Enjoy Optimal Trading with us.

OPTIM INVESTMENTS

OPTIM Investments

Data Protection Manual

Updated: 12 October 2020

CONTENTS

1. Introduction 3
2. Definitions and Interpretation 4
3. Principles of Processing of Personal Data 6
4. Scope of the Policy 6
5. Lawfulness, Fairness and Transparency 7
6. Consent 9
7. Rights of Data Subjects 10
8. Rights of Information and Access 11
9. Personal Data Breaches 13
10. Transfer of Data Outside Mauritius 13
11. Data Storage 13
12. Data Pseudonymisation 14
13. Data Accuracy and Clean Desk Policy 15
14. Data Privacy Office 16
APPENDIX 1 – WITHDRAWAL OF CONSENT PROCESS 17
APPENDIX 2 - PROCEDURES IN CASE OF PERSONAL DATA BREACHES 17
APPENDIX 3 - PROCEDURE IN CASE OF OBJECTION FROM DATA SUBJECT 17
APPENDIX 5 – DATA RIGHTS FORM 17

Forward: This Policy sets out the control standards and procedures that are implemented in OPTIM Investments Limited ("OPTIM Investments", "Company" or the "Firm"), in relation to the Company's compliance with applicable rules and regulations in data protection, including the collection, processing, storing and transferring of personal data. The overall aim is to ensure adherence to the guidelines, policies and procedures for data protection, making the culture of data protection by design and default an embedded element of the Company's modus operandi.

1. INTRODUCTION

The primary function of this Data Protection Policy (the "Policy") is to provide a control environment within the Firm in terms of the Data Protection Act 2017 of Mauritius ("DPA" or the "Act"). In addition, this Policy has been developed for the promotion of good practice within the Firm in relation to the collection, use, processing, handling and storage, amongst others, of personal client data by the employees. Staff members are expected under the Act to understand their role and accountabilities in relation to the enforcement and promotion of good data protection principles in their day-to-day activities.

It is the policy of the Firm that all personnel must comply with the policies and process standards as set out in this Policy, unless specific exceptions to the Policy set out herein have been explicitly agreed. Employees must familiarize themselves with these procedures and policies and the specific requirements of applicable laws and rules to their particular areas. Employees should also be aware of, and are expected to follow the established internal control procedures which are documented in this Policy.

Employees must review the policies and procedures set forth in this Policy at regular intervals and are required to comply with its requirements.

This Policy is not intended to be a fully comprehensive document addressing all legal, operational and practical aspects, related to the Act. Certain issues and/or aspects of the Act have not been dealt in fully as they still require further definition and/or clarification. These and other issues that will arise afterwards will be addressed and developed in this Policy as and when required over time.

Company employees who are of doubt in relation to the Data Protection principles applicable within the Firm should escalate their queries to the Compliance Department.

Personal data, which is the information relating to an identified or identifiable individual, is collected and used almost every day and everywhere. Personal data can be an individual's name, address, email or mobile number or location data, amongst others. As the value of personal data grows, the risks to personal data inevitably increase. In addition, with rapid technological change and innovation, controlling personal data is becoming more and more difficult especially with data intensive online activities. The new Act has been enacted to sustain and strengthen the control and personal autonomy of data subjects over their personal data. It has been designed to align with the key principles found in international laws namely the EU General Data Protection Regulation (GDPR) (EU) 2016/679.

A robust Data Protection Policy is of the utmost importance for the good conduct of the Firm's business and it is compulsory that each and every employee reads it carefully.

This Policy ensures that the Firm:

- complies with the DPA and follows good practice;
- protects the rights of staff, customers, business partners and third parties;
- Stores and processes personal data in line with local and foreign laws; and
- Protects itself from the risks of a data or security breaches, amongst others

It is of critical importance that the policies and standards specified in this document be strictly adhered to by all staff members of the Firm. Failure to comply with same may lead to the Firm being exposed to a series of legal and regulatory risks.

Any failure to adhere to the requirements of this Policy will be regarded and treated as a disciplinary matter, and may lead to summary dismissal.

