GraceKennedy Limited Policy	
Policy Name	**DATA PROTECTION POLICY**

1. PURPOSE STATEMENT

The Company recognizes that as part of our operations we collect and process Data. The purpose of this policy is to describe the data protection standards, and the applicable principles governing privacy and data protection laws, regulations, and best practices (the Applicable Laws) that the Company will comply with to ensure individual's rights related to their Personal Data are protected.

2. DEFINITIONS

"Company" refers to GraceKennedy Limited, each of its subsidiaries, joint venture entities and associated companies (where applicable).

"Consent" refers to any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the individual

"Data" refers to information in a format that can be processed, including electronic data and physical data.

"Data Controller" refers to:

(i) the natural or legal person, agency, or any other body, that alone or jointly with others determines the purposes for which and the manner in which any Personal Data are, or are to be, processed, and

(ii) where Personal Data are processed only for purposes for which they are required under any legislation to be processed, the person on whom the obligation to process the Personal Data is imposed by or under that legislation is a Data Controller.

"Data Processor" in relation to Personal Data, means any person, other than an employee of the Data Controller, who processes the data on behalf of the Data Controller.

"Data Storage" refers to rules that describe how and where data should be safely stored to prevent unauthorized access, retrieval, and Processing.

"Data Subject" refers to an individual that can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more identifying characteristics specific to the physical, physiological, genetic, mental, economic, cultural, or social identity which are reasonably likely to lead to the identification of the individual.

"Personal Data" refers to any information (however stored) relating to an individual data subject (living, or who has been deceased for less than thirty years) who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more identifying characteristics specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. This Data could be anything from a name, an email address, geolocation data, or even a username or IP address in the possession of, or likely to come into the possession of, the Data Controller; and includes any expression of opinion about that individual and any indication of the intentions of the Data Controller or any other person in respect of that individual.

"Processing" in relation to information or Personal Data means obtaining, recording or storing the information or Personal Data, or carrying out any operation or set of operations (whether or not by automated means) on the information or data, including—

(i) Collection, recording, organisation, adaptation or alteration of the information or data;
(ii) Storing, retrieving, structuring, consulting or using the information or data;
(iii) Disclosing the information or data by transmitting, disseminating or otherwise making it available; or
(iv) Aligning, combining, blocking, restricting, erasing or destroying the information or data, or rendering the data anonymous.

3. SCOPE

3.1. This policy applies to all aspects of the governance of Personal Data including the collection, Processing, storage, and handling of Personal Data and any other principles and procedures related to Personal Data of an individual, in electronic and physical format. The governance of Personal Data extends to all business processes, information systems and components, personnel acting on behalf of the Company, and the Company's facilities.

3.2. This policy applies to Personal Data provided by individuals to the Company, including but not limited to:

(i) Directors
(ii) Employees, whether employed on a full-time or part-time basis
(iii) Previous employees, whether employed on a full-time or part-time basis
(iv) Job candidates
(v) Contractors, suppliers, and other people working on behalf of the Company
(vi) All customers of the Company

3.3. In the event of a conflict between the provisions of this policy and the laws of the country in which the Company operates, the provisions of this policy will be superseded by the provisions of the law to the extent necessary for compliance with the law.

4. POLICY STATEMENTS

4.1 The Rights of Data Subjects

4.1.1 The Applicable Laws confer on individuals also referred to as Data Subjects a set of rights regarding their Personal Data. The Company is

obligated under the Applicable Laws to ensure that the individual's rights are protected and is committed to compliance with these obligations.

4.1.2 The Data Subjects whose Personal Data the Company holds have the following rights which the Company will observe

(i) The right to be informed - Data Subjects should be told the type of information the Company collects about them and the purpose for which it is collected.
(ii) The right of access - Data Subjects have a right to know whether the Company is Processing their Personal Data and to be given a copy of the Personal Data being held about them in keeping with any requirements under the Applicable Laws.
(iii) The right to rectification – inaccurate Personal Data is to be corrected within a reasonable time and where information is incomplete it must be updated. The Company will ensure Data Subjects can easily update their information as necessary.
(iv) The right to erasure (the right to be forgotten) – Personal Data held by the Company is to be erased when certain conditions are met.
(v) The right to restrict Processing – the Company can store but not use Personal Data.
(vi) The right to data portability – Data Subjects are provided with their Personal Data the Company holds for transmission to another Data Controller where this is technically feasible.
(vii) The right to object in relation to automated decision-making including profiling – Data Subjects can object to their Personal Data being Processed for direct marketing and being included in automated decisions and profiling.
(viii) The right to object to direct marketing – Data Subjects can object to the Processing of their Personal Data for direct marketing purposes.

