alteo

Alteo Group Data Protection Policy

Contents

During the course of its activities, Alteo collects, stores and processes, in general, Personal Data about individuals. These include its employees, clients, business contacts, visitors, shareholders, directors and other third parties Alteo has a relationship with or may need to contact (the "**Data Subjects**"). All these individuals have rights regarding the way their Personal Data is handled. Alteo recognizes that the correct and lawful treatment of this Personal Data being so collected and processed will enhance trust and confidence of Data Subjects in Alteo.

This Group Data Protection Policy (the "**Policy**") describes how Personal Data, whether it be in physical or digital form, is *inter alia* collected, recorded, made available, stored, erased, or processed, in general, in compliance with the Data Protection Act 2017 (hereinafter referred as the "**Act**" or "**DPA 2017**"), and with the European Union General Data Protection Regulation ("**GDPR**"), (the **Act** and the **GDPR** being collectively referred to as the "**Data Protection Laws"**).

This Policy ensures that Alteo follows good governance practices; that it is transparent about how it stores and processes Personal Data; that it protects the rights of Data Subjects; and that it protects itself from the risks of a data breach.

1.1 DEFINITION OF KEY TERMS

Data protection terms which are used in this Policy are defined in Schedule1.

1.2 APPLICABILITY

This Policy applies to:

(i) the entities of the Alteo Group, and under Alteo management, as listed in **Appendix I** hereto (hereinafter referred to as "**Alteo**", "**Group**", "**Company**", "**Controller**" or "**Processor**");

(ii) Alteo's employees, contractors, suppliers and other people working on behalf of the Group; and

(iii) Alteo's processors, sub-processors and anyone who processes Personal Data of the Data Subjects of Alteo.

Anyone processing Personal Data for Alteo is required to comply with this Policy. Any breach of this Policy may result in disciplinary action and/or legal actions.

1.3 PURPOSE

The Group is committed to protecting the privacy and confidentiality of the Personal Data of its Data Subjects. Alteo is a Controller and/or Processor of Personal Data, duly registered with the Data Protection Commissioner (the "**Commissioner**"), and it thus has the statutory duty to adopt internal policies and implement procedures and processes to ensure data protection.
This Policy does not form part of any contract Alteo has with its Data Subjects, be it its employees or its clients and service providers and may be amended at any time. It serves to set out the rules on data protection, confidentiality, security, and the legal conditions that must be satisfied when Alteo processes Personal Data of Data Subjects.

1.4 GROUP DATA PROTECTION OFFICER ("GDPO")

The GDPO is Ms. Roovisha Seetohul, the Head of Legal and Corporate Affairs of Alteo Group. The GDPO is responsible for ensuring that the Data Protection Laws and this Policy are complied with. Any questions about this Policy or the Data Protection Laws or any concerns that the Policy or the Data Protection Laws not having been complied with should be referred to the GDPO, whose contact details are as follows:

Ms. Roovisha Seetohul
Email: dpo@alteo.mu
T (230) 402-9050

1.5 COMMUNICATION

The GDPO shall ensure that this Policy is communicated to all Alteo entities and that all employees and other relevant stakeholders of Alteo have taken cognisance of the Policy.

1.6 GENERAL POLICY GUIDELINES

This Policy must be read together with other policies, process documents, templates and/or guidelines which are mentioned herein.

1.7 REVISIONS AND UPDATES

This Policy shall be reviewed annually, or earlier where applicable, in line with any amendment/s to the Data Protection Laws and/or operational processes that may have changed.

2. GOVERNANCE

2.1 OBJECTIVES

Alteo recognises the importance of the privacy of Personal Data and the ensuing requirement for the correct and lawful treatment of this Personal Data, within the principles of good governance and the obligations of the Data Protection Laws. To provide for an effective process of compliance, risk management and internal control system, a data governance framework is required to provide for structures, processes, information flows, controls, and decision making. Specific roles and responsibilities shall be delegated to different individuals within Alteo to govern and oversee compliance with the Data Protection Laws.

A robust governance strategy ensures that a culture of data protection is adopted at every level and strengthens transparency pertaining to data processing within Alteo.