2. DEFINITIONS AND INTERPRETATION

In this Policy the following terms shall have the following meanings:

2.1 "Consent"

Means any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which they signify their agreement to personal data relating to them being processed;

2.2 "Controller"

Means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing;

2.3 "Data subject"

Means an identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;

2.4 "Physical or mental health",

In relation to personal data, includes information on the provision of health care services to the individual, which reveals his health status;

2.5 "Personal data"

Means any information relating to a data subject;

2.6 "Processing"

Means an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

2.7 "Processor"

Means a person who, or public body which, processes personal data on behalf of a controller;

2.8 "Profiling"

Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

2.9 "Pseudonymisation"

Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;

2.10 "Special categories of personal data"

In relation to a data subject, means personal data pertaining to**:**

a. Their racial or ethnic origin;

b. Their political opinion or adherence;

c. Their religious or philosophical beliefs;

d. Their membership of a trade union;

e. Their physical or mental health or condition;

f. Their sexual orientation, practices or preferences;

g. Their genetic data or biometric data uniquely identifying them;

h. The commission or alleged commission of an offence by them;

i. Any proceedings for an offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any Court in the proceedings; or

j. Such other personal data as the Data Protection Commissioner of Mauritius may determine to be sensitive personal data

2.11 "Third party"

Means a person or public body other than a data subject, a controller, a processor or a person who, under the direct authority of a controller or processor, who or which is authorised to process personal data.

3. PRINCIPLES OF PROCESSING OF PERSONAL DATA

The object of the DPA is to provide for the protection of the privacy rights of individuals in view of the developments in the techniques used to capture, transmit, and manipulate, record or store data relating to individuals.

To this end, the DPA is underpinned by 6 imperative principles (section 21 of the Data Protection Act 2017).

Specifically, section 21 of the Act requires that personal data be:

1. Processed lawfully, fairly and in a transparent manner in relation to any data subject;
2. collected for explicit, specified and legitimate purposes and not further processed in a Manner incompatible with those purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and,
6. Processed in accordance with the rights of data subjects.

These principles apply regardless of whether data is stored electronically, on paper or on other materials

4. SCOPE OF THE POLICY

This Policy document applies to all forms of data that the Firm may hold in relation to identifiable individuals, even if that information technically may likely fall outside the scope of the DPA. These forms include and are not restricted to the following categories of personal data in relation to a data subject:

a. names;
b. Residential addresses;
c. Email addresses;
d. Telephone numbers;
e. Racial or ethnic origin;
f. Political opinion or adherence;
g. Religious or philosophical beliefs;
h. Membership of a trade union
i. Physical or mental health or condition;
j. Sexual orientation, practices or preferences;
k. Genetic data or biometric data uniquely identifying him;
l. Commission or alleged commission of an offence by him;
m. Any proceedings for an offence committed or alleged to have been committed by a data subject, the disposal of such proceedings or the sentence of any Court in the proceedings; or
n. Such other personal data as the Commissioner may determine to be sensitive personal data;
o. Any other information of a personal nature permitting the identification of an individual.

5. LAWFULNESS , FAIRNESS AND TRANSPARENCY

As a matter of policy, the Firm regards the lawful and correct treatment of personal information as indispensable in maintaining the confidence of the data subjects with whom we deal with. Staff members shall ensure at all times that personal data are collected only for the requirements of our business and only if the collection of the data is necessary for that purpose.

5.1 DATA LIMITATION

Every staff member of the Firm has the responsibility for ensuring that data are collected, stored and handled appropriately and as per the set procedures stated herein.

Personal data must at all times be collected for explicit, specified and legitimate purposes and not further processed in a way incompatible with those purposes. As such, each staff member, business unit and/or department that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles mentioned therein.

5.2 DATA MINIMISATION AND STAFF DUTIES

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Staff members must:

1. Ensure that, in the course of their work duties, fair collection and use of personal information;

2. Specify the purposes for which information is being collected and used by the Company;

3. Collect and process appropriate information, and only to the extent that it is needed to fulfil their business and operational needs or to comply with any legal requirements;

4. Ensure that the rights of data subjects about whom information is held, can be fully exercised under the Act. Such rights include:

    i. The right to be informed that processing is being undertaken;

    ii. The right of access to one's personal information;

    iii. The right to prevent processing in certain circumstances; and,

    iv. The rights to correct, rectify, block or erase information which is regarded as wrong information.

5. Take appropriate technical and organisational security measures to safeguard the Company's clients' personal information; and

6. Ensure that personal information is not transferred abroad without suitable safeguards.

The Firm's Board of Directors is ultimately responsible for ensuring that the Company meets its legal obligations.

