KONICA MINOLTA

# JOHANNESBURG BUSINESS SYSTEMS
# t/a Johannesburg Konica Minolta
# "JKM"

| | |
|---|---|
| **Policy Name** | **POPIA and PAIA Compliance Management Framework and Manual** |
| **Version number** | 1/2022 |
| **Policy sponsor** | Margie Burchell De Villiers |

## Approval process

| MANAGER/ POSITION | NAME | SIGNATURE | DATE |
|---|---|---|---|
| INFORMATION OFFICER / MANAGING DIRECTOR | MARGIE DE VILLIERS BURCHELL | | 23.8.22 |
| DEPUTY INFORMATION OFFICER / GENERAL MANAGER | JANE CALLEBAUT | | 23-08-22 |

| Document Confidentiality | | |
|---|---|---|
| Public | Private | Restricted |
| X | | |

1. INTRODUCTION 4
2. PURPOSE OF THE POPIA COMPLIANCE MANAGEMENT FRAME-WORK 4
3. SCOPE 5
4. OBJECTIVE OF THE POPIA COMPLIANCE MANAGEMENT FRAMEWORK 5
5. APPLICABLE PRINCIPLES 5
5.1 Principle 1: Accountability 5
5.2 Principle 2: Processing limitation 5
5.3 Principle 3: Specific purpose 6
5.4 Principle 4: Limitation on further processing 6
5.5 Principle 5: Information quality 6
5.6 Principle 6: Transparency/ openness 6
5.7 Principle 7: Security safeguards 6
5.8 Principle 8: Data Subject participation 6
6. PURPOSE OF THE PROCESSING OF PERSONAL INFORMATION 6
7. CATEGORIES OF DATA SUBJECTS AND PERSONAL INFORMATION/ SPECIAL PERSONAL INFORMATION 7
8. CROSS-BORDER FLOWS OF PERSONAL INFORMATION 7
10. DESCRIPTION OF INFORMATION SECURITY MEASURES TO BE IMPLEMENTED BY JKM 8
11. OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION BY A DATA SUBJECT 8
12. REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION 8
13. DATA PROTECTION IMPACT ASSESSMENT(GDPR) 8
14. RIGHT TO DATA PORTABILITY (GDPR) 9
SECTION B: PAIA 10
15. INTRODUCTION 10
16. GUIDE OF THE SOUTH AFRICAN HUMAN RIGHTS COMMISSION AND THE INFORMATION REGULATOR (SOUTH AFRICA) 11
17. ACCESS TO RECORDS HELD BY JKM 11
17.1 Personal Requester 11
17.2 Other Requester 11
17.3 Request Procedure 12
17.4 Decision 12

17.5 Grounds for refusal of access to records in terms of PAIA 13
17.6 Remedies available to the requester upon refusal of a request for access in terms of PAIA 14
17.6.1 Internal remedies: 14
17.6.2 External remedies: 14
18. FEES 14
19. CATEGORIES OF RECORDS HELD BY JKM: SECTION 51(1)(E) 15
19.1 Financial records 15
19.2 Agreements or contract records 15
19.3 Employees 15
19.4 Company policies and directives 15
19.5 Regulatory 15
19.6 Client information 15
19.7 Systems, solutions and information technology 15
19.8 Reference materials 16
SECTION C: INFORMATION OFFICER 17
20. INTRODUCTION 17
21. GENERAL RESPONSIBILITIES OF INFORMATION OFFICER 17
SECTION D: OPERATIONAL CONSIDERATIONS 18
22. POPIA / PAIA COMPLIANCE PROCESS 18
23. OPERATING CONTROLS 19
SECTION E: GDPR 20
24. EU General Data Protection Regulation 20
ANNEXURE 1 21
ANNEXURE 2 22
ANNEXURE 3 24
ANNEXURE 4 27
ANNEXURE 5 30

## SECTION A: POPIA

---

### 1. INTRODUCTION

The Protection of Personal Information Act 4 of 2013, (POPIA) Compliance Management Framework consists of policies, processes, standards, systems, and structures that help identify and manage the risks around the processing of personal information. The success of a Framework relies heavily on the commitment and attitude of all employees and Management.

We are committed to compliance with the Protection of Personal Information Act (POPIA). Chapter 3 of POPIA provides for the minimum conditions for lawful processing of personal information by a responsible party. These conditions may not be derogated from unless specific exclusions apply as outlines in POPIA. JKM is the Responsible Party as defined in POPIA.

This policy and compliance framework establishes measures and standards for the protection and lawful processing of personal information within our organisation and provides principles regarding the right of individuals to privacy and to responsible safeguarding of their personal information.

### 2. PURPOSE OF THE POPIA COMPLIANCE MANAGEMENT FRAMEWORK

The purpose of the POPIA Compliance Management Framework is to establish and implement an appropriate strategic framework that defines the responsibilities of both management and employees and facilitates the implementation, monitoring and reporting on robust practices and standards for the effective management of compliance obligations regarding the processing of personal information. The establishment of an effective compliance management framework will reduce and/or mitigate the following risks:

- Damage to JKM's reputation.
- Inadequate internal control systems and processes that may lead to fraud, corruption, unlawful processing and/or inefficiencies in the processing of personal information.
- Non-compliance with regulatory requirements.
- Financial loss.

JKM's POPIA Compliance Framework and procedures including processes as set-out here, gives effect to the compliance policy.

# 3. SCOPE

This Framework applies to all JKM's employees and relevant stakeholders. Employees are those who are permanent, temporary, or casual and include contractors and consultants. This document outlines the structure, measures, principles, standards, and key processes that JKM will implement to ensure compliance with obligations expected by its own data and information governance structures and the Information Regulator.

# 4. OBJECTIVE OF THE POPIA COMPLIANCE MANAGEMENT FRAMEWORK

The object of a POPIA Compliance Management Framework is to:

- Promote a culture of compliance and responsibility within JKM, when processing personal information and highlighting its importance and connection to JKM's corporate culture;
- Foster continuous improvement in compliance processes, systems, and standards ensuring obligation are always met by establishing monitoring and reporting mechanisms that will assist in identifying and assessing on non-compliance and tracking remedial actions;
- Maintain and grow JKM's reputation in the marketplace and;
- Demonstrate JKM's corporate and social responsibility with regard to processing personal information.