2.2 GOVERNANCE FRAMEWORK AND THE DATA PROTECTION COMMITTEE

Taking into account Alteo's structure and size, a privacy governance framework has been defined. As such, a Data Protection Committee ("**Committee**") shall be set up, composed of the GDPO who presides the Committee, a Data Protection Coordinator ("**DPC**"), and several Data Protection Support Officers ("**DPSOs**"). The Committee is guided by Terms of Reference which clearly explain the privacy governance framework and define the roles and responsibilities of the different members of the Committee. The Committee shall have the responsibility to monitor Alteo's compliance with the Data Protection Laws and with this Policy.

The Committee shall meet regularly, as per an established calendar, unless an unforeseen incident requires the attention of the Committee urgently. The Committee shall ensure that appropriate structures are put in place at the required levels within Alteo.

2.3 KEY AREAS OF RESPONSIBILITY

2.3.1 THE BOARD OF DIRECTORS

The Board of Directors of Alteo Limited is ultimately responsible for ensuring that Alteo meets its legal obligations.

2.3.2 The GDPO

The GDPO shall report on data protection responsibilities, risks and issues to the Audit and Risk Committee of Alteo Limited, which has been delegated by the Board of directors of Alteo Limited to monitor the Group's risk management and internal control systems.

The GDPO shall, with the assistance of the DPC and each DPSO, oversee the following within each Business Unit:

(i) Implementation of appropriate data security and organisational measures;
(ii) Record keeping of all processing operations;
(iii) Data protection impact assessments (as required);
(iv) Monitoring compliance with the Data Protection Laws;
(v) Training employees on the proper handling of personal data; and
(vi) Data protection audits.

The GDPO is also the point of contact of different stakeholders of the Group, including company directors, shareholders, employees, clients, service providers, as well as the Data Protection Office. The GDPO handles data protection questions from Data Subjects covered by this Policy and deals with requests from individuals to see the data Alteo holds about them (also called 'data subject access requests').

2.3.3 THE DATA PROTECTION COMMITTEE

The members of the Committee have the overall responsibility to oversee data privacy compliance and risk management at operational level.

2.3.4 THE HEAD OF IT AND INNOVATION OF ALTEO ("HEAD OF IT")

Alteo has a Group Information Technology and Security Policy regarding its Information Technology Systems ("**Alteo's IT Policy**"), which is owned by the Head of IT.

As more amply detailed in Alteo's IT Policy, the Head of IT ensures *inter alia*, that all systems, services and equipment used for storing data meet acceptable security standards; that regular checks and scans are performed to monitor the proper functioning of security hardware and software; and that a proper evaluation of any third-party services Alteo considers using to store or process data takes place (for instance, cloud computing services).

2.4 TRAINING AND AWARENESS

In-depth training on data protection by trainers who are well versed in the field shall be provided to members of the Data Protection Committee and a more general privacy training shall be provided to all other employees of Alteo who process personal data including sensitive data.

All trainings provided shall be formally documented by the DPSOs to be able to monitor who has been trained and when. Thus, the DPSOs shall ensure that all employees are adequately trained and well prepared to carry on their day-to-day operations which involves the processing of Personal Data, in full compliance with the Data Protection Laws.

3. POLICY STATEMENTS

3.1 DISCLOSURE OF PERSONAL DATA

3.1.1 INTERNAL DISCLOSURE

Alteo has distinct legal entities and may be required to share personal data between entities of the Group. It shall do so when (i) it has a legal basis for doing so; (ii) the data being disclosed is adequate, relevant and limited to the purpose for which it is being disclosed; (iii) when it has a data sharing agreement in place; and (iv) where the Data Subjects whose data are being shared have been notified of such sharing in a data privacy notice.

3.1.2 EXTERNAL DISCLOSURE

Alteo does not routinely disclose Personal Data to other organisations and/or authorities unless:

(i) The disclosure is required by law;
(ii) The disclosure is necessary for the performance of a contract;
(iii) The disclosure is necessary to protect the vital interests of a Data Subject or another person;
(iv) Express consent has been provided by the relevant Data Subject;
(v) The disclosure has a legal basis which is set out under section 28 of the DPA 2017.

3.2 EMPLOYEE DATA PRIVACY NOTICE

An Employee Data Privacy Notice is available for all Alteo Employees, which explains to Employees how and why Alteo processes their Personal Data and their rights concerning their Personal Data.

