS TO PERSONAL INFORMATION IN TERMS OF POPIA

- 14.1** A data subject has the right to request that Kargo provide confirmation as to whether Kargo retains any personal information about a data subject. However, any such request must be accompanied by proof of identification and must be made in accordance with Kargo's **PAIA** process, which is to be found online.
- 14.2** Kargo will attend to any such requests within a reasonable time, at a prescribed fee (if any), in a reasonable manner and format and in a form that is generally understandable.
- 14.3** Kargo will provide a written estimate of the fee prior to providing the access. The fee will be payable upfront.

15. REQUESTS FOR ACCESS TO INFORMATION IN TERMS OF PAIA

- 15.1** A requester must comply with all the procedural requirements as contained in section 53 of PAIA relating to a request for access to a record.
- 15.2** A requester must complete the prescribed Request for access form attached as Annexure "D" and submit the completed request for access form as well as payment of a request fee (if applicable) and a deposit (if applicable), to the information officer at the postal or physical address, facsimile number or electronic mail address stated above.

15.3 The request for access form must be completed with enough detail so as to enable the information officer to identify the following:

- 15.3.1** the record/s requested;
- 15.3.2** the identity of the requester;
- 15.3.3** the form of access that is required, if the request is granted;
- 15.3.4** the postal address or fax number of the requester; and
- 15.3.5** the right that the requester is seeking to protect and an explanation as to why the record is necessary to exercise or protect such a right.

15.4 If a request for access is made on behalf of another person, the requester must submit proof of the capacity in which the requester is making the request to the reasonable satisfaction of the information officer.

15.5 If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally.

15.6 Kargo will consider the request and inform the requester in writing of Kargo's decision within a period of 30 days.

15.7 Kargo's response will include one of the following:

- 15.7.1** The request does not contain enough information to enable Kargo do search for the requested record and additional information is required;
- 15.7.2** The period to search for the record may exceed more than six hours and a deposit will be payable;
- 15.7.3** Kargo has access to the record and the requester may have access to it upon payment of fees raised in accordance with PAIA;
- 15.7.4** The access to the record is refused, for the reasons set out in the reply. If a deposit has been paid, Kargo may refund the deposit but not the request fee.
- 15.7.5** Kargo may or must refuse access to certain portions of the information, but Kargo will give access to the parts that may be disclosed.

16. REFUSAL OF ACCESS TO RECORDS

16.1 Kargo may refuse to grant access to a requested record that falls within a certain category. This includes the following:-

- 16.1.1** Protecting personal information that Kargo holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;
- 16.1.2** Protecting commercial information that the Kargo holds about a third party or Kargo (for example trade secrets: financial,

commercial, scientific or technical information that may harm the commercial or financial interests of the organisation or the third party);

- 16.1.3** If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;
- 16.1.4** If disclosure of the record would endanger the life or physical safety of an individual;
- 16.1.5** If disclosure of the record would prejudice or impair the security of property or means of transport;
- 16.1.6** If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;
- 16.1.7** If disclosure of the record would prejudice or impair the protection of the safety of the public;
- 16.1.8** The record is privileged from production in legal proceedings, unless the legal privilege has been waived;
- 16.1.9** Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of Kargo;
- 16.1.10** Disclosure of the record would put Kargo at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
- 16.1.11** The record is a computer programme; and
- 16.1.12** The record contains information about research being carried out or about to be carried out on behalf of a third party or Kargo.
- 16.1.13** If Kargo has searched for a record and a reasonable belief exists that such record does not exist, the requester will be notified by way of an affidavit or affirmation.

17. RIGHTS

17.1 A data subject has the right to:-

- 17.1.1** Be notified about personal information being collected about a data subject, which is done in accordance with this policy;
- 17.1.2** Be notified in the event of a data subject's personal information being accessed or acquired by any unauthorised person;
- 17.1.3** Establish whether Kargo holds personal information pertaining to that data subject and to request access to their personal data subject to certain exemptions that may apply, which includes the payment of a legally permissible fee.
- 17.1.4** Request the correction of personal information that Kargo holds about a data subject.
- 17.1.5** Request the deletion or destruction of their personal information.

- 17.1.6** Object to processing of your personal information for direct marketing purposes;
- 17.1.7** Object to their personal information being processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69(1) of **POPIA**.

17.2 Kargo does not have an internal appeal process and therefore the decision made by the information officer pertaining to a request for access is final. Should a data subject not be satisfied with the decision of the Kargo information officer, the data subject may approach the Information Regulator and exercise any other external remedies at its disposal.

