KASA GROUP

GENERAL DATA PROTECTION POLICY

ABSTRACT
This policy outlines the Company's processes and procedures to ensure compliance with the Data Protection Act 2017.

Published Date
18/10/2024

VERSION 1.0

TABLE OF CONTENTS

GENERAL DATA PROTECTION POLICY 2
1 Introduction 2
2 Policy statement 6
3. Responsibilities and roles 7
4. Data protection principles 8
4.1 Lawfulness, fairness and transparency 8
4.2 Purpose limitation 9
4.3 Data minimization 10
4.4 Accuracy 10
4.5 Storage limitation 11
4.6 Integrity and confidentiality 12
4.7 Accountability and compliance 14
5. Data subjects' rights 14
6. Consent 15
7. Security of data 16
8. Disclosure of data 17
9. Retention and disposal of data 18
10. Data transfers 18
11. Information asset register/data inventory 20
Document Owner and Authorisation 21

GENERAL DATA PROTECTION POLICY

1 Introduction

1.1 The European Union General Data Protection Regulation 2016 ('GDPR') and the Mauritius Data Protection Act 2017 ('DPA') have been enacted to further protect the rights and freedoms of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

1.2 KGL in this General Privacy Policy, 'KGL' refers to KASA GROUP LTD, and all the words and expressions used in this Privacy Notice shall be interpreted and construed in line with the definitions used in KGL's General Data Protection Policy.

1.3 KGL has its registered office situated at 42, Edith Cavell Street, Port-Louis, Republic of Mauritius and its administrative headquarters situated at the same address. KGL's other contact details are as follows:

Telephone Number: +230 2027500

1.4 Although established, based and domiciled in Mauritius, KGL has expanded its business activities beyond the jurisdiction of Mauritius including but not limited to parts of the European Union.

1.5 For the purpose of the present document, the following words and/or expressions are understood to have the following meaning:

'Personal data'	any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, 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 natural person.
'Sensitive and/or Special categories of personal data'	personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union

	membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
‘Data Controller’	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
‘Data Processor’	the natural or legal person, public authority, agency or other body who process personal data for and on behalf of the Data Controller.
‘Data Subject’	the person whose personal data is processed by the Data Controller.
‘Processing’	any operation or set of operations which is performed on personal data or on 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.
‘Profiling’	any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person’s performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the Data Subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

'Third party'	a natural or legal person, public authority, agency or body other than the Data Subject, the Data Controller, the Data Processor and persons who, under the direct authority of the Data Controller or the Data Processor, are authorised to process personal data.
'Supervisory Authority'	the independent public authority responsible for the enforcement of the GDPR and the DPA and the regulation and supervision of data processing. In Mauritius, a Data Protection Office, headed by the Data Protection Commissioner, has been established under the DPA.

1.6 The GDPR and the DPA apply to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

1.7 The DPA will apply to all Data Controllers and Data Processors that are established in the Republic of Mauritius who process the personal data of Data Subjects.

1.8 The GDPR will apply to all Data Controllers and Data Processors that are established in the European Union who process the personal data of Data Subjects, in the context of that establishment. It will also apply to Data Controllers and Data Processors outside of the European Union that process personal data in order to offer goods and services, or monitor the behavior of Data Subjects who are resident in the European Union.

1.9 In light of the definitions of 'Data Controller' and 'Data Processor' set out in paragraph 1.5 above and in view of the matters set out in paragraph 1.4 above, KGL is a Data Controller and a Data Processor under both the GDPR and the DPA.

2 Policy statement

2.1 The Board of Directors and management of KGL are committed to compliance with all relevant laws in respect of personal data including the GDPR and the DPA for the protection of the rights and freedoms of individuals whose information KGL collects and processes in the course of its activities.