3.3 EXTERNAL PRIVACY NOTICE

An external Privacy Notice is available for the entities found in the different Business Units of Alteo. The external Privacy Notice targets Data Subjects, other than Employees, whose Personal Data are

being processed by Alteo, such as clients, directors, shareholders, third party service providers, suppliers and other external stakeholders. The external Privacy Notice provides *inter alia*, the following information:

(i) The purpose of data processing and the legal basis for processing;
(ii) How Personal Data is shared within the Group and the recipient of the Personal Data;
(iii) To which country/ies will the data be transferred and the level of protection afforded by the country/ies;
(iv) The period for which Personal Data will be stored;
(v) The ability to withdraw consent at any time;
(vi) The right to request access to, rectify, erase, object to or restrict processing of Personal Data;
(vii) The right to lodge a complaint with the Data Protection Commissioner; and
(viii) The contact information of the GDPO.

Each DPSO shall be responsible to ensure that the operations of their designated Business Unit align with this Policy, and that Data Subjects of their designated Business Unit are aware of the applicable Privacy Notice which sets out how their Personal Data is being processed.

3.4 INFORMATION TECHNOLOGY AND SECURITY

Alteo is committed to ensure the security of Personal Data to prevent unauthorised access, accidental deletion, and malicious hacking attempts. The computers storing the information are kept in a secure environment with restricted physical access. Alteo uses secure firewalls and other measures to restrict electronic access. All automated collection tools (social media, mobile platform, websites etc.) shall enable cookies and a consent mechanism shall be used to seek the consent of end-users before certain types of cookies collect Personal Data of end users. A Cookie Policy will also be made available to end users to inform them of the type of cookies being used and the Personal Data being collected by the cookies.

3.5 PROCESSING OF PERSONAL DATA AND DATA SUBJECTS' RIGHTS

3.5.1 DATA SUBJECTS

Personal Data is any information related to an identified or identifiable living individual. An identifiable individual is one who can be identified, directly or indirectly, by reference to an identifier which includes but is not limited to:

- his/her first name, family name;
- an identification number, e.g ID Number, Social Security Number;
- factors specific to his/her physical traits, e.g fingerprints;
- his/her habits, tastes;

- his/her health details.

As part of its business activities, Alteo processes Personal Data from its Employees and non-employees, such as:

(a) Employees

- Identity Details, such as name, NIC number; data of birth;
- Contact Details, such as phone number, email and physical address;
- Bank Details (where applicable);
- Leaves, such as annual leave, sick leaves;
- Remuneration, such as salary, travel allowance;
- Fingerprints;
- CCTV camera footage;
- Photos;
- Health data;
- Marital Status and number of children;
- CV.

(b) Non-Employees

- Identity Details, such as name, NIC number;
- Contact Details such as phone number, email address and physical address;
- Bank Details (where applicable);
- IP Address.

3.5.2 DATA COLLECTION AND PROCESSING

Alteo collects different types of Personal Data to fulfil its needs and obligations. Personal Data can be collected by either of the following means:

- From the Data Subject in person;
- Online Bookings;
- Online registration;
- Use or view of Alteo's websites via browsers' cookies; or
- Via email received by Alteo.

3.5.3 LEGAL BASIS FOR PROCESSING OF PERSONAL DATA

Personal Data cannot be processed unless there is a lawful basis for doing so. Lawful processing takes place where:

(a) The processing is necessary:

- 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;
- for compliance with any legal obligation to which the Controller is subject;
- in order to protect the vital interests of the Data Subject or another person;
- to the legitimate interests pursued by the Controller or by a third party to whom the data are disclosed;
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
- the exercise, by any person in the public interest, of any other functions of a public nature;
- for the performance of a task carried out by a public authority ; or
- for the purpose of historical, statistical or scientific research.

(b) The data subject consents to the processing for one or more specified purposes.

When consent is the lawful basis for processing personal data:

- Alteo must ensure that the consent obtained meets the criteria of being freely given, specific, informed and unambiguous. When consent is given, it should be granular and not bundled so that it is clear to what the Data Subject has consented and the consent should be taken in writing so that consent may be proved in case it is disputed. Data subjects should be informed that they have the right to withdraw consent at any time and free of charge and the mechanism to withdraw consent should be simple. No pre-ticked boxes shall be used to gather consent of the Data Subjects.