4.1.3 Data Subjects are entitled under the Applicable Laws to enforce their rights against the Company in relation to the Personal Data the Company holds for them. The Company may be exempted from observing the rights of the Data Subjects in the circumstances set out in 4.1.4. Such exemptions may limit the Data Subjects rights.

4.1.4 The categories of exemptions referred to in section 4.1.3. are:

(i) in the interests of national security
(ii) law enforcement and taxation
(iii) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
(iv) journalistic purposes or the purpose of academic artistic or literary expression
(v) discharge of functions conferred on a person by legislation or any function of a public nature exercised in the public interests such as: public safety, ethics for regulated professions and important national economic or financial interests such as monetary, budgetary or taxation matters.
(vi) prejudicial to the rights of another Data Subject
(vii) compromises confidentiality obligations.

The applicability of the exemptions will be considered on a case by case basis.

4.2 **Collection and Processing of Personal Data**

4.2.1 The Company must process Personal Data in a transparent way. The Company will ensure that Data Subjects are aware that their Personal Data is being processed and how to exercise their rights.

4.2.2 The following minimum requirements shall apply to the collection and Processing of Personal Data.

4.2.2.1 Personal Data shall be:

(i) collected only for a lawful specified purpose(s) and in keeping with the requisite procedures for authorizing the collection of Personal Data and shall not be processed in a manner inconsistent with the purpose(s) for which it was collected

(ii) processed fairly and for lawful purposes only, and where applicable with the informed consent of the Data Subject

(iii) adequate, relevant, and limited to, the purpose for which it is being processed.

(iv) accurate and where necessary, kept up to date through the means of auditing, review processes, and the implementation of security controls.

(v) processed by the Company in accordance with Data Subjects rights and the relevant standards for the Processing of Personal Data as established by the Applicable Laws

(vi) safeguarded from unauthorized or unlawful Processing, accidental loss or destruction or damage by internal or external parties.

(vii) retained in a form that permits identification of Data Subjects for no longer than is necessary to fulfill the purposes for which the Personal Data are processed unless the Applicable Laws provide otherwise.

(viii) for the purposes of direct marketing, obtained with the consent of the Data Subjects or if the Data Subjects are customers of the Company the Data Subjects' contact details have been received in the context of sale of goods or services and the Company is marketing similar goods and services to the customer.

4.2.2.2 Personal Data shall not be:

(i) Disclosed either within the Company or externally unless in accordance with the Company's published guidelines for Data access.

(ii) Transferred to another state or territory unless that state or territory ensures an adequate level of protection for the rights of Data Subjects in relation to the Processing of Personal Data except in the following cases:

(i) the Data Subjects Consent to the transfer;

(ii) the transfer is necessary for the performance of a contract between the Data Subjects and the Data Controller or for the taking of steps at the request of the Data Subject with a

view to the Data Subjects entering into a contract with the Data Controller

(iii) the transfer is necessary for the conclusion or performance of a contract, between the Data Controller and a person other than the Data Subject, which is entered into at the request of the Data Subject or is in the interests of the Data Subject

(iv) the transfer is necessary for reasons of substantial public interest

(v) the transfer is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), obtaining legal advice or is otherwise necessary for the purpose of establishing, exercising, or defending, legal rights

(vi) the transfer is necessary in order to protect the vital interests (health, physical integrity or life) of the Data Subjects

(vii) the transfer is part of the Personal Data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the personal data are or may be disclosed after the transfer

(viii) the transfer is made on terms (which may include contractual terms) that are of a kind approved by the relevant supervisory authority as ensuring adequate safeguards for the rights and freedoms of Data Subjects