# 5. APPLICABLE PRINCIPLES

## 5.1 Principle 1: Accountability

To ensure that reasonable steps are taken to ensure that personal information obtained from Data Subjects, it is legally obtained, processed responsibly, stored securely, and destroyed responsibly. This includes all personal information about JKM's employees and other stakeholders, including customers (hereinafter referred to as 'Data Subjects').

## 5.2 Principle 2: Processing limitation

Personal information must only be collected directly from Data Subjects to the extent required. The information must only be processed with the consent of the Data Subjects and only used for the purpose for which it was obtained. Information, which is by law required to be released, must be done in accordance with the defined legal parameters. In this event, the Data Subject must be informed.

## 5.3 Principle 3: Specific purpose

Personal information must only be processed for the specific purpose for which it was obtained and must not be retained for any longer than it is needed to achieve such purpose.

## 5.4 Principle 4: Limitation on further processing

Further processing of personal information must be compatible with the initial purpose for which the information was collected. Information is collected for the purposes of providing services to Data Subjects and for employment purposes.

## 5.5 Principle 5: Information quality

JKM must ensure that personal information held is accurate and updated regularly and that the integrity of the information is maintained by appropriate security measures. The information must be complete, up to date and accurate. It will therefore be necessary for Data Subjects to update their information and confirm that it is still relevant.

## 5.6 Principle 6: Transparency/ openness

There must be transparency between the Data Subject and JKM.

## 5.7 Principle 7: Security safeguards

JKM must take reasonable steps to ensure that adequate safeguards are in place to ensure that personal information is being used responsibly and is not unlawfully accessed. Technical and organisational measures will be used to ensure the integrity of personal information, and guard against the risk of loss, damage, or destruction. JKM is committed to ensuring that information is only used for legitimate purposes with the consent of Data Subjects and only by authorised employees.

## 5.8 Principle 8: Data Subject participation

The Data Subject must be made aware that their information is being processed and must have provided their informed consent to such processing. They are entitled to correct and update any information held by JKM, on a regular basis.

# 6. PURPOSE OF THE PROCESSING OF PERSONAL INFORMATION

As outlined in paragraph 5.3 above, personal information may only be processed for a specific purpose. The purposes for which JKM processes or will process personal information is set out an Annexure 1.

## 7. CATEGORIES OF DATA SUBJECTS AND PERSONAL INFORMATION/ SPECIAL PERSONAL INFORMATION

As per section 1 of POPIA, a Data Subject may either be a natural or a juristic person. Annexure 1 sets out various categories of Data Subjects that JKM processes personal information on and the types of personal information relating thereto.

## 8. CROSS-BORDER FLOWS OF PERSONAL INFORMATION

Section 72 of POPIA provides that personal information may only be transferred out of the Republic:

a) If the recipient country can offer such data an "adequate level" of protection. This means that its data privacy laws must be substantially like the Conditions for Lawful Processing as contained in POPIA; or
b) If the Data Subject consents to the transfer of their personal information; or
c) If the transfer is necessary for the performance of a contractual obligation between the Data Subject and JKM; or
d) If the transfer is necessary for the performance of a contractual obligation between JKM and a third party, in the interests of the Data Subject; or
e) If the transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were, the Data Subject, would likely provide such consent.

JKM does not do any cross-border transfers of any personal information relating to employees, members, companies or organisations.

In the event that JKM does cross-border transfers, it acknowledges and will comply with the requirements of the General Data Protection Rules of the European Union (GDPR). The GDPR specifies that a cross-border transfer is allowed based on international agreements for judicial cooperation. The grounds for a cross-border transfer includes the transfer being made from a register which, according to the EU or a Member States' law, is intended to provide information to the public, and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case.

## 10. DESCRIPTION OF INFORMATION SECURITY MEASURES TO BE IMPLEMENTED BY JKM

Section D of Annexure 1 sets out the types of security measures to be implemented by JKM to ensure that personal information is respected and protected.

A preliminary assessment of the suitability of the information security measure implemented or to be implemented by JKM may be conducted in order to ensure that the personal information that is processed by JKM is safeguarded and processed in accordance with the Conditions for Lawful Processing.

## 11. OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION BY A DATA SUBJECT

Section 11(3) of POPIA and regulation 2 of the POPIA Regulations provides that a Data Subject may at any time object to the processing of his/hers/its personal information in the prescribed form attached to this framework as Annexure 2 subject to exceptions contained in POPIA.

## 12. REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION

Section 24 of POPIA and regulation 3 of the POPIA Regulations provides that a Data Subject may request for their personal information to be corrected / deleted in the prescribed form attached as Annexure 3 to this framework.

## 13. DATA PROTECTION IMPACT ASSESSMENT(GDPR)

The GDPR sets out requirements for conducting Data Protection Impact Assessments ('DPIAs'). A data controller is required to, where necessary, carry out a review to assess whether the processing of personal data is in accordance with the DPIA, particularly when there is a change in risks to processing operations. If the personal information of EU subjects is being processed, the provisions of this clause will become applicable.

DPIA will be conducted if:

- a data controller utilises new technologies to process personal data;
- the processing may result in a high risk to the rights and freedoms of an individual;
- when a systematic and extensive evaluation of personal aspects relating to natural persons is involved, which is based on automated processing or profiling;
- there is processing on a large scale of special categories of data; and
- there is systematic monitoring of a publicly accessible area on a large scale.

The assessment will contain at least the following:

- a systematic description of the envisaged processing;
- operations and legitimate purposes of the processing;
- the necessity and proportionality of the operations in relation to the purposes; and
- the risks to the rights and freedoms of Data Subjects.

A data controller must consult the supervisory authority prior to any processing that would result in a high risk in the absence of risk mitigation measures as indicated by the DPIA.

POPIA does not contain equivalent provisions regarding a DPIA. However, Section 4(b) of the POPIA Regulations outline that the responsibilities of Information Officers include ensuring a personal information impact assessment is conducted to make certain that adequate measures and standards exist to enable compliance with the conditions for the lawful processing of personal information.