- the GDPO shall be consulted to ensure that the consent of Data Subjects is appropriately obtained, processed, and stored. Different consent forms are available from the GDPO.

The personal data of a child under the age of 16 years shall not be processed by Alteo, unless consent is given by the child's parent or guardian.

Each DPSO shall identify the type of Personal Data collected within their Business Units, the purpose of collections and legal basis for processing. The aforesaid information must be documented in accordance with recommendations of the Terms of Reference of the Data Protection Committee.

3.5.4 PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA

There are six (6) fundamental principles set out in the DPA Act 2017 which Alteo must comply with when processing personal data.

Particularly, it shall ensure that Personal Data are:

(i) processed lawfully, fairly and in a transparent manner in relation to any Data Subject;
(ii) collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with such purposes;
(iii) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
(iv) 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;
(v) 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
(vi) Processed in accordance with the rights of data subjects under the Act.

Employees of Alteo who obtain, handle, process, transport and store Personal Data for Alteo, must also always adhere to the above principles.

3.5.5 PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

Data Protection Laws confer upon the Data Subject a number of rights relating to the Personal Data being processed by Alteo. These rights are set out below. The Data Subject should contact the GDPO should he/she wish to exercise any of the said rights.

(a) Right of access

Data Subjects must make a Data Subject Access Request ("DSAR") to get access to the Personal Data Alteo holds about them. This must be made in writing and should be forwarded to the GDPO using the following email address: dpo@alteo.mu.

The GDPO will assess the query and will give a copy, free of charge, of the Personal Data requested in an intelligible form using clear and plain language to the Data Subject. The Company will, within one (1) month from receiving the request, inform the Data Subject in writing whether or not any action has been taken pursuant to his/her request. The said period of one (1) month may be extended by a further month where necessary, considering the complexity and the number of requests made by the Data Subjects.

Where the request is manifestly excessive, the Company may charge a fee for providing the information or taking the action requested or it may not take the action requested. The Company will bear the burden of proving the manifestly excessive character of the request.

Alteo shall always verify the identity of anyone making a DSAR before handing over any information. When receiving telephone enquiries, Alteo will only disclose Personal Data it holds on its systems if the following conditions are met:

(i) The caller's identity has been checked to make sure that information is only given to a person who is authorised to receive it.
(ii) Alteo shall never respond to a request regarding the Personal Data of Data Subjects unless the request is put in writing.
(iii) Payment of the relevant prescribed access fee if the request is manifestly excessive.
(iv) The conditions set out in the Act in respect of the Data Subjects' right of access are fulfilled.

Alteo will not be required to provide information where this proves to be impossible or involves a disproportionate effort.

(b) Rectification, erasure or restriction of processing

The Data Subject may also, at any time, request:

(i) to have any inaccurate Personal Data Alteo holds on the Data Subject corrected. This includes the right to supplement and/or update existing personal data provided to Alteo;

(ii) that Alteo erases any Personal Data it holds on the Data Subject where:

- such data is no longer necessary in relation to the purpose for which it was collected or otherwise processed;
- the Data Subject has withdrawn his/her consent to Alteo holding and processing such data and there are no overriding legitimate grounds for the continued processing; or
- the Personal Data of the Data Subject has been unlawfully processed.

This right is however not absolute, and it will not be applicable where the exceptions provided for by law apply, including where Alteo's processing of the Personal Data is necessary for the purpose of historical, statistical, or scientific research or for compliance with a legal obligation or for the establishment, exercise or defence of a legal claim.

It will be necessary for Alteo to restrict processing of the Personal Data of a Data Subject where:

(i) the accuracy of the Personal Data is contested by the Data Subject, for such period as may be necessary to enable Alteo to verify the accuracy of the data;

(ii) Alteo no longer needs the Personal Data for the purpose of processing, but the Data Subject requires them for the establishment, exercise or defence of a legal claim;

(iii) the processing of the Personal Data is unlawful but the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead; or

(iv) the Data Subject has objected to the processing of his/her data.

Such restriction will apply pending verification as to Alteo's legitimate grounds to keep processing the Personal Data, despite the objection of the Data Subject.