(ix) the transfer has been authorised by the relevant supervisory authority as being made in such a manner as to ensure adequate safeguards for the rights of Data Subjects

4.3 **Consent of Data Subjects to Processing**

4.3.1 The Company will collect Personal Data in a transparent manner in accordance with the Applicable Laws ensuring that Data Subjects have consented to the Processing unless Consent is not required. Consent shall be obtained from Data Subjects in accordance with the Company's consent procedures. The principle of transparency requires that any information and communication relating to the Processing of Personal Data is easy to access and understand and is presented in clear and plain language. where an exemption to obtaining the Data Subject's consent to Processing is not applicable.

4.3.2 Where applicable, the Company will provide each Data Subject with information regarding the Processing of their Personal Data to allow the Data Subject to provide informed consent.

4.4 **Data Protection Training**

The Company will train employees to help them understand their responsibilities regarding compliance with the Company's policies and procedures for Data Protection.

4.5 **Organisational & Technical Measures**

The Company commits to establishing appropriate organisational and technical measures to ensure and demonstrate Processing of Personal Data in accordance

with the Applicable Laws, taking into consideration the state of technological development and the cost of implementing these measures. These measures may include:

(i) preventing the unauthorised or unlawful Processing, accidental loss damage or destruction of Personal Data.
(ii) pseudonymisation and encryption of Personal Data.
(iii) restricting and monitoring access to Personal Data.
(iv) developing transparent data collection procedures.
(v) training employees in online privacy and security measures as well as in physical record security.
(vi) maintaining secure networks to protect online data from cyberattacks.
(vii) establishing clear procedures for reporting privacy breaches or data misuse.
(viii) policies and procedures for reporting incidents or data breaches are established.
(ix) ensuring that contractual agreements are in place with Data Processors who process data on behalf of the Company.
(x) preserving confidentiality, integrity, availability and resilience of Processing systems and services.
(xi) restoring the availability of, and access to, Personal Data in a timely manner in the event of a physical or technical incident.
(xii) establishing data protection practices (document shredding, data encryption, frequent backups, access authorization, etc.).
(xiii) regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing of Personal Data.
(xiv) ensuring all physical and technical infrastructure containing data is protected and secured.

Reference should be made to the relevant Information Technology policies and the established access management guidelines further details on the technical and organizational measures.

4.6 Data Storage & Retention

The Company will ensure that Personal Data is handled in a manner consistent with the rights of the Data Subject by the establishment of policies and procedures that stipulate the manner in which Personal Data is stored, retrieved, retained and destroyed. Personal Data should be regularly reviewed and if is no longer required, should be deleted, and destroyed . Reference should be made to the policies and and procedures for the custody, storage, retention and destruction of Personal Data for further details on the obligations and responsibilities of the Company and personnel acting on its behalf.

4.7 Providing Information – Data Subject Access Requests

The Company shall establish and implement policies and procedures for managing Data Subjects' access requests.

4.8 Data Breaches

The Company shall establish and implement policies and procedures for managing Data Breaches.

4.9 Data Protection Impact Assessments

The Company shall conduct data protection impact assessments in accordance with Applicable Laws. The assessment shall evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be considered when determining the appropriate measures to be taken in order to demonstrate that the Processing of Personal Data complies with the Applicable Laws.

4.10 **Monitoring of Processing Activities**

The Company shall review the Personal Data Processing activities it undertakes to ensure that the Processing complies with the purposes for which the Data is obtained. Records will be kept of the Company's Processing activities to demonstrate compliance with its obligations under the Applicable Laws.

4.11 **Data Protection Officer**

Where the criteria set out in the Applicable Laws for the appointment of a data protection officer are satisfied, the Company will appoint a data protection officer to monitor in an independent manner the Company's compliance with the Applicable Laws.

5. BREACH OF POLICY

A breach of this policy may also violate other laws which can lead to significant penalties for the Company. An employee who breaches this policy, may face disciplinary action including separation from the Company in accordance with the Corrective/Disciplinary Action Policy.

6. POLICY REVIEW

This policy shall be reviewed at least every three (3) years.