## 14. RIGHT TO DATA PORTABILITY (GDPR)

Unlike the GDPR, POPIA does not refer to a right to data portability. The GDPR defines the right to data portability as the right to receive data processed based on contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format' and to transmit that data to another controller without hindrance. The GDPR does not explicitly limit the scope of the right to data portability to special categories of personal data. EU Data Subjects' rights of portability are acknowledged.

## SECTION B: PAIA

## 15. INTRODUCTION

The Promotion of Access to Information Act 2 of 2000, (PAIA) gives third parties the right to approach private bodies and the government to request information held by them, which is required in the exercise and/or protection of any rights. On request, the private body or government is obliged to release such information unless PAIA expressly states that the records containing such information may or must not be released. This manual informs requestors of procedural and other requirements which a request must meet as prescribed by PAIA.

**Nature of Business**

The Company is an incorporated company, focused on providing office automation equipment and solutions with related activities.

**Contact Details**

| | |
|---|---|
| Name of body: | Johannesburg Business Systems trading as Johannesburg Konica Minolta |
| Head of body: | Margie De Villiers Burchell |
| Information Officer: | Margie De Villiers Burchell |
| Deputy Information Officer: | Jane Callebaut |
| Physical address: | 93 Boeing Road East |
| | Bedfordview 2007 |
| Postal address: | PO Box 337 |
| | Kengray 2100 |
| Telephone number: | 011 453 5333 |
| Email address: | margie@jhbkonicaminolta.co.za |
| | jane@jhbkonicaminolta.co.za |

## 16. GUIDE OF THE SOUTH AFRICAN HUMAN RIGHTS COMMISSION AND THE INFORMATION REGULATOR (SOUTH AFRICA)

A guide to PAIA is available from the South African Human Rights Commission. The guide contains such information as may be reasonably required by a person who wishes to exercise any right contemplated in PAIA. Any enquires regarding this guide and its contents should be directed to:

The Information Regulator (South Africa)

Physical address: D House, 27 Stiemens Street, Braamfontein 2001

Postal address: PO Box 31533 Braamfontein 2017

Tel: 010 023 5241/42

Complaints Email: complaints.IR@justice.gov.za

General Enquiries: inforeg@justice.gov.za

Website: https://justice.gov.za/inforeg/index.html

## 17. ACCESS TO RECORDS HELD BY JKM

Records held by JKM may be accessed on request only once the requirements for access have been met. A requester is any person making a request for access to a record of JKM and in this regard, PAIA distinguishes between two types of requesters:

### 17.1 Personal Requester

A personal requester is a requester who is seeking access to a record containing personal information about the requester. Subject to the provisions of PAIA and applicable law, JKM will provide the requested information, or give access to any record about the requester's personal information. The prescribed fee for reproduction of the information will be charged by JKM.

### 17.2 Other Requester

This requester (other than a personal requester) is entitled to request access to information pertaining to third parties. However, JKM is not obliged to grant access prior to the requester fulfilling the requirements for access in terms of PAIA. The prescribed fee for reproduction of the information will be charged by JKM.

## 17.3 Request Procedure

A requester must comply with all the procedural requirements contained in PAIA relating to a request for access to a record. A requester must complete the request from attached hereto as Annexure 4 and submit it, as well as the payment of a requester fee, if applicable to the Information Officer or Deputy Information Officer at the physical address or email address as stated herein. The request from must be filled in with enough information to at least enable the Information Officer to identify:

- The record or records requested
- The identity of the requester
- What form of access is required?
- The postal address, fax, or email address of the requester.

A requester must state that he or she requires the information to exercise or protect a right, and clearly state what the nature of the right is, so to be exercised or protected. The requester must also provide an explanation of why the requested record is required for the exercise or protection of that right.

JKM will process a request within 30 days, unless the requester has stated special reasons which would satisfy the Information Officer/Deputy Information Officer that circumstances dictate that this period not be complied with.

The requester shall be informed in writing whether access has been granted or denied. If, in addition, the requester requires the reasons for the decision in any other manner, he or she must state the way it is required. If a request is made on behalf of another person, the requester must then submit proof of the capacity in which the requester is making the request to the satisfaction of the Information Officer or the Deputy Information Officer.

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

## 17.4 Decision

JKM will decide whether to grant or decline a request and give notice with reasons(if required) to that effect. The 30-day period within which JKM has to decide whether to grant or refuse a request, may be extended for a further period of not more than 30 days if the request is for a large quantity of information, or the request requires a search for information that has been backup up and stored offsite and the information cannot reasonably be obtained within the original 30-day period. The Information Officer/Deputy Information Officer will notify the requester in writing should an extension be necessary.

## 17.5 Grounds for refusal of access to records in terms of PAIA

The following are the grounds on which JKM may, subject to the exceptions contained in Chapter 4 of PAIA, refuse a Request for Access in accordance with Chapter 4 of PAIA.

17.5.1 Mandatory protection of the privacy of a third party who is a natural person, including a deceased person, where such disclosure of personal information would be unreasonable.

17.5.2 Mandatory protection of the commercial information of a third party, if the records contain:

a) Trade secrets of that third party;

b) Financial, commercial, scientific, or technical information of the third party, the disclosure of which could likely cause harm to the financial or commercial interests of that third party; and/ or

c) Information disclosed in confidence by a third party to JKM, the disclosure of which could put that third party at a disadvantage in contractual or other negotiations or prejudice the third party in commercial competition.

17.5.3 Mandatory protection of confidential information of third parties if it is protected in terms of any agreement.

17.5.4 Mandatory protection of the safety of individuals and the protection of property.

17.5.5 Mandatory protection of records that would be regarded as privileged in legal proceedings.

17.5.6 Protection of the commercial information of JKM, which may include:

a) Trade secrets;

b) Financial /commercial, scientific, or technical information, the disclosure of which could likely cause harm to the financial or commercial interests of JKM;

c) Information which, if disclosed, could put JKM at a disadvantage in contractual or other negotiations or prejudice JKM in commercial competition; and/or

d) Computer programmes which are owned by JKM, and which are protected by copyright and intellectual property laws.

17.5.7 Research information of JKM or a third party, if such disclosure would place the research or the researcher at a serious disadvantage, and

17.5.8 Requests for records that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources.

## 17.6 Remedies available to the requester upon refusal of a request for access in terms of PAIA

### 17.6.1 Internal remedies:

JKM does not have internal appeal procedures. As such, the decision made by the Information Officer/Deputy Information Officer is final, and requesters will have to exercise such external remedies at their disposal if the Request for Access is refused.