(c) Right to object

A Data Subject has the right to object in writing and at any time to Alteo's processing of his/her Personal Data at any time. Upon receiving such objection, Alteo will stop processing the Personal Data, except where it can demonstrate compelling legitimate grounds for the processing, which override the Data Subject's interests, rights and freedoms or for the establishment, exercise or defence of a legal claim to continue such processing.

Where Personal Data are processed for the purpose of direct marketing, the Data Subject may object to processing of Personal Data concerning him/her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where a Data Subject objects to processing of Personal Data for the purpose of direct marketing, the Personal Data will no longer be processed for that purpose. Such right of the Data Subject to object to processing for marketing will be explicitly brought to the attention of the Data Subject.

(d) Right to lodge a complaint

Data subjects should be informed that should they feel that Alteo has not processed their Personal Data lawfully or as per the requirements of the Act, they should contact Alteo through its Group Data Protection Officer. However, should they remain unsatisfied, they may lodge a complaint with the Commissioner in Mauritius. The contact details are as follows:

Data Protection Office
5th Floor, SICOM Tower, Wall Street, Ebène
Email address: dpo@govmu.org or dpo2@govmu.org
Phone number: + (230) 460-0251
Fax: + (230) 489-7341

(e) Right to data portability

Under the GDPR, the Data Subject has the right to obtain his/her Personal Data processed by Alteo in a "structured, commonly used and machine-readable format." The Data Subject also has the right to ask Alteo to transfer his/her data to another organisation. However, please note that we will do so only if the transfer is "technically feasible". This right to data portability only applies to data that **(i)** is held electronically; and **(ii)** the Data Subject has provided to the Company.

Data which the Data Subject has provided does not just mean information typed in, such as a username or email address. It may include Personal Data the Company has gathered from monitoring the activities of the Data Subject when he/she has used a device or service. This may include **(i)** website or search usage history; or **(ii)** traffic and location data.

The Data Subject exercises his/her right to portability by making the request directly to the Company in writing.

3.6 DATA SECURITY AND RISK MANAGEMENT

3.6.1 SECURITY CONTROLS

Alteo is committed to ensuring the security of the Personal Data it processes to prevent the unlawful or unauthorized access to; alteration of; the disclosure of; the accidental loss of; and destruction of the data in its control. Alteo shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate:

(i) the pseudonymisation and encryption of personal data (where possible);
(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(iv) different process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
(v) a process to notify the relevant authorities and Data Subjects in the event of a data breach; and
(vi) security measures and procedures which include:

- **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

- **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. Personal information is always considered confidential (except if publicly available).

- **Methods of disposal.** Paper documents should be shredded. Personal data stored on digital storage devices will be erased when they are no longer necessary.

- **Application of clear desk principles (further explained in Alteo's IT Policy)**

- **Equipment.** Employees must ensure that individual monitors do not show confidential information to passers-by and that they password protect and log off from their PC when it is left unattended.

- **Processor Agreements.** When dealing with Personal Data, agreements between the Company and its processors or sub-processors have to be put in place with specific clauses relating to the respective obligations and responsibilities of the controller and processor/sub-processor in terms of data protection. Alteo needs to assess the professionalism, integrity and security measures put in place by the processor in accordance with its data protection obligations and to the satisfaction of the Company.

- **Sharing agreements.** When sharing personal data (such as with the different entities of the Group, with auditors, bankers, lawyers or other companies outside the Group) a data sharing agreement between Alteo and the sharing entities may be envisaged with specific clauses relating to the respective obligations and responsibilities of the Controller and the sharing party in terms of data protection.

3.6.2 DATA PROTECTION BY DESIGN

Data protection by design is about considering data protection issues at the time of conception of a new project which will involve the processing of Personal Data. This ensures compliance with the principles of data protection. Therefore, whenever Alteo shall embark on any new project that requires the processing of Personal Data of a Data Subject, it shall ensure that privacy considerations are high on the agenda. The intended processing activities, the risks that these may rise and the appropriate technical and organisational measures to minimise the risks and ensure compliance with the Data Protection Laws shall be taken into consideration.