2.2 KGL's compliance with the GDPR and the DPA is described by this General Data Protection Policy as supplemented by the other documents namely:

2.2.1 KGL's Training Policy;

2.2.2 KGL's Employment (Privacy) Notice;

2.2.3 KGL's Recruitment (Privacy) Notice;

2.2.4 KGL's General Privacy Policy;

2.2.5 KGL's Retention of Records Procedure;

2.2.6 KGL's Consent Procedure Notice;

2.2.7 KGL's Information Security Policy; and

2.2.8 Non-Disclosure Agreements.

2.3 The GDPR, the DPA, this General Data Protection Policy and the documents referred to in paragraph 2.2 above shall apply to all of KGL's personal data processing functions, including those performed on customers', potential customers', clients', potential clients', employees', suppliers', distributors', contractors' and other stakeholders' and/or partners' personal data, and any other personal data KGL processes from any source.

2.4 Any breach of the GDPR, the DPA, this General Data Protection Policy and/or any of the documents referred to in paragraph 2.2 above by an employee or préposé of KGL will be dealt with under KGL's disciplinary policy. And should such a breach appear to give rise to a criminal offence, the matter will be reported as soon as possible to the appropriate authorities. Furthermore, KGL will report any breach

to the relevant data protection supervisory authority and also inform the Data Subject whose data has been breached.

2.5 Partners and any third parties working with or for KGL, and who have or may have access to personal data, will be expected to have read, understood and undertaken to comply with this General Data Protection Policy. No third party may access personal data held by KGL without having first entered into a data confidentiality or privacy agreement with KGL, which imposes on the third-party obligations no less onerous than those to which KGL is committed. In that respect, KGL has implemented third-parties' agreements as Supplier Privacy Agreements and Distributor Privacy Agreements.

2.6 In order to foster a data protection and privacy culture amongst its stakeholders, KGL will provide ongoing and appropriate training so as to further protect the rights and freedoms of data subjects. In that respect, KGL has elaborated and implemented a Training Policy.

3. Responsibilities and roles

3.1 KGL is both a Data Controller and a Data Processor under both the GDPR and the DPA.

3.2 Top Management and all those in managerial or supervisory roles throughout KGL are responsible for developing and encouraging good information handling practices within KGL.

3.3 Furthermore, the Board of Directors of KGL has appointed a Data Protection Officer whose identity and contact details are as follows:

- Name: Dilmohamud Aishah
- Postal address: 42, Edith Cavell Street, Port-Louis, Mauritius.
- Email address: adilmohamud@kasa.mu
- Telephone No: 2027500

3.4 KGL's Data Protection Officer is accountable to the Board of Directors of KGL for the management of personal data within KGL and for ensuring that compliance with data protection legislation and that good practice can be demonstrated. This accountability includes:

- the development and implementation of the GDPR, the DPA and this General Data Protection Policy; and
- security and risk management in relation to compliance with this General Data Protection Policy.

3.5 KGL's Data Protection Officer, who the Board of Directors of KGL considers to be suitably qualified and possessing all the relevant

expertise, has been appointed to also take responsibility for KGL's compliance with this General Data Protection Policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that KGL complies with the GDPR and the DPA.

3.6 KGL's Data Protection Officer has specific responsibilities in respect of procedures such as the Data Subject request and is the first point of call for Data Subjects seeking clarification on any aspect of data protection compliance.

3.7 Notwithstanding the role and responsibilities of KGL's Data Protection Officer, compliance with data protection legislation is the responsibility of all employees and préposés of KGL who process personal data for and on behalf of KGL.

3.8 Employees and préposés of KGL are responsible for ensuring that any personal data about them and supplied by them to KGL is accurate and up-to-date. The rights and freedoms of employees and prospective employees of KGL under both the GDPR and DPA are more specifically dealt with in KGL's Employment (Privacy) Notice and Recruitment (Privacy) Notice respectively.

4. Data protection principles

All processing of personal data will be conducted by KGL in accordance with the data protection principles as set out in the GDPR and the DPA.