18. ACCURACY OF INFORMATION AND ONUS

- 18.1** **POPIA** requires that all your personal information are complete, up to date and accurate.
- 18.2** Kargo will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify Kargo if, for example, a change in circumstances mean that the data needs to be updated.
- 18.3** It is the responsibility of Kargo to ensure that any notification regarding the change is noted and acted on.

19. AMENDMENTS AND BINDING ON SUCCESSORS IN TITLE

- 19.1** Kargo reserves the right to amend this policy and consent notice from time to time.

20. BREACHES OF PERSONAL INFORMATION

- 20.1** A Data Breach refers to any incident in terms of which reasonable grounds exist to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person.
- 20.2** Whilst Kargo endeavours to ensure that your personal information is securely processed and stored, data Breach can happen for many reasons, which include:
 - 20.2.1** loss or theft of data or equipment on which personal information is stored;
 - 20.2.2** inappropriate access controls allowing unauthorised use;
 - 20.2.3** equipment failure;
 - 20.2.4** human error;
 - 20.2.5** unforeseen circumstances, such as a fire or flood;
 - 20.2.6** deliberate attacks on systems, such as hacking, viruses or phishing scams; and/or

- 20.2.7** alteration of personal information without permission and loss of availability of personal information.

20.3 Kargo will address any Data Breach in accordance with the terms of **POPIA**, which requires Kargo to notify the Regulator and any affected party in writing (unless the applicable law or a government authority requires that we delay notification to the data subject) in the event of a data breach (or a reasonable belief of a data breach) in respect of that data subject's personal information.

20.4 Kargo will provide such notification as soon as reasonably possible after it has become aware of any data breach in respect of such data subject's personal information.

20.5 Where Kargo acts as an 'operator' for purposes of **POPIA** and should any data breach affect the data of data subjects whose information we process as an operator, Kargo shall (in terms of **POPIA**) notify the relevant responsible party immediately where there are reasonable grounds to believe that the personal information of relevant data subjects has been accessed or acquired by any unauthorized person.

20.6 Breaches for which individual employees are responsible may lead to disciplinary action.

21. INFORMED CONSENT TO PROCESS PERSONAL INFORMATION

- 21.1** By providing Kargo and its operators with personal information you:
 - 21.1.1** consent to the use of the personal information supplied by yourself.
 - 21.1.2** consent and give Kargo permission to process and further process your personal information as and where required and acknowledge that you understand the purposes for which the personal information is required and for which it will be used.
- 21.2** Should any of the Personal Information which has been provided by the personal providing the data concern or pertain to a legal entity whom that person represents, that person confirms that they have the necessary authority to act on behalf of such legal entity and that such person has the right to provide the personal information and required consent to Kargo to process and use the personal information.
- 21.3** Should any of the Personal Information belong to any of a data subjects dependants and/or beneficiaries who are under age, the data subject consents in their capacity as their legal guardian and competent person to provide Kargo the appropriate permission to process their personal information for the purposes for which these details were given.

22. AUDITS, CONTROL AND POLICY CHANGES

22.1 Compliance with this policy and applicable data protection laws will be reviewed by Kargo regularly, at least once a year, on a risk based approach, or on specific request from Kargo's information officer by way of an internal compliance risk assessment, audits including on specific data protection topics and other checks.

22.2 Kargo may update this policy from time to time to ensure that individuals are kept informed of how personal information is used. The company will notify of changes by flagging the updated policy on the company website.

23. ANNEXURE A - CATEGORISATION OF RECORDS HELD

Assignment code	Type of access	Categorisation
1	May be Disclosed	Public Access Document
2	May not be Disclosed	Request after commencement of criminal or civil proceedings [s7]
3	May not be Disclosed	Subject to copyright
4	Limited Disclosure	Personal Information that belongs to the requester of that information [s61]
5	May not be Disclosed	Unreasonable disclosure of personal information Natural person [s63(1)] or Juristic Person (POPI)
6	May not be Disclosed	Likely harm the commercial or financial interest of third party [s64(a)(b)]
7	May not be Disclosed	Likely to harm the company or third party in contract or other negotiations [s64(c)]
8	May not be Disclosed	Would breach a duty of confidence owed to a third party in terms of an Agreement [s65]
9	May not be Disclosed	Likely to compromise the safety of individuals or protection of property [s66]
10	May not be Disclosed	Legally privileged document [s67]
11	May not be Refused	Environmental testing/investigation which reveals public safety/environmental risk [s64(2); s68(2)]
12	May not be Disclosed	Commercial information of Private Body [s68]
13	May not be Disclosed	Likely to prejudice research and development information of the Company or a third party [s69]
14	May not be Refused	Disclosure in public interest [s70]