### 17.6.2 External remedies:

In accordance with sections 56(3)(c) and 78 of PAIA, a requester may apply to a court for relief within 180 days of notification of the decision for appropriate relief.

## 18. FEES

PAIA provides for two types of fees:

Fees are set out in Annexure 5.

A request fee, (which will be a standard fee) and an access fee, which must be calculated by considering reproduction costs, search and preparation time and cost, as well as postal / delivery costs where applicable. When a request is received by the Information Officer/Deputy Information Officer, the relevant Officer shall by notice require the requester, other than a personal requester, to pay the prescribed request fee, if any, before further processing of the request can take place. If a search for the information is necessary and the preparation and disclosure of the information for disclosure, requires more time than prescribed in the regulations for this purpose, the Information Officer/Deputy Information Officer shall notify the requester to pay a deposit if the request is granted.

The Information Officer/Deputy Information Officer shall withhold information until the requester has paid the fee as indicated. A requester whose request for access to information has been granted, must pay an access fee for reproduction, search, preparation, and for any time in excess of the prescribed hours to prepare the information for disclosure including making arrangements to make it available in the request form. If a deposit has been paid in respect for access, which is refused, then the Information Officer/Deputy Information Officer shall cause a refund of the deposit to be paid to the requester.

## 19. CATEGORIES OF RECORDS HELD BY JKM: SECTION 51(1)(E)

### 19.1 Financial records

- Financial statements of JKM
- Insurance Information

### 19.2 Agreements or contract records

- Standard agreements
- Contracts concluded with third party service providers
- Supplier contracts

### 19.3 Employees

- List of employees
- Personal information of employees
- Employee contracts of employment
- Salaries of employees
- Leave records
- Personnel files of employees
- Performance appraisals
- Training records

### 19.4 Company policies and directives

- Internal policies and directives relating to employees and JKM

### 19.5 Regulatory

- Licenses or Authorities

### 19.6 Client information

- Customer details
- Contact details of customers
- Communications with customers

### 19.7 Systems, solutions, and information technology

- Intellectual property pertaining to solutions and products used
- Usage of solutions and products

## 19.8 Reference materials

- Newsletters and Journal Articles
- Magazines
- Newspaper articles

## SECTION C: INFORMATION OFFICER

---

### 20. INTRODUCTION

POPIA and PAIA require the appointment of an Information Officer and permit them to delegate any power or duty to a Deputy Information Officer, as necessary to make the body as accessible as reasonably possible. In terms of section 55(2) of POPIA, Information Officers and Deputy Information Officers shall take up their duties only after being registered with the Information Regulator. These so registered Information Officers and Deputies are the same Information Officers as referred to in section 1, 14 and 51 of PAIA. The Information Officers of public and private bodies perform their duties and responsibilities in terms of both POPIA and PAIA.

JKM acknowledges the contents of and will comply with the Guidance Note on Information Officers and Deputy Information Officers of the Information Regulator dated 1 April 2021.

### 21. GENERAL RESPONSIBILITIES OF INFORMATION OFFICER

The Information Officer will:

- Be registered with the Regulator
- Encourage compliance
- Develop, implement, monitor, and maintain a POPIA and PAIA Compliance Management Framework
- Deal with requests
- Handle complaints
- Assist the Regulator with investigations
- Ensure compliance with the policies developed within the framework
- Support training and awareness
- Submit annual reports as required to the Regulator

## SECTION D: OPERATIONAL CONSIDERATIONS

---

### 22. POPIA / PAIA COMPLIANCE PROCESS

Management and the Information Officer are responsible for administering and overseeing the implementation of this framework and policy and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes. All employees, associates and individuals directly associated with JKM will be trained, according to their functions, in the regulatory requirements, policies, guidelines that govern the protection of personal information, and access thereto. Periodic reviews, audits and gap analyses will be conducted to evaluate, maintain, and improve an effective and responsive monitoring system within JKM and its use of personal information.

The content of this compliance framework depends on JKM's business activities. It is based on the principles of good governance, proportionality, transparency, and sustainability. JKM is committed to compliance with POPIA and PAIA, regulations, codes of conduct and organisational standards, as well as standards of good corporate governance, best practices, ethics and Data Subject expectations.

JKM will develop and implement a POPIA/ PAIA compliance process that includes effective monitoring practices. The compliance process will encompass compliance risk identification, compliance risk assessment, compliance risk management and compliance monitoring. This plays an essential role in assisting management to discharge its responsibility to comply with applicable regulatory requirements in respect of POPIA and PAIA. The function presently is performed by the Director/Information Officer. The following methodology form an integral part of the POPIA / PAIA compliance process:

a) Methodology I - Compliance risk identification

All the POPIA/ PAIA regulatory requirements that have been identified together form the regulatory universe of JKM in respect of POPIA and PAIA.

b) Methodology II - Compliance risk assessment

The Information Officer/Deputy Information Officer will prioritise the regulatory requirements by rating each according to their risk.

b) Methodology III - Compliance risk management

Control measures that will ensure compliance and facilitate the implementation thereof.

c) Methodology IV - Compliance risk monitoring and reporting

The controls that have been implemented will be monitored to determine the level of compliance and whether the controls are effective; this will also include reporting on the findings to the Regulator.

JKM acknowledges that the compliance process is an important activity. This process enables the Information Officer/Deputy Information Officer to identify, prioritise, manage and monitor the POPIA/PAIA compliance risks that face JKM thereby significantly reducing the potential for non-compliance with the regulatory requirements and industry norms.

## 23. OPERATING CONTROLS

JKM shall establish appropriate standard operating procedures that are consistent with this policy and regulatory requirements. This will include:

- Review of information security responsibilities and allocation to a responsible person;
- Data Breach Policy;
- Incident reporting and management;
- User ID addition or removal;
- Information security training and education; and
- Data backup.

## SECTION E: GDPR

### 24. EU General Data Protection Regulation

GDPR and POPIA are very similar in that they set out to protect personal information/data. The main difference is the mismatch of the effective dates. In respect of GDPR, which was effective from May 2018, South African businesses must comply with POPIA effective from 1 July 2021.