KGL therefore undertakes to comply with the following principles:

4.1 Lawfulness, fairness and transparency

4.1.1 KGL will at all times:

(a) identify a lawful basis before processing personal data and inform Data Subjects of the same prior to the processing of their personal data; and

(b) act fairly and transparently towards Data Subjects by making available to the latter, as far as reasonably practicable, all relevant information pertaining to the intended processing of their personal data whether the personal data is obtained directly from the Data Subjects or from other sources.

4.1.2 The information that KGL will provide to the Data Subjects includes:

(a) the contact details of KGL and of its Data Protection Officer;

(b) the specific and explicit purpose(s) for which the personal data is needed as well as the legal basis for the processing of the same;

(c) the period for which the personal data will be stored;

(d) the existence of the Data Subjects' rights to request access, rectification, erasure or to object to the processing; and

(e) the recipients or categories of recipients of the personal data, where applicable;

(f) KGL's obligations to report to the relevant supervisory authority, possible breaches of data protection rules and principles and inform the concerned Data Subjects of the same; and

(g) where applicable, whether KGL intends to transfer personal data to a recipient in a third country and the level of protection afforded to the personal data in that third country.

4.1.3 All such information will be readily available in KGL's General Privacy Policy.

4.2 Purpose limitation

4.2.1 KGL shall at all times ensure that where personal data is obtained for a specified purpose, the said data will not be used for another purpose that differs from the purpose initially notified to the Data Subject in KGL's General Privacy Policy.

4.2.2 KGL shall, in its General Privacy Policy, define upfront what the personal data will be used for and limit the processing to only what is necessary to meet that purpose.

4.3 Data minimization

4.3.1 KGL shall at all times ensure that the personal data it processes is adequate, relevant and limited to what is necessary for the processing.

4.3.2 KGL will not collect from the Data Subject information that is not strictly necessary for the purpose for which it is obtained as explained in KGL's General Privacy Policy.

4.3.3 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, will include a fair processing statement via a link to KGL's General Privacy Policy.

4.3.4 Through Data Protection Impact Assessments ('DPIAs'), KGL will every year ensure that all data collection methods are reviewed by either an internal audit or external expert to ensure that collected data continues to be adequate, relevant and not excessive.

4.4 Accuracy

4.4.1 Data that is stored by KGL will be reviewed and updated as necessary. No data will be kept unless it is reasonable to assume that it is accurate.

4.4.2 All KGL staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3 It is also the responsibility of the Data Subject to ensure that data held by KGL is accurate and up to date. Data Subjects will from time to time be requested by KGL to fill-in forms and check-lists which will include a statement that the data contained therein is accurate.

4.4.4 Employees of KGL are required to notify KGL promptly of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of KGL to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.5 KGL is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, considering the volume of data collected, the speed with which it might change and any other relevant factors.

4.4.6 On at least an annual basis, KGL will review the retention dates of all the personal data processed by it, by reference to its Data Inventory, and will identify any data that is no longer required. This data will be securely deleted/destroyed.

4.4.7 KGL's Data Protection Officer is responsible for responding to requests for rectification from Data Subjects within one month. This can be extended to a further two months for complex requests. If KGL decides and is justified in law not to comply with the request, KGL's Data Protection Officer will respond to the Data Subjects to explain KGL's reasoning and justification and inform them of their rights to complain to the supervisory authorities.

4.4.8 KGL's Data Protection Officer is responsible for making appropriate arrangements, where third-party organizations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used; and for passing any correction to the personal data to the third party where this is required.

4.5 Storage limitation

4.5.1 Personal data will always be kept by KGL in a form such that the Data Subject can be identified only as long as is necessary for processing.

4.5.2 Where personal data is retained beyond the processing date, it will be encrypted and/or pseudonymized in order to protect the identity of the Data Subject.