24. ANNEXURE A – RECORDS CATEGORISATION ASSIGNMENT

Department	Type of record	Assignment code	Type of access
Finance	Audited Financial statements	12	May not be Disclosed
	Tax Records (Company & Employees)	12	May not be Disclosed
	Asset Register	12	May not be Disclosed
	Management Accounts	12	May not be Disclosed
	Financial records of customers	4,5,8	
Human Resources	Employee Records	4,5,9	Limited Disclosure / May not be Disclosed
	Employee Contracts	4,5	Limited Disclosure / May not be Disclosed
Legal	General Contract Documentation	6,12	May not be Disclosed
	Company Guidelines, Policies and Procedures	12	May not be Disclosed
	Statutory and Environmental Records	12	May not be Disclosed
Sales and Marketing	Market Information	12,13	May not be Disclosed
	Sales records and attendances	12, 13	May not be Disclosed
	Marketing and Future service strategies	12	May not be Disclosed
	Current Product Information	1,4	May be Disclosed / Limited Disclosure
	Public Corporate Records	1	May be Disclosed
	Media Releases	1	May be Disclosed
Operations	Performance Records	12	May not be Disclosed
	Customer Information and Database	12	May not be Disclosed
Other	Customers related documentation	6,7,12,13	May not be Disclosed
	Other records not set out herein	To be confirmed on a case by case basis	To be confirmed on a case by case basis

25. ANNEXURE B - RECORDS AVAILABLE IN ACCORDANCE WITH OTHER LEGISLATION

- 25.1 Basic Conditions of Employment Act No. 75 of 1997
- 25.2 Companies Act No. 71/2008
- 25.3 Compensation of Occupational Injuries and Health Diseases Act No.130 of 1993
- 25.4 Consumer Affairs Act No. 71 of 1988
- 25.5 Consumer Protection Act, 68 of 2008
- 25.6 Copyright Act No. 98 of 1978
- 25.7 Credit Agreements Act No. 75 of 1980
- 25.8 Currency and Exchanges Act No. 9 of 1933
- 25.9 Customs and Excise Act No. 91 of 1964
- 25.10 Electronic Communications and Transactions Act, 25 of 2002
- 25.11 Employment Equity Act No. 55 of 1998
- 25.12 Financial Advisory and Intermediary Services Act No. 37 of 2002
- 25.13 Financial Intelligence Centre Act No. 38 of 2001
- 25.14 Financial Markets Control Act No. 55 of 1989
- 25.15 Harmful Business Practices Act No. 23 of 1999
- 25.16 Hazardous Substances Act No. 15 of 1973
- 25.17 Health Act No. 63 of 1977
- 25.18 Income Tax Act No. 58 of 1962
- 25.19 Insolvency Act No. 24 of 1936
- 25.20 Insurance Act No. 27 of 1943
- 25.21 Intellectual Property Laws Amendments Act No. 38 of 1997
- 25.22 Labour relations Act No 66 of 1995
- 25.23 Land Survey Act 8 of 1997
- 25.24 Long Term Insurance Act No. 52 of 1998
- 25.25 National Credit Act National Payment Systems Act No. 78 of 1998
- 25.26 Occupational Health and Safety Act No.85 of 1993
- 25.27 Protection of Businesses Act No. 99 of 1978
- 25.28 Protection of Personal Information Act, 4 of 2013
- 25.29 Regulation of Interception of Communications and Provision of Communication Related Information Act, 70 of 2002
- 25.30 Road Transport Act No. 74 of 1977
- 25.31 Second Hand Goods Act No. 23 of 1955
- 25.32 Short Term Insurance Act No. 53 of 1998
- 25.33 Skills Development Levies Act No. 9 of 1999
- 25.34 Skills Development Act No. 97 of 1998 Stamp Duties Act No. 77 of 1968
- 25.35 The Constitution of the Republic of South Africa, 1996
- 25.36 The Cybercrimes Act, 19 of 2020
- 25.37 Trade Marks Act No. 194 of 1993
- 25.38 Unemployment Contributions Act No. 4 of 2002
- 25.39 Unemployment Insurance Act No. 30 of 1966
- 25.40 Value-Added Tax Act No. 89 of 1991