As far as GDPR is concerned, South African businesses will have to comply with the EU data protection regulations when processing the data of EU subjects i.e., by providing services to or doing business with an EU partner (including UK, despite Brexit) or by holding personal information of an EU Data Subject.

JKM's compliance with POPIA in respect of the processing and safe-keeping (protection) of personal information, is in line with the GDPR. See provisions relating to GDPR under Section A.

# ANNEXURE 1

## Processing of Personal Information

### A. Purpose of Processing

JKM uses personal information under its care in the following manner:

- Administration
- Rendering services according to contractual agreements/instructions/mandate
- Staff administration
- Complying with company, labour, tax, and employment laws
- Keeping records of account

### B. Categories of Data Subjects and their Personal Information

JKM may possess records relating to suppliers, shareholders, service providers, staff, vendors and employees:

| Data Subject | Information Processed |
|---|---|
| Employees - Natural persons | Names, contact details, physical and postal address, date of birth, ID numbers, tax related information, banking details, nationality, gender, confidential information, pregnancy, marital status, ethnicity, age, language , education information, financial information, employment history, health/ well-being details, criminal behaviour |
| Employers -Juristic persons / entities | Names of contact persons, name of legal entity, physical and postal address, contact details, Registration number, banking details, authorised signatories, beneficial owners |
| Service Providers | Names of contact persons, name of legal entity, physical and postal address, contact details, Registration number, founding documents, tax related information, banking details, authorised signatories, beneficial owners |
| Vendors | Names of contact persons, name of legal entity, physical and postal address, contact details, Registration number, founding documents, tax related information, banking details, authorised signatories, beneficial owners |

### C. Actual or Planned Transborder Flows of Personal Information

There is presently no actual or planned transborder flow of information.

### D. General Description of Information Security Measures

JKM uses up to date technology of ensure the confidentiality, integrity and availability of personal information under its control. Measures include:

- Firewalls
- Virus protection software and update protocols
- Logical and physical access control
- Secure setup of hardware and software making up the IT structure

# ANNEXURE 2

## Form to Object to the Processing of Personal Information in terms of POPIA:

## Objection to the Processing of Personal Information

## In terms of section 11(3) of POPIA and Regulation 2(1)

Please note:

a. Affidavits or other documentary evidence in support of the objection needs to be attached to this form.
b. If more space is required add additional pages as appendices to this form.

| **Details of Data Subject** | |
|---|---|
| Name and surname | |
| Address | |
| | |
| | |
| | |
| Phone number | |
| Cell number | |
| E-mail address | |
| **Details of Responsible Party** | |
| Name and surname of responsible person, public or private body | |
| Address | |
| | |
| | |
| | |
| Phone number | |
| Cell number | |
| E-mail address | |

| Reasons for objection (please provide full details) |
| --- |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |
| |

Signed at _____ this _____ day of _____ 20__.

**Signature of Applicant (Data Subject)** _____

# ANNEXURE 3

## Request for Amendment, Correction or Erasure of Personal Data

Section 24 of POPIA and Regulation 3, provides that a Data Subject may request for their personal information to be corrected or deleted as held by JKM.

As a main rule, your request will be handled free of charge. However, if we were to find your request to be manifestly unfounded, excessive, or repetitive, we may charge a reasonable fee based on the administrative cost of providing the information but not exceeding R500.00.

Please fill out the details below and we will get back to you within 30 calendar days of the date that the fully completed form, proof of identity and other supporting documents (if required), has been received by us. The documents must be sent to the following address: Information Officer, JKM, 93 Boeing Road East, Bedfordview 2007. Jane@jhbkonicaminolta.co.za

| Details of the person requesting the amendment, correction or erasure | |
|---|---|
| Full name | |
| Address | |
| Date of birth / ID Number | |
| Email address | |
| Phone Number | |

| Your role (tick the correct role) | |
|---|---|
| | I am the Data Subject |
| | I am not the Data Subject, though I am acting on behalf of the Data Subject by virtue of a power of attorney |
| | I am not the Data Subject, though I am acting on behalf of the Data Subject as his/her parent or legal guardian |

| Proof of identity and authority submitted (tick the applicable) | |
|---|---|
| | Driving License |
| | Passport |
| | Identity document |
| | Power of attorney |
| | Evidence of parental responsibility/ guardianship |

| Amendment | |
|---|---|
| | I wish to amend my personal data (proof of identify must be provided) |
| | I wish to amend personal data concerning a Data Subject that I am acting on behalf of (proof of identity of representative, a power of attorney and proof of identity of the Data Subject must be provided) |
| | I wish to amend personal data concerning a Data Subject to whom I am parent or legal guardian (proof of identity and evidence of parental responsibility or legal guardianship must be provided) |
| Type of personal data you wish to amend | |
| Describe the amendment | |

| Correction | |
|---|---|
| | I wish to correct my personal data (proof of identify must be provided) |
| | I wish to correct personal data concerning a Data Subject that I am acting on behalf of (proof of identity of representative, a power of attorney and proof of identity of the Data Subject must be provided) |
| | I wish to correct personal data concerning a Data Subject to whom I am parent or legal guardian (proof of identity and evidence of parental responsibility or legal guardianship must be provided) |
| Type of personal data you wish to correct | |
| Describe the correction | |

| Erasure | |
|---|---|
| | I wish to erase my personal data (proof of identify must be provided) |
| | I wish to erase personal data concerning a Data Subject that I am acting on behalf of (proof of identity of representative, a power of attorney and proof of identity of the Data Subject must be provided) |
| | I wish to erase personal data concerning a Data Subject to whom I am parent or legal guardian (proof of identity and evidence of parental responsibility or legal guardianship must be provided) |
| Type of personal data you wish to erase | |

By signing this form, you certify that the information you have provided is correct to the best of your knowledge ad that you are the person to whom it relates or that you are legally entitled to act on behalf of such person.

You understand that it may be necessary to obtain further information to comply with this request.