3.6.3 MONITORING

All Employees acting under the authority of a Controller or Processor shall not process Personal Data except on instructions from the Controller and/or Processor, i.e. which forms part of their duties only. Any non-compliance thereto may be reported to a DPSO or the GDPO.

Furthermore, each DPSO shall monitor compliance with this present Policy and the appropriate implementation of security measures within its respective Business Unit. Compliance monitoring shall be effected *inter alia* as follows:

- Through verification carried out by DPSOs which shall ensure that each Business Unit is implementing the present Policy, including managing the data lifecycle from acquisition to processing, storage to archiving/purging with the objective to minimise data collection point, secure the data flow and at rest, deletion of data if not used for specific purpose;

- Via Internal Auditors, who shall be required to investigate aspects of risk assessment and in particular the adequacy of the mechanisms for identifying, assessing and controlling significant risks to Alteo.

3.6.4 CROSS – BORDER TRANSFER AND SAFEGUARDS

Alteo may from time to time transfer certain Personal Data outside of Mauritius. However, any such transfer of data does not change any of Alteo's commitments to safeguard privacy and the Personal Data remains subject to existing confidentiality obligations. Alteo shall ensure that any cross-border transfer is necessitated and lawful.
Furthermore, all provisions of the present Policy shall be applied in order to ensure that the level of protection of Data Subjects whose Personal Data are transferred abroad are not undermined. Each DPSO shall be responsible to ensure that such protection is appropriately complied with at all times.

Alteo may transfer any Personal Data it holds to a country outside of Mauritius, provided that:

(i) Notification of the transfer is made to the Data Protection Commissioner through the GDPO. The notification will have to mention the appropriate safeguards with respect to the protection of Personal Data which has been taken by the Company to protect the data being transferred; or

(ii) The Data Subject has given explicit consent to the proposed transfer having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards; or

(iii) The transfer is necessary for one of the reasons set out in the Act which would include:

- the performance of a contract between Alteo and the Data Subject or the implementation of pre-contractual measures taken at the Data Subject's request;
- protection of the vital interests of the Data Subject;
- when it is legally required for reasons of public interest;
- for the establishment, exercise or defence of legal claims; or
- for the purpose of compelling legitimate interests pursued by the Controller or the Processor which are not overridden by the interests, rights and freedoms of the Data

Subjects involved.

3.6.5 DATA PRIVACY IMPACT ASSESSMENT

Where processing operations are likely to result in a high risk to the rights and freedoms of Data Subjects by virtue of their nature, scope, context and purposes, Alteo will, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

The Data Protection Office has come up with a non-exhaustive list of criteria which can be considered for evaluating whether a processing operation is likely to present high risks. In the event the processing operation meets 2 or more criteria, it can be considered as likely to present high risks. The list of criteria is as follows:

(i) Evaluation or scoring personal aspects/behavior of people including profiling;
(ii) Automated decision making producing legal or similar significant effects;
(iii) Systematic monitoring by observing, monitoring or controlling Data Subjects;
(iv) Processing of sensitive data (special categories of personal data) or data of a highly personal nature;
(v) Data processed on a large scale;
(vi) Matching or combining data sets;
(vii) Data on vulnerable person for whom the data relates (e.g., people with mental illness, or elderly people, patients, children, etc.);
(viii) Innovative use or application of new technological or organizational solutions; or
(ix) When the processing prevents Data Subjects from exercising a right or using a service or a contract.

A DPIA must include, amongst other things:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by Alteo;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of Data Subjects; and
- the measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the regulations, taking into account the rights and legitimate interests of Data Subjects and other persons concerned.

If there is uncertainty regarding whether it is appropriate to carry out a DPIA for a specific project, by

default the project team should err on the side of caution and ensure that one is performed. Further guidance may be sought from the Data Protection Office. It is the GDPO who has the responsibility to advise the Company, in all independence, whether a DPIA is required for a processing operation or not.

The DPIA needs to be signed by 3 people, namely, the one who carries out the DPIA, the one who reviews the DPIA and the one who approves the DPIA. Once completed, a copy of the DPIA needs to be submitted to the Data Protection Office.

Once a DPIA is completed, it is advisable to redo the assessment every 2 years to cater for any element which may have changed.