26. ANNEXURE C1 – INFORMATION PROCESSED PERTAINING TO EMPLOYEES

	Type of Information Collected	Purpose for processing information
Employees (Including full time salaries staff, wage staff and directors) and prospective employees	Contact information, such as name, alias, address, identity and/or registration number, phone number, cell phone number, vehicle make and registration number, and similar contact details	Management of Employees Employee wellness programmes The performance of HR related functions General communications
	Career, education and employment related information such as job preferences or interest, work performance or history, salary history, nationality and immigration details, demographic data, professional licensing requirements, compliance activities, accreditations and educational history, and similar data.	To conclude employment contracts and to manage recruitment. Succession planning. Promotions and demotions General communication Due diligence Verifying details and credentials
	Race and disability related information (“ Special Personal Information ”)	Compliance with BBBEE laws
	Religion (“ Special Personal Information ”)	Correct and fair treatment issues
	Sexual and Medical History (“ Special Personal Information ”)	Correct and fair treatment issues
	Trade Union affiliation (“ Special Personal Information ”)	Correct and fair treatment issues
	Financial, Credit and Criminal history (“ Special Personal Information ”)	To perform risk assessments and to protect Kargo’s legitimate interests
	Children’s details (“ Special Personal Information ”)	Benefits related
	Biometrics such as fingerprints and employee images, which include still pictures, videos, voice and other data (“ Special Personal Information ”)	Required for access to Kargo’s premises and to provide access to Kargo’s IT infrastructure Required for security and monitoring information and to comply with Health and Safety Laws.
	Family members details	Benefits related
	Tax and Financial Information, such as banking details, tax registration numbers	To perform contractually and to comply with Kargo’s tax duties and obligations.
	IT information which will include IT user names and passwords, authentication methods and roles which are required for various legitimate interests and lawful reasons.	Required for access to Kargo’s premises and to provide access to Kargo’s IT infrastructure
	Payroll records and banking details	Contractual and Employment related matters and to comply with laws and duties.
	Health History and records (“Special Personal Information”)	Contractual and Employment related matters and to comply with laws and duties.
	Private or confidential correspondence received from an employee for investigative and / or security purposes as well as for employment, legal or contractual purposes.	Investigative and/security purposes Legal Purposes Contractual purposes
Social Media and online activities and presence, such as posts and similar data.	Contractual and employment related matters and to comply with Kargo’s public duties	
Training records, Electronic access records, Surveillance records	Contractual and Employment related matters and to comply with laws and duties.	

27. ANNEXURE C2 – CUSTOMER INFORMATION PROCESSED

Data Subject	Type of Information Collected	Purpose for processing information
Customers	Contact information, such as name, alias, address, identity and/or registration number, phone number, cell phone number, vehicle make and registration number, and similar contact details.	Authenticating access to Kargo's systems Due diligence General communications Verifying details Statistical analysis In connection with legal proceedings
	Credit bureau reports and financial history	Due diligence To perform risk assessments Verification of details To detect and protect against fraud, or other criminal or malicious activity To effectively manage any insurance requirements;
	All information captured on credit applications, rate applications, suretyships, handheld devices, in vehicle computers, tables and other mobile devices, website forms and information conveyed telephonically by customers	Due diligence To perform contractually Verification of details Statistical analysis In connection with legal proceedings To pursue Kargo's business objectives and strategies
	MYKARGO login details and other IT related information which includes usernames, passwords, account numbers, authentication methods and roles	Authenticating access to Kargo's services and improving Kargo's information security General risk management, security and emergency incident control as well as for providing IT access and support and for authentication and for data and cybersecurity purposes.
	Tax and Financial Information, such as banking details, tax registration numbers	To perform contractually To comply with tax duties and obligations. To process debits and credits
	Information recorded on waybills, rate enquiries, quotations and estimates	To perform contractually To provide customer support To investigate claims and disputes To report claims and disputes
	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 customer. (" Special Personal Information ")	Correct and fair treatment issues To perform contractually To attend to queries, complaints and claims To comply with all legal obligations Statistical analysis
	All correspondence, including private or confidential correspondence received from customers	Investigative and/security purposes Legal Purposes Contractual purposes
	Other publicly available personal data, including any information shared on a public platform (such as Facebook, Twitter, or public feed).	Due diligence In connection with legal proceedings To pursue Kargo's business objectives and strategies
	The name of the data subject 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;	To perform contractually To provide customer support To investigate claims and disputes To report claims and disputes