Signature: _____

Date: _____

# ANNEXURE 4

## Request for Access to the Record of Private Body

## (Section 53(1) of the Promotion of Access to Information Act 2 of 2000

## And Regulation 10)

**A. Particulars of Private Body**

The Head:

**B. Particulars of the Person Requesting access to the record**

| |
|---|
| a) The particulars of the person who requests access to the records must be given below.<br>b)The address and/ or contact numbers in South Africa to which information is to be sent must be given.<br>c) Proof of the capacity in which the request is made, if applicable, must be attached. |

Full names and surname: _____

Identity number: _____

Postal address: _____

_____

Telephone / cell number: _____

Fax number: _____

Email address: _____

Capacity in which the request is made, when made on behalf of another person:

**C. Particulars of the Person on whose behalf the request is made**

| |
|---|
| This section must be completed ONLY if the request for information is made on behalf of another person. |

Full names and surname: _____

Identity number: _____

**D. Particular of Record**

| |
|---|
| a) 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.<br>b) If the provided space is inadequate, please continue on a separate page and attach to this form. The requester must sign all the additional pages. |

Description of record or relevant part of the record: _____

_____

_____

_____

_____

Reference number, if available: _____

Any further particulars of record: _____

_____

_____

_____

_____

## E. Fees

a) A request for access to a record, other than a record containing personal information about yourself, will be processed only after a request fee has been paid.
b) You will be notified of the amount required to be paid as the request fee.
c) The fee payable for the access to the record depends on the form in which access is required ad the reasonable time required to search for and prepare a record.
d) If you qualify for the exemption of the payment of any fee, please state the reason for exemption.

Reason for exemption from payment of fees: _____

_____

_____

_____

_____

## F. Form of Access to Record

If you are prevented by a disability to read or listen to the record in the form of access provided for in 1 to 4 hereunder, 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 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, videos, computer-generated images, sketches etc)* | | | | | |
| | View the images | | Copy of the images * | | Transcript of the images* |
| **3. If record consists of recorded words or information which can be reproduced in sound** | | | | | |
| | Listen to the soundtrack | | | 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 the computer readable form (CD, DVD, or digital audio format) |
| *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. | | | | | |

## G. 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 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:

_____

_____

_____

_____

## 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 that 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 _____ of 20___

_____

Signature of Requester/ Person on whose behalf request is made

# ANNEXURE 5

## Applicable Fees in respect of Private Bodies in relation to PAIA

**Fees on respect of Private Bodies**

1. The fee for a copy of the manual as contemplated in regulation 9(2)(c ) is for every copy of an A4 size page or part thereof.
2. The fees for reproduction referred to in regulation 11(1) are as follows:

| | | |
|---|---|---|
| a) | For every photocopy of an A4 size page or part thereof | R1.50 |
| b) | For every printed copy of an A4 size page or part thereof held on a computer or in an electronic or machine-readable form | R1.50 |
| c) | For a copy in a computer-readable form on: | |
| i) | Flash drive (to be provided by requester) | R40.00 |
| ii) | DVD (provided by requester) | R60.00 |
| iii) | Digital audio format (provided by requester) | R40.00 |
| iv) | For a transcription of visual images, for an A4 size page or part thereof | Per external service provider |
| v) | For a copy of visual images | Per external service provider |
| vi) | For a transcript of an audio record, for an A4 size page of part thereof | R25.00 |
| vii) | For a copy of an audio record –<br>Flash drive (provided by requester)<br>Compact disc (provided by requester)<br>Compact disc (provided to requester) | <br>R40.00<br>R40.00<br>R60.00 |

3. The request fee payable by a requester, other than a personal requester, referred to in regulation 11 (2) is R100,00.
4. 4. The access fees payable by a requester referred to in regulation 11 (3) are as follows:

| | | |
|---|---|---|
| a) | For every photocopy of an A4 size page or part thereof | R1.50 |
| b) | For every printed copy of an A4 size page or part thereof held on a computer or in an electronic or machine-readable form | R1.50 |
| c) | For a copy in a computer-readable form on: | |
| i) | Compact disc (provided by requester)<br>Compact disc (provided to requester) | R40.00<br>R60.00 |
| ii) | DVD (provided by requester)<br>DVD (provided to requester) | R40.00<br>R60.00 |
| iii) | Digital audio format (provided by requester)<br>Digital audio format (provided to requester) | R40.00<br>R60.00 |
| iv) | For a transcription of visual images, for an A4 size page or part thereof | Per external service provider |
| v) | For a copy of visual images | Per exfternal service provider |
| vi) | For a transcript of an audio record, for an A4 size page of part thereof | R25.00 |
| viii) | For a copy of an audio record (see above) | R40.00 to R60.00 |

| | | |
|---|---|---|
| j) | To search for and prepare the record for disclosure, R30.00 for each hour or part thereof reasonably required for such search and preparation. | R30.00 per hour or part thereof |

| | |
|---|---|
| A. For the purposes of section 54(2) of PAIA, the following applies: | |
| 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. | |
| B. The actual postage is payable when a copy of a record must be posted to a requester. | |

## LEGAL DISCLAIMER

The information contained in this website is intended but not guaranteed to be complete, correct and up to date. This information is made available, without any representation or warranty, either express or implied. Johannesburg Konica Minolta accepts no responsibility for the suitability or accuracy of the information and any errors or omissions that may occur.

The information and content on this website are subject to change without notice.

Johannesburg Konica Minolta may, in its sole discretion, at any time, suspend or terminate the operation of this website or any products or services provided on this website, without prior notice.

Cover afforded in terms of information contained in this website is subject to the terms and conditions found in the policy of insurance.

Copyright in respect of all works found on the website and which have been created and developed by Johannesburg Konica Minolta or on instruction for Johannesburg Konica Minolta, shall vest in it.

Any trademarks registered by Johannesburg Konica Minolta belong to it. These trademarks may not be copied, transmitted or used by anyone else unless expressly permitted by Johannesburg Konica Minolta.

Any reference to or use of a product, service or process of a third party does not imply recommendation, approval or affiliation to the product, service or process by Johannesburg Konica Minolta.

Johannesburg Konica Minolta, its directors, officers and employees, shall accept no liability whatsoever for any loss, whether direct, indirect or consequential arising from information made available on these pages and for any actions or transactions resulting there from use of the website and any actions arising there from shall be governed in all respects by the law of the Republic of South Africa. By using this website, the user consents to the jurisdiction of the courts of South Africa in respect of all disputes.