4.5.3 Personal data will be retained in line with KGL's Retention of Records Procedure. Once its retention date is passed, it will be securely destroyed as set out in the Retention of Records Procedure save and except if the further storage and retention of the data is necessary for KGL's legitimate interests (such as defending itself in possible legal proceedings) and/or for KGL to comply with a legal obligation.

4.6 Integrity and confidentiality

4.6.1 KGL will at all times process personal data in a manner that ensures appropriate security of the said data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

4.6.2 In that respect, KGL's Data Protection Officer will carry out a risk assessment considering all the circumstances of KGL's controlling or processing operations.

4.6.3 In determining appropriateness, KGL's Data Protection Officer will also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on KGL itself, and any likely reputational damage including the possible loss of customer trust.

4.6.4 When assessing appropriate technical measures, KGL's Data Protection Officer will consider the following:

a) password protection;

b) automatic locking of idle terminals;

c) removal of access rights for USB and other memory media;

d) virus checking software and firewalls;

e) role-based access rights including those assigned to temporary staff;

f) encryption of devices that leave KGL's premises such as laptops;

g) privacy enhancing technologies such as pseudonymisation and anonymisation; and

h) identifying appropriate international security standards relevant to KGL.

4.6.5 When assessing appropriate organisational measures, KGL's Data Protection Officer will consider the following:

(a) the appropriate training levels throughout KGL;

(b) measures that consider the reliability of employees (such as references etc.);

(c) the inclusion of data protection in employment contracts and/or the implementation of an Employment (Privacy) Notice;

(d) identification of disciplinary action measures for data breaches by KGL's employees;

(e) monitoring of KGL staff for compliance with relevant security standards;

(f) physical access controls to electronic and paper-based records;

(g) adoption of a clear desk policy;

(h) storing of paper-based data in lockable and fire-proof filing cabinets;

(i) restricting the use of portable electronic devices outside of the workplace;

(j) restricting the use of employees' own personal devices being used in the workplace;

(k) adopting clear rules about passwords;

(l) making regular backups of personal data and storing the media off-site; and

(m) the imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside Mauritius and/or the European Union.

4.6.6 These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.6.7 KGL's compliance with this principle is more fully contained in its Information Security Policy.

4.7 Accountability and compliance

4.7.1 KGL will at all times promote good governance and demonstrate its accountability in respect of data protection principles.

4.7.2 In addition to strictly adhering to the transparency requirements, KGL Ltd will, to the best of its abilities, explicitly and publicly demonstrate that it scrupulously complies with the data protection principles and all the applicable data protection laws including the GDPR and the DPA.

4.7.3 Not only does KGL ensure through its Training Policy that it's staff is appropriately trained and knowledgeable in the treatment of personal data, but in order to further buttress its determination at affording the best possible protection to the rights and freedoms of Data Subjects, KGL has implemented all the relevant data protection policies such as this General Data Protection Privacy as well as all the necessary technical and organisational measures in line with the GDPR and the DPA.

4.7.4 KGL intends to carry out regular DPIAs as well as reviews of its policies, procedures, technical and organisational measures and to update the same in order to always better safeguard the rights and freedoms of Data Subjects.

4.7.5 In that respect, KGL encourages its customers and the public at large to provide and to communicate to it regular feedbacks on the manner in which it treats and protects personal data.

4.7.6 All such feedbacks are to be addressed to KGL's Data Protection Officer whose contact details are set out at paragraph 3.3 above.

5. Data subjects' rights

5.1 KGL wishes to most unequivocally inform Data Subjects at large that they have the following rights regarding data processing, and the data that is recorded by KGL about them:

(a) to make subject access requests regarding the nature of information held and to whom it has been disclosed;

(b) to prevent processing likely to cause damage or distress;

(c) to prevent processing for purposes of direct marketing;
(d) to be informed about the mechanics of automated decision-taking process that will significantly affect them;
(e) not to have significant decisions that will affect them taken solely by automated process;
(f) to sue for compensation if they suffer damage by any contravention of the GDPR and/or the DPA;
(g) to act to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data;
(h) to request the supervisory authorities to assess whether any provision of the law has been contravened;
(i) to have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another Data Controller; and
(j) to object to any automated profiling that is occurring without consent.