3.6.6 LEGITIMATE INTEREST ASSESSMENT

Whenever the legal basis for processing personal data is legitimate interest, a legitimate interest assessment needs to be carried out. The legitimate interest assessment consists of three limbs which are as follows:

Purpose Test: Alteo needs to assess whether there is a legitimate interest behind the processing;

Necessity Test: It needs to assess whether the processing is necessary for the purpose identified;

Balancing Test: It needs to consider the impact on the individual's interests and rights and freedoms and assess whether this overrides the Company's interests.

3.7 DATA LIFECYCLE MANAGEMENT

3.7.1 RECORD OF PROCESSING OPERATIONS

Alteo ensures that the Personal Data it processes are up to date and accurate by documenting its data source, location and flows, including where such data is transferred abroad. These processes shall be reviewed, either quarterly, bi-anually or annually, depending on the complexity and sensitivity of the data. Each DPSO shall identify, list and analyse the personal data processed within their respective Business Unit.

Alteo needs to maintain a record of all processing operations under its responsibility. The record shall set out –

(i) the name and contact details of the Controller and/or Processor, and, where applicable, its representative and the data protection officer;

(ii) the purpose of the processing;
(iii) a description of the categories of Data subjects and of Personal Data;
(iv) a description of the categories of recipients to whom Personal Data have been or will be disclosed, including recipients in other countries;
(v) any transfers of data to another country and the suitable safeguards;
(vi) where possible, the envisaged time limits for the erasure of the different categories of data; and
(vii) a description of the technical and organizational measure implemented by the Company.

According to the Act, Alteo will, on request, make the record available to the Data Protection Office.

3.7.2 RETENTION AND DISPOSAL

Alteo shall have a Data Retention and Disposal Policy which establishes the standards of retention, and deletion, and the Data Retention and Disposal Schedule specifically records the retention periods for different categories of personal data.

Where there is no specific statutory obligation to maintain Personal Data for a specific period, or where the statutory delay to keep Personal Data has lapsed, the GDPO shall in consultation with respective Heads of Department, determine the appropriate retention period, which is morefully explained in the Data Retention and Disposal Policy.
Alteo's Data Retention and Disposal Schedule shall be under the joint responsibility of the GDPO and Heads of Departments together with the respective DPSO.

3.8 DATA BREACH MANAGEMENT

3.8.1 PERSONAL DATA BREACH RESPONSE

(a) Identifying a Personal Data Breach

A Personal Data Breach occurs when accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data has occurred, and may include the following:

(i) sending Personal Data (accidentally or deliberately) to internal or external persons who do not have a legitimate need to have access to such Personal Data;
(ii) databases containing Personal Data being compromised, for instance by being illegally accessed by hackers;
(iii) an intruder stealing or accessing a device containing the Company's customer database and misusing it to impersonate the customers;

(iv) loss or theft of computer devices, mobile devices, or paper records containing Personal Data;
(v) paper records containing Personal Data being left unprotected for anyone to see;
(vi) staff accessing or disclosing Personal Data outside the requirements or authorisation of their job;
(vii) being deceived by a third party into improperly releasing the Personal Data of another person; and
(viii) the loss of Personal Data due to unforeseen circumstances such as a fire or flood.

(b) Procedures upon Personal Data Breach

There shall be designed a Personal Data Breach Management Policy for a timely and effective framework to identify privacy-related incidents, an internal escalation communication plan, containment, and recovery of information which has been subject to a security breach, if possible. The procedure shall *inter alia* include:

- Nature of breach;
- Internal Communication;
- Impact of Breach;
- Remedial Action Taken;
- Name and Contact Information of the DPSO;
- Reference to response time of 72 hours, or any plausible justifications for extension of this delay;
- Conclusive action on the incident; and
- Documentation of all incident reports.

3.8.2 BREACH NOTIFICATION

(a) Data Protection Commissioner

Pursuant to the Act, in the case of a Personal Data Breach, Alteo will without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Data Breach to the Commissioner. Where the Company fails to notify the Personal Data Breach to the Commissioner within the 72 hours' time delay, it will provide the Commissioner with the reasons for the delay.