Without limiting the generality of the aforesaid, the information provided on this website is intended to provide you, the user, with objective information about Johannesburg Konica Minolta's products and services and is not intended to constitute a recommendation, guidance or proposal in regard to the suitability of any product in respect of any need your pet may have.

While every effort has been made to ensure the accuracy of information contained on this website, Johannesburg Konica Minolta and its directors, officers and employees provide no representation or warranty, express or implied, regarding the accuracy, completeness or correctness of information contained in this website.

If you would like any more information about our website and the contents of this policy please contact Jane Callebaut on jane@jhbkonicaminolta.co.za

**JOHANNESBURG BUSINESS SYSTEMS**

KONICA MINOLTA

| | |
|---|---|
| **Policy Name** | **PRIVACY AND SECURITY POLICY** |
| **Version number** | **1/22** |
| **Policy sponsor** | **Margie De Villiers Burchell** |

Approval process

| **MANAGER/ COMMITTEE** | **NAME** | **SIGNATURE** | **DATE** |
|---|---|---|---|
| **INFORMATION OFFICER** | MARGIE DE VILLIERS BURCHELL | | 23.8.22 |
| **DEPUTY INFORMATION OFFICER** | JANE CALLEBAUT | | 23-08.22 |

# 1. Purpose

Privacy and confidentiality is important to Johannesburg Konica Minolta and personal information is dealt with in terms of their Privacy and Security Policy. This privacy and security policy outlines Johannesburg Konica Minolta practices and commitment to all its stakeholders in this regard. Johannesburg Konica Minolta takes all reasonable steps to ensure that it aligns its business practices with the terms of this policy.

Johannesburg Konica Minolta collects, holds, uses and discloses ('processes') information about individuals which may constitute personal data (including sensitive personal data) under the Protection of Private Information Act ("POPIA"). By providing Johannesburg Konica Minolta with personal data (including sensitive data), it is accepted that personal data be processed by Johannesburg Konica Minolta for the purposes described in this policy.

This policy aims to ensure that personal data is processed in a responsible and secure manner to ensure privacy and confidentiality thereof.

# 2. Organisational Scope

The policy fits within the Compliance Management Framework. All stakeholders of Johannesburg Konica Minolta are affected by the Privacy and Security Policy.

# 3. Policy Statement, Principles and Guidelines

## 3.1 Use of Information

Johannesburg Konica Minolta values its stakeholders, and as such, is committed to respecting and maintaining personal information confidential and to keep such information secure. Johannesburg Konica Minolta will use all personal information to enhance its clients' experiences, the service that it provides and to communicate with its clients, unless expressly directed by its clients not to do so. Johannesburg Konica Minolta will therefore treat all personal information as private and confidential and undertake to deal with all Information in a responsible and lawful manner.

Johannesburg Konica Minolta will take all reasonable steps to prevent unauthorised access to personal information in its possession and to which it has access to. Kindly note that will Johannesburg Konica Minolta only requests personal information required for the purposes of assessing and providing its clients with the products and services required . This information is essential to conclude agreements and comply with its legal and regulatory obligations.

Johannesburg Konica Minolta will further only process personal information for purposes consistent with the normal course of its business to uphold its legitimate interests.

Johannesburg Konica Minolta is required by law, to process and maintain all personal information in accordance with prescribed standards or generally accepted information management practices (including prescribed retention periods) to ensure that your information is complete, accurate, up to date and secure.

3.2 Personal information

In general, anyone may visit Johannesburg Konica Minolta's website without revealing any personal information. There are times, however, when Johannesburg Konica Minolta or its partners may request personal information. If requested, you may choose to give us your personal information, for example your name and address or email addresses. This information may be needed, for example, to correspond with you, to process a request, or to provide you with a quote or with information.

Johannesburg Konica Minolta will advise you how it will use personal information before it collects the personal information from you. If you inform Johannesburg Konica Minolta that you do not want it to use your personal information as a basis for further contact with you or for any other purpose, it will abide by your request.

3.3 Technology, security, and quality of information on the Website

Johannesburg Konica Minolta intends to protect the quality and integrity of personal information. To prevent unauthorised access, maintain data integrity and ensure the appropriate use of information, Johannesburg Konica Minolta has established appropriate physical and technological protocols to safeguard the personal information provided to it. We will update and enhance these measures on an ongoing basis, to ensure they remain appropriate and relevant.

However, Johannesburg Konica Minolta cannot guarantee the security of any information transmitted to it online and parties do so at their own risk.

We will make commercially reasonable efforts to respond to requests to correct inaccuracies in your personal information in a timely manner. To assist us in correcting inaccuracies in personal information, stakeholders are requested to kindly return messages containing the inaccuracies to Johannesburg Konica Minolta with details of the correction requested.

Johannesburg Konica Minolta has deployed appropriate technology and implemented security measures to protect against the loss, misuse or alterations of the information under its control, by unauthorised third parties. We are committed to providing and developing secure online services.

As such, all interactions with Johannesburg Konica Minolta transactional site, are protected through encryption that complies with international standards. We have implemented data encryption to protect your data and secure your transactions. Encryption is used to protect the transmission of your personal information when transacting with us.

Our internet servers are protected by firewalls and intrusion detection systems. Access to information on these servers is restricted to authorised personnel only. The Johannesburg Konica Minolta user database is backed up on a regular basis, and its services do not allow anonymous or otherwise unauthenticated access at any time.

We regularly test the effectiveness of the security of its systems and respond to any threats that may be detected.

Of course, no data transmission over the internet can be guaranteed 100% secure, and Johannesburg Konica Minolta does not warrant that your information will be secure.

3.4 Information collection

To monitor and improve the website, Johannesburg Konica Minolta may use technology to gather information about your use of the website including details of operating system, browser version, domain name, and IP address (the IP address is a string of numbers that tells us which server you are using but does not identify you).

The process of gathering the information as described immediately above uses a technology known as "cookies". Cookies are small pieces of data that allow our web server to recognise users on our website. Cookies are issued by a specific web server, stored in the user's web browser and can only be read by the issuing server.

Apart from merely establishing basic connectivity and communications, Johannesburg Konica Minolta may use this data in aggregate form to develop customized services that may be tailored to individual interests and needs. We will use cookies to save email and username so website users, don't have to re-enter it each time they visit the site. Johannesburg Konica Minolta may also use cookies to customise website users' preference settings for future return visits. This is also to facilitate speedy service to clients and enhances experience on the website. At no point in time will any of the personal information be stored in a cookie.