5.2 KGL will further ensure that Data Subjects may exercise the aforesaid rights as follows:
- Data Subjects may make data access requests; and
- Data Subjects have the right to complain to KGL in relation to the processing of their personal data, the handling of a request and appeals on how complaints have been handled by KGL.

6. Consent

6.1 KGL understands 'consent' to mean that it has been explicitly and freely given, and is a specific, informed and unambiguous indication of the Data Subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The Data Subjects can withdraw their consent at any time.

6.2 As and when required as per either the GDPR or the DPA, consent requests will be separate from other terms and conditions and will not be a precondition of signing up to a service unless it is necessary for that service.

6.3 When requesting Data Subjects to give their consent to a particular processing operation, KGL will not use pre-ticked opt-in boxes. Only unticked opt-in boxes or similar active opt-in methods will be used.

6.4 Furthermore, KGL will at all times give Data Subjects granular options to consent separately to different types of processing wherever appropriate.

6.5 Also, KGL will always keep records of consents given by Data Subjects in order to show what they have consented to, including what they were told, and when and how they consented.

6.6 KGL also understands 'consent' to mean that the Data Subject has been fully informed of the intended processing and has signified his or her agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

6.7 At no point in time will KGL imply that consent has been given. Consent will not be inferred from non-response to a communication

6.8 For the processing of Sensitive Personal Data or Special Categories Personal Data, KGL will invariably request and obtain explicit written consents of Data Subjects prior to processing the same unless an alternative legitimate basis for processing exists under either the GDPR or the DPA.

7. Security of data

7.1 All the employees of KGL are responsible for ensuring that any personal data that KGL holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by KGL to receive that information. In that respect, KGL has entered into confidentiality agreements such as Non-Disclosure Agreements with its employees.

7.2 All personal data will be accessible only to those employees of KGL who need to use it. All personal data will be treated by KGL with the highest security and will be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected; and/or
- stored on (removable) computer media which are encrypted.

7.3 Upmost care will be taken to ensure that PC screens and terminals at KGL are not visible except to authorised employees of KGL.

7.4 Manual records will not be left where they can be accessed by unauthorised personnel and will not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they will be removed from secure archiving.

7.5 Personal data will only be deleted or disposed of in line with KGL's Retention of Records Procedure. Manual records that have reached their retention date will be shredded and disposed of. Hard drives of

redundant PCs will be removed and immediately destroyed before disposal.

7.6 As the processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data, KGL staff will, in exceptional circumstances and only for the legitimate interests of KGL's business, have to be specifically authorised to process data off-site.

8. Disclosure of data

8.1 KGL will ensure that personal data is not disclosed to unauthorised third parties without the consent of the Data Subject concerned save and except if the information is required for one or more of the following purposes:

a. the furtherance of the legitimate interests of KGL and its business activities;

b. the safeguard national security and public interest;

c. the prevention or detection of crime including the apprehension or prosecution of offenders;

d. the assessment or collection of tax duty;

e. the discharge of regulatory functions imposed by law upon KGL;

f. the compliance by KGL with regulatory frameworks and other obligations imposed by law;

g. the defence by KGL of legal proceedings brought against KGL;

h. the prevention of serious harm to a third party; and

i. the protection of the vital interests of an individual.

8.2 All requests to provide data for one of the reasons set out in paragraph 8.1 above must be supported by appropriate written

evidence and/or paperwork and all such disclosures must be specifically authorised by KGL.

9. Retention and disposal of data

9.1 KGL will not keep personal data in a form that permits identification of Data Subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 KGL may store data for longer periods if the personal data will be processed solely for:

a. archiving purposes in the public interest;

b. scientific or historical research purposes or statistical purposes; and/or

c. any of the reasons set out in paragraph 8.1 above;

9.3 subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the Data Subjects concerned.