The Legal Department shall, as and when required, be responsible for:

1. Keeping the Board updated about data protection responsibilities, risks and issues;

2. Reviewing all data protection procedures and related policies, in line with an agreed schedule;

3. Arranging data protection training and advice for the people covered by this Policy;

4. Handling data protection questions from staff and anyone else covered by this Policy;

5. Dealing with requests from individuals to see the data the Firm holds about them (also called "subject access requests"); and

6. Checking and approving any contracts or agreements with third parties that may handle the Firm's sensitive data.

5.3 GENERAL STAFF GUIDELINES

The only people able to access data covered by this Policy should be those who need it for their work.

Personal data must not be shared informally. When access to confidential information is required, employees shall request it from their line managers. Employees should keep all data secure, by taking sensible precautions and following the standards of this Policy. In particular, strong passwords must be used and they should never be shared.

Personal data should not be disclosed to unauthorised people, either within the Firm or externally.

Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, personal data should be deleted and disposed of.

Employees should request help from their line manager or the Legal Department if they are unsure about any aspect of data protection.

When working with personal data, employees should ensure the screens of their personal computers and laptops are always locked when left unattended. Employees, laptops users in particulars, should not save copies of personal data to personal pen drives and other removable media without proper encryption.

6. CONSENT

Consent is any freely given, specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which the data subject signifies their agreement to personal data relating to them being processed.

6.1 WHY IS CONSENT IMPORTANT?

Consent is one of the lawful bases for the processing of personal data. Given our willingness to continuously remain a DPA-compliant financial institution, the Firm will make every effort to give its clients ongoing control over how we use data subjects' data, thus ensuring that our organisation is thoroughly transparent and accountable.

Handling consent therefore builds customer trust and engagement and enhances the reputation of our operations. Relying on inappropriate or invalid consent could destroy trust, harm our reputation and might leave our Firm exposed to substantial fines.

Thus, when dealing with clients, staff members shall constantly have in mind the key elements of consent: it must be ***freely given***, ***specific, informed*** and there ***must be an indication signifying agreement***.

At the time of collection, data subjects should be readily informed about the right to withdraw their consent at any time. Consent shall therefore be:

1. **Specific, and unambiguous**; by setting out the purpose of the various phases of the processing;

2. **Informed**; data subjects should be informed about the right to withdraw their consent at any time;

3. **Clear**; easy to withdraw without affecting the lawfulness of processing; as well as,

4. **Verifiable**; appropriate records shall be kept to demonstrate what the individual has consented to, including what they were told, when and how they consented

6.2 Collection of consent

Consent shall be collected at the outset of establishing a client relationship.

6.3 When consent is not required?

There are certain specific cases provided for in section 28 of the Act where consent is not required.

Staff shall process clients' personal data only if:

a. The data subject consents to the processing for one or more specified purposes; or

b. The processing is necessary:

   1. For the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

   2. For compliance with any legal obligation to which the controller is subject;
   3. In order to protect the vital interests of the data subject or another person;
   4. for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
   5. The performance of any task carried out by a public authority;
   6. The exercise, by any person in the public interest, of any other functions of a public nature;
   7. For the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
   8. For the purpose of historical, statistical or scientific research.

6.4 PERSONAL DATA OF CHILDREN

Pursuant to section 30 of the Act, staff members shall not process the personal data of a child below the age of 16 years unless consent is given by the child's parent or guardian. As such, staff members should obtain consent from whoever holds parental responsibility for them.

As a rule, Know Your Customer and Customer Due Diligence ("KYC/CDD") measures shall be conducted on the child's parent or guardian to verify that the person giving the own consent in these circumstances is lawfully authorised to do so and doing so in the interests and benefits of the child.

7. RIGHTS OF DATA SUBJECTS

Section 37 of the Act provides that "*every controller shall, on the written request of a data subject provide, at reasonable intervals, without excessive delay and, subject to subsection (7), free of charge, confirmation as to whether or not personal data relating to the data subject are being processed and forward to him a copy of the data.*"

The above rights include the rights to access, rectify, erase and restrict the processing of personal data. The principle of "fair and transparent" processing means a client must be provided all relevant information in relation to the processing of his/her data, unless s/he already has this information**.**

Where the staff member obtains personal data directly from the data subject, the latter should be informed of the following rights under the law:

1. The purpose/s for which the data are being collected;
2. The intended recipients of the data;
3. Whether or not the supply of the data by that data subject is voluntary or mandatory;
4. The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
5. The existence of the right to request from the controller access to and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing;
6. The existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
7. The period for which the personal data shall be stored;
8. The right to lodge a complaint with the Data Protection Commissioner of Mauritius;
9. Where applicable, that the controller intends to transfer personal data to another country and on the level of suitable protection afforded by that country; and
10. Any further information necessary to guarantee fair processing in respect of the data subject's personal data, having regard to the specific circumstances in which the data are collected.