28. ANNEXURE C3 – THIRD PARTY SERVICE PROVIDERS AND SUPPLIERS

Data Subject	Type of Information Collected	Purpose for processing information
Suppliers Sub-contractors	Contact information, such as name, alias, address, identity and/or registration number, phone number, cell phone number, vehicle make and registration number, and similar contact details.	Due diligence General communications Verifying details Statistical analysis In connection with legal proceedings
Contractors Service providers	Third party information such as CIPC records, Credit bureau reports and financial history	Due diligence To perform risk assessments Verification of details To detect and protect against fraud, or other criminal or malicious activity To effectively manage any insurance requirements;
	Supplier agreements	Due diligence To perform contractually Verification of details Statistical analysis In connection with legal proceedings To pursue Kargo's business objectives and strategies
	Tax and Financial Information, such as banking details, tax registration numbers	To perform contractually To comply with tax duties and obligations. To process debits and credits
	Training records, Surveillance records	Contractual and Employment related matters and to comply with laws and duties. Due diligence In connection with legal proceedings
	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. (" Special Personal Information ")	Correct and fair treatment issues To perform contractually To attend to queries, complaints and claims To comply with all legal obligations Statistical analysis
	All correspondence, including private or confidential correspondence received	Investigative and/security purposes Legal Purposes Contractual purposes
	Other publicly available personal data, including any information shared on a public platform (such as Facebook, Twitter, or public feed).	Due diligence In connection with legal proceedings To pursue Kargo's business objectives and strategies
	The name of the data subject 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;	To perform contractually To provide customer support To investigate claims and disputes To report claims and disputes

29. ANNEXURE C4 – SHAREHOLDER INFORMATION PROCESSED

Data Subject	Type of Information Collected	Purpose for processing information
Shareholders	Shareholders personal information	Due diligence General communications Verifying details Statistical analysis To perform contractually

30. ANNEXURE C4 – VISITORS INFORMATION PROCESSED

Data Subject	Type of Information Collected	Purpose for processing information
Visitors	Physical access records	Security related purposes
	Biometric information	Security related purposes
	Electronic access records, scans and photographs	Security related purposes
	Surveillance records (e.g. CCTV footage)	Security related purposes

REQUEST FOR ACCESS TO RECORD OF KARGO

F. Form of access to record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 below, state your disability and indicate in which form the record is required.

Disability:	Form in which record is required:
Mark the appropriate box with an X .	
NOTES:	
(a) Compliance with your request for access in the specified form may depend on the form in which the record is available.	
(b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.	
(c) The fee payable for access to the record, if any, will be determined partly by the form in which access is requested.	

1. If the record is in written or printed form:					
	copy of record*		inspection of record		
2. If record consists of visual images - (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.):					
	view the images		copy of the images*	transcription of the images*	
3. If record consists of recorded words or information which can be reproduced in sound:					
	listen to the soundtrack (audio cassette)		transcription of soundtrack* (written or printed document)		
4. If record is held on computer or in an electronic or machine-readable form:					
	printed copy of record*		printed copy of information derived from the record*	copy in computer readable form* (stiffy or compact disc)	

*If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.	YES	NO
--	-----	----

G. Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Indicate which right is to be exercised or protected:

.....

.....

.....

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

.....

.....

.....

REQUEST FOR ACCESS TO RECORD OF KARGO

H. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved / denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

.....

Signed at this day..... ofyear

.....
SIGNATURE OF REQUESTER /
PERSON ON WHOSE BEHALF REQUEST IS MADE

32. PAIA FEES**APPENDIX B****PRESCRIBED FEES**

(Section 54(7) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)) [Regulation 11 (3)]	
1 PLEASE NOTE THAT ALL PRICES LISTED BELOW ARE INCLUSIVE OF VALUE-ADDED TAX (VAT)	
(a) For every photocopy of an A4-size page or part thereof	R 1.25
(b) For every printed copy of an A4-size page of part thereof held on a computer or in an electronic or machine-readable form	R 0.85
(c) For a copy in a computer-readable form on	
(i) stiffy disc	R 8.55
(ii) compact disc	R79.80
(d) (i) For a transcription of visual images, for an A4-size page or part thereof	R45.60
(ii) For a copy of visual images	R68.40
(e) (i) For a transcription of an audio record, for an A4-size page or part thereof	R22.80
(ii) For a copy of an audio record	R34.20
(f) To search for and prepare the record for disclosure – R34.20 for each hour or part thereof reasonably required for such search and preparation.	
[Section 54(2) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)] [Regulation 11 (3)]	
2 PLEASE NOTE THAT ALL PRICES FOR THE ITEMS LISTED BELOW ARE INCLUSIVE OF VALUE-ADDED TAX (VAT)	
(a) Six hours as the hours to be exceeded before a deposit is payable; and	
(b) One third of the access fee is payable as a deposit by the requester.	
[Section 54(7) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)] [Regulation 11 (3)]	
3 PLEASE NOTE THAT THE PRICE FOR THE ITEMS LISTED BELOW IS INCLUSIVE OF VALUE-ADDED TAX (VAT)	
The actual postage fee is payable when a copy of a record must be posted to a requester.	

ADDITIONAL PRESCRIBED INFORMATION

The Minister of Justice has prescribed no additional information.