Should a website user choose to do so, it is possible (depending on the browser being used), to be prompted before accepting any cookies, or to prevent the browser from accepting any cookies at all. This may however cause certain

features of the website not to be accessible. If a user does not wish us to collect the information the browser should allow the disablement of cookies.

3.5 Sharing of information

Johannesburg Konica Minolta will not sell, rent, or trade any personal information to any third party. We will disclose information when lawfully required to do so to comply with any relevant legislation, or any legal process; and by any regulatory authority, and the Regulators it may appoint for the various sectors.

Sometimes Johannesburg Konica Minolta may share aggregated information (for example, demographic data) with its stakeholders and business partners, but it will not disclose personal information to third parties save with personal consent or as provided in this privacy statement. We will never sell email addresses to third parties for purposes of email spamming. If a stakeholder has agreed to this, Johannesburg Konica Minolta may use personal information to send information on new services or products that may be of interest to the stakeholder, and from time to time will mail, email or SMS information about Johannesburg Konica Minolta, its products and services, or to its partners and their products or services. If at any time you do not wish to continue receiving this information, you may contact our Information Officer and we will remove you from the mailing list.

Johannesburg Konica Minolta may be required to disclose person information for matters of public interest (e.g. to assist in the prevention of crimes). Before complying with these requests, it will take every precaution to ensure the authorities involved have legitimate grounds to make such a request.

We may process and disclose personal information, for statistical purposes, that does not relate to any person specifically (i.e. de-identified information) as it deems appropriate.

3.6 Clickstream data

Johannesburg Konica Minolta may collect anonymous information from visitors to its websites to help it provide better customer service. For example, it keeps track of the domains from which people visit its website and measures visitor activity on its website. In doing so we ensure the information cannot be used to identify users. This information is sometimes known as "clickstream data". Johannesburg Konica Minolta or its analytics vendors may use this data to analyse trends and statistics and to help it provide better customer service. If you do not wish your personal information to be used in this way, users are kindly requested to notify our Information Officer.

3.7 Personalised URL link

On occasion, a personalised URL (link) is displayed on the Johannesburg Konica Minolta website that directs a visitor to a personalised web page. The personal URL is readily identifiable and may result in the disclosure of personal information. By clicking on that link and accessing a personal web page the user agrees to allow us to collect information about the session visits. We may use this information to help it provide the user with information that matches the user's interests. If you do not wish your personal information to be used in this way, kindly notify our Information Officer.

3.8 Children

If any, of Johannesburg Konica Minolta's websites are directed towards children, we are committed to comply with all applicable laws aimed at the protection of children and in particular the protection of their personal information.

3.9 Interception of Communications

Subject to the provisions of the Regulation of Interception of Communications (RIC) Act 70 of 2002, the user of the website hereby agrees to Johannesburg Konica Minolta's right to intercept, block, filter, read, delete, disclose, and use all communications sent or posted by the user to the website, its staff and employees. You agree and acknowledge that the consent provided by you, herein, satisfies the "writing" requirement as detailed in the ECT Act and the RIC Act.

3.10 Updates

This privacy statement was last updated in August 2022. Johannesburg Konica Minolta reserves the right to amend or modify its Privacy and Security Policy at its sole discretion, at any time, without any prior notice to the user, in response to meeting legislative requirements and dynamic business needs. All amendments to the policy will be posted on the website.

## 4. Legislative Compliance

Johannesburg Konica Minolta is required to manage its policy documentation within a legislative framework. The following legislation is relevant to this policy:

- Constitution of the Republic of South Africa Act 108 of 1996
- Electronic Communications and Transactions Act no 25 of 2002
- Promotion of Access to Information Act 2 of 2000
- Protection of Personal Information Act 4 of 2013

## 5. References

POPIA and PAIA Compliance Risk Management Framework

**JOHANNESBURG BUSINESS SYSTEMS**

KONICA MINOLTA

| | |
|---|---|
| **Policy Name** | **EMAIL DISCLAIMER POLICY** |
| **Version number** | 1/22 |
| **Policy sponsor** | **Margie De Villiers Burchell** |

Approval process

| **MANAGER/ COMMITTEE** | **NAME** | **SIGNATURE** | **DATE** |
|---|---|---|---|
| **INFORMATION OFFICER** | MARGIE DE VILLIERS BURCHELL | | 23 8 22 |
| **DEPUTY INFORMATION OFFICER** | JANE CALLEBAUT | | 22-08-22 |

## EMAIL LEGAL NOTICE

### 1. Confidentiality

This email is confidential and may contain privileged or copyright information. You may not present this message to another party without consent from the sender. If you are not the intended recipient please notify the sender and delete this email, and you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

### 2. Liability

This email is not a binding agreement and does not conclude an agreement without the express confirmation by the sender's authorised manager or a designated representative of Johannesburg Konica Minolta.

### 3. Viruses

Johannesburg Konica Minolta has deployed appropriate technology and implemented required firewalls and intrusion detection systems to protect against any viruses or defects. It is committed to providing and developing secure incorrupt services. However, it does not certify that this email is free of viruses or defects.

In the event, that this email is corrupted, Johannesburg Konica Minolta does not warrant against the damage and loss incurred as a result of the virus or defect, and will not be held liable for any damage and loss caused as a result thereof.

### 4. Requested

Johannesburg Konica Minolta does not consent to its employees sending unsolicited emails which contravene the law. In the event that you feel this email is such, please notify Johannesburg Konica Minolta in order for the appropriate corrective action to be taken.

### 5. Advice

Any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company. Any actions taken on the basis of this email are at the reader's own risk.

### 6. Other

The sender of this email is expressly required not to make any defamatory statements. Any such communication is contrary to company policy and outside the scope of the employment of the individual concerned. Johannesburg Konica Minolta will not accept

any liability in respect of such communication, and the employee responsible will be personally liable for any damages or other liability arising.

Please note that Johannesburg Konica Minolta reserves the right to access, block, monitor and intercept e-mail addressed to Users in it in accordance with Johannesburg Konica Minolta 's e-mail policy.