However, where the controller does not obtain personal data directly from the client, the latter shall, as soon as reasonably practicable, be informed of his/her rights.

8. RIGHTS OF INFORMATION AND ACCESS

Pursuant to the Act, an individual has the right to:

1. Obtain confirmation whether his/her personal data are being processed;
2. Access the data (i.e. to a copy); and
3. Be provided with supplemental information about the processing.

Access rights are intended to allow individuals to check the lawfulness of processing and the right to have a copy of their personal data. However, these rights should not adversely affect the rights of others.

How should such requests be handled?

A written request must be made to the privacy officer of the Firm by the data subject. A copy of the requested information will be provided without excessive delay and free of charge. Such confirmation shall include whether or not personal data relating to the data subject are being processed.

Depending on the request of the client, or in case the request is manifestly excessive, the Firm may charge a reasonable fee for providing the required information or taking the actions requested by the client.

8.1 Right of rectification

An individual has the right to:

1. Rectify inaccuracies in personal data held about them.
2. Complete incomplete data; and,
3. Record a supplementary statement.

8.2 Rights of erasure

Pursuant to with section 41 of the Act, the Firm has the right to erase personal data in the following circumstances:

1. The data are no longer necessary in relation to the purpose for which they were collected or otherwise processed.
2. The data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing.
3. The data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing.
4. The personal data have been unlawfully processed.

In such instances, the Firm will also forthwith inform its authorised third parties processing the personal data that the data subjects have requested the erasure of any links to, or copy or replication of, their personal data.

However, such requests shall not be complied with where the processing of personal data is necessary for:

1. Reasons of public interest in the field of public health
2. The purpose of historical, statistical or scientific research
3. Compliance with a legal obligation to process the personal data to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
4. The establishment, exercise or defence of a legal claim.

8.3 Right to object

Data subjects have the right to object in writing at any time to the processing of personal data concerning them.

For example, clients have the right to object to direct marketing which includes profiling.

For the avoidance of doubt, profiling is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict certain aspects concerning that person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

8.4 Exercise of rights

A data subject can, at any time, exercise their rights to access, rectify, erase or object to the processing of their personal data. The Firm will therefore also use reasonable means to verify the identity of the person making the request but should not keep or collect data just so as to be able to meet subject access requests. Data subjects will be required to fill-in and returned a signed copy of the Rights of Data Subject Form provided in Appendix 5.

9. PERSONAL DATA BREACHES

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, client's personal data being either transmitted, stored or otherwise processed.

Under Section 25 and 26 of the Act, the Firm shall, without undue delay, and where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Commissioner.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a client, the Firm shall, after prior communication the Data Protection Commissioner of Mauritius, communicate the personal data breach to the client.

10. TRANSFER OF DATA OUTSIDE MAURITIUS

Personal data can be transferred to another country provided that the Firm has put in place appropriate safeguards with respect to the protection of the personal data and complies with the conditions of transfer established in section 36 of the DPA.

11. DATA STORAGE

Personal data will be stored securely and will only be accessible to authorised staff. Information will be stored in compliance with the provisions of the Act.

When data is stored on paper, it should be classified and kept securely where unauthorised people cannot access or see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reasons:

1. When not required, the paper or files should be kept in a locked drawer or filing cabinet.
2. Employees must make sure that paper and printouts are not left in places where unauthorised people could see them, like on a printer.
3. Data printouts should be disposed of as per the Data Disposal Policy.

When data is stored electronically, it must be protected, through at least one of the following means:

1. Data should be protected by strong passwords that are changed regularly and never shared between employees.
2. If data is stored on removable media (like a CD, DVD or portable storage drives or devices), these should be kept locked away securely when not being used.
3. Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
4. Servers containing personal data should be sited in a secure location, away from general office space.
5. Data should be backed up frequently. Those backups should be tested regularly, in line with the Firm's standard backup procedures.
6. Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

7. All servers and computers containing data should be protected by approved security software and a firewall.

12. DATA PSEUDONYMISATION

Data pseudonymisation, as defined in the Act, means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information and the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable individual.