9.4 Where personal data needs to be disposed of, KGL will do so securely in accordance with the principle set out in paragraph 4.6 above, thereby protecting the rights and freedoms of Data Subjects.

10. Data transfers

10.1 As a rule, personal data lawfully collected by KGL from a particular jurisdiction ('the Original Jurisdiction') shall not be transferred to a jurisdiction other than the Original Jurisdiction ('Other Jurisdiction') unless KGL is satisfied that there is an appropriate level of protection for the fundamental rights and freedoms of the Data Subjects in the Other Jurisdiction similar to the level of protection afforded in the Original Jurisdiction (hereinafter referred to as the 'Adequacy Test').

10.2 In carrying out the Adequacy Test, KGL will consider the following factors:

- the nature of the information being transferred to the Other Jurisdiction;

- the data protection laws of the Original Jurisdiction and the data protection laws, codes of practice and international obligations if any, of the Other Jurisdiction;
- how the information will be used on the Other Jurisdiction and for how long;
- the security measures that are to be taken as regards the data in the Other Jurisdiction; and
- whether the data protection supervisory authority of the Original Jurisdiction approves or prohibits such transfer of data to the Other Jurisdiction.

10.3 Should KGL not be satisfied by the level of data protection afforded in the Other Jurisdiction after carrying out the Adequacy Test, KGL will not transfer the data to the Other Jurisdiction unless:

a. the Data Subject concerned has explicitly consented to the proposed transfer after having been informed of the possible risks of such transfers for the Data Subject due to the absence of appropriate safeguards;

b. the transfer is necessary for the performance of a contract between the Data Subject concerned and KGL or the implementation of pre-contractual measures taken at the Data Subject's request;

c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject concerned between KGL and another natural or legal person;

d. the transfer is necessary for important reasons of public interest;

e. the transfer is necessary for the establishment, exercise or defence of legal claims involving and/or impacting on KGL; and/or

f. the transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

11. Information asset register/data inventory

11.1 KGL shall establish a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR and DPA compliance project.

11.2 KGL's data inventory and data flow relate to:

a. its business processes that use personal data;
b. its sources of personal data;

c. the categories of Data Subjects whose data are processed by it;
d. the categories of personal data it processes;
e. its data processing activities;
f. the documents it uses for its compliance with the GDPR and DPA;
g. the recipients and potential recipients of the personal data it processes;
h. the roles of its Data Protection Officer and other employees are responsible for all data protection issues; and
i. any data transfers.

11.3 KGL is aware of risks associated with the processing of particular types of personal data and the level of risks to individuals associated with the processing of their personal data.

11.4 Consequently, DPIAs will be carried out every year in relation to the processing of personal data by KGL, and in relation to processing undertaken by other organisations on behalf of KGL.

11.5 KGL shall manage the risks identified by the DPIAs in order to reduce the likelihood of a non-conformance with this General Data Protection Policy.

11.6 Where a type of processing, in particular using new technologies and considering the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, KGL shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

11.7 Where, as a result of a DPIA it is clear that KGL is about to commence processing of personal data that could cause damage and/or distress to Data Subjects, the decision as to whether or not KGL may proceed must be escalated for review to its Data Protection Officer and/or its Board of Directors as the case may be. The latter shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

Document Owner and Authorisation

KASA GROUP LTD is the owner of this document.

This document and all other related documents referred to herein may, from time to time, be reviewed in line with any changes in the law.

This General Data Protection Privacy Policy as well as all the other documents referred to herein have been duly approved by the Board of Directors of KGL 18 October 2024.

By order of the Board of Directors of KGL.

Made in good faith on 18 October 2024 at 42, Edith Cavell Street, Port-Louis, Republic of Mauritius.