By correctly pseudonymising or anonymizing its data, the Firm will have the ability to share, disseminate or publish a greater amount of personal data with fewer restrictions. Personal identifiers such as name, address, date of birth, reference number, amongst others, are removed from the data source thus allowing the information to be used for secondary purposes and made available within a controlled environment to other government agencies and/or local authorities for historical scientific research or for statistical purposes.

12.1 Anonymization

Anonymization is the process of removing, obscuring, aggregating and/or altering any identifiers in a dataset which can point to the particular person(s) the data relates to. In addition to the legal requirement to share information with government or local authorities, the Firm has additional regulatory obligations to ensure transparency in its processes and, as such, routinely publishes and distributes information as appropriate. As and when required, the Firm will therefore anonymize personal data in the course of its normal business activities.

12.2 Anonymization process

The anonymization process will be strictly restricted to the IT department of the Firm. Therefore, the concerned staff will:

1. Proceed with the anonymization in such a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate security (technical) or organizational measures; and,

2. Strictly abide to appropriate safeguards with respect to the protection and storage of the anonymized data.

13. DATA ACCURACY AND CLEAN DESK POLICY

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. In addition, it is the responsibility of each employee to take reasonable steps to ensure that personal data are:

1. Held in as few places as necessary. Staff should not create any unnecessary additional data copies or sets.

2. Updated at every available opportunity. For instance, by confirming a customer's details when s/he calls.

3. Updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

14. Data Privacy Office

14.1 Name and contact details of the Data Privacy Office:

Contact Name:	
Title/Department:	**Head of Legal and Compliance**
Email:	**legal@optimfx.com**
Phone:	

14.2 Complaints and queries

If you have any queries or complaints about our compliance with this Policy, or if you would like to make any complaints to us, you may contact the Data Privacy Office either by email at legal@optimfx.com or in writing to:

Mailing Address:	**Data Privacy Office** **OPTIM Investments Limited** **C/o Alexander Management Services Limited** **3rd Floor, Manor House** **30 St Georges St** **Port Louis**

15. APPENDIX 1 – WITHDRAWAL OF CONSENT PROCESS

Procedure for Withdrawal of Consent

Step 1: Client contacts the Firm's customer support department or communicates with Company via any other means (e.g. by post or email)

Step 2: Withdrawal of consent is communicated to the Privacy Office

Step 3: Privacy Office communicates the withdrawal of consent request to the relevant departments of the Firm, such as marketing and sales.

Step 4: Notification is sent to client to acknowledge their request of withdrawal of consent and inform them that either (i) documents shall/have been destroyed accordingly; or (ii) that some or all of the documents will be retained, explaining the legal grounds for that (e.g. regulatory retention obligations, litigation etc).

16. APPENDIX 2 - PROCEDURES IN CASE OF PERSONAL DATA BREACHES

Procedure for Personal Data Breach & Communication to Data subjects

Step 1: Personal data breach occurs.

Step 2: Data Privacy Office informs the Data Protection Commissioner of Mauritius within 72hrs of the breach.

Step 3: Data Privacy Office simultaneously notify the affected data subjects of the breach unless the same falls under the exempted circumstances under the Act.

Step 4: Corrective actions are undertaken.

17. APPENDIX 3 - PROCEDURE IN CASE OF OBJECTION FROM DATA SUBJECT

Step 1: Objection received in writing from data subject.

Step 2: Direct the objection to the Data Privacy Office.

Step 3: Data Privacy Office analyses whether there are any compelling legitimate grounds for the processing which override the Data Subject's interests, rights and freedom.

Step 4: If no, procedures for withdrawal of consent and destruction of personal data are followed.

Step 5: If yes, notify client that we have legitimate grounds for the processing of their data.

18. APPENDIX 4 – DATA RIGHTS FORM

I _____ WITH ACCOUNT NUMBER _____ REQUEST THE REMOVAL OF ALL AND ANY STORED PERSON DATA FROM THE OPTIM INVESTMENTS CLIENT CABINET, TRADING TERMINAL AND SERVER AND ANY PRINT OR STORED RECORDS FROM THE COMPANIES DATABASE.

NAME:_____

SIGNATURE: _____

DATE: _____

OPTIM Investments Limited
30 Saint Georges Street,
3rd Floor, Manor House, Port Louis
www.optimfx.com | info@optimfx.com