All identified, actual or possible Personal Data Breaches must immediately be reported to the GDPO, including where a service provider who acts as the processor of data of the Company becomes aware of a Personal Data Breach. The GDPO will then make the notification to the Commissioner as referred to above. The notification to the Commissioner will be made using the

prescribed form. The notification will:

(i) describe the nature of the Personal Data Breach, including where possible, the categories and approximate number of Data Subjects and the categories and approximate number of Personal Data records concerned;
(ii) communicate the name and contact details of the GDPO or other contact point where more information may be obtained; and
(iii) recommend measures to address the Personal Data Breach, including, where appropriate, measures to mitigate the possible adverse effects of the breach.

(b) Data Subject

Where a Personal Data breach is likely to result in a high risk to the rights and freedoms of a Data Subject, Alteo will, after the notification to the Commissioner, communicate the Personal Data Breach to the Data Subject without undue delay. The communication to the Data Subject will describe in clear language the nature of the Personal Data breach and set out the information and the recommendations provided for in the preceding paragraph.

The communication of a Personal Data Breach to the Data Subject will not be required where Alteo can show that:

(i) it has implemented appropriate technical and organisational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach, in particular, those that render the Personal Data unintelligible to any person who is not authorised to access it, such as encryption;
(ii) it has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialize; or
(iii) it would involve disproportionate effort. In such a case, there will instead be a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner.

Where Alteo has not already communicated the Personal Data Breach to the Data Subject, the Commissioner may, after having considered the likelihood of the Personal Data Breach resulting in a high risk, require it to do so.

4. OTHER PROVISIONS

4.1 WEBSITES

4.1.1 PRIVACY NOTICES

All Alteo managed websites shall include a Privacy Notice, adapted to reflect its specific operations. Each Privacy Notice shall provide *inter alia* for the rights of Data Subjects and provide the contact details of the GDPO. Furthermore, all Privacy Notices shall be subject to regular reviews, and the updated version shall be cited within the said document.

4.1.2 COOKIES

Cookies are text files placed on computers to collect standard internet log information and visitor behavior information. When a user visits any of Alteo's managed websites, information may automatically be collected through cookies. More information on cookies may be found in Alteo's Cookie Policy.

4.2 CCTV

Certain operational sites of Alteo use CCTV for security purposes. Recognizable images captured by CCTV systems are Personal Data in that they relate to an identified/identifiable individual. Each DPSO shall, if applicable to their Business Unit, comply with Alteo's CCTV Policy, which shall provide *inter-alia* for the following:

- The location of the CCTVs;
- The clear and prominent signs to be placed so that the public is aware that it is entering an area which is covered by CCTV;
- The retention period and backup;
- Security and organizational measures, in respect to access, alteration, disclosure, accidental loss and destruction;
- Access rights and disclosure obligations to Data Subjects; and
- Incident response management.

4.3 USE OF FINGERPRINT

Certain Business Units within Alteo use fingerprint technology to facilitate their payroll process, i.e., in respect of attendance and/or overtime monitoring and/or for access to their premises. All Employees are informed of the purpose for which their fingerprint is collected, and their relative rights. A consent form shall be provided to the Employee, which will provide that should an Employee not wish to provide his/her fingerprint, an alternative option shall be provided to the Employee, e.g., access card.

4.4 IMAGES AND EVENTS

4.4.1 EMPLOYEES

(a) Internal Use

During an Employee's employment, Alteo may process photos of the Employee for administrative, identification and access purposes. Alteo Employees are informed of such internal use upon joining Alteo and are assured that such photos shall not be utilized for any external use, listed below, unless their express consent has been obtained.

(b) External Use

Alteo, from time to time, uses photos and/or videos of its Employees, for *inter alia* the below-named purposes:

(i) Advertisement of Alteo Business operations;
(ii) Employee events;
(iii) Product Launches;
(iv) Golf Events;
(v) Annual Reports; and/or
(vi) Other business communications.

These images may be used in print and digital format including print publications, websites, e-marketing, posters, banners, advertising microfilms, social media etc. Employees' consent must be sought for any of the above requirement and recorded in the Employee's file.

4.4.2 NON-EMPLOYEES

Alteo occasionally organizes or participates in corporate or commercial events, whether for CSR projects, launch of a new product, sport events, or trade shows. Prior to each event, the respective DPSO shall ensure that the Data Subjects are informed that their photos and/or videos or other Personal Data are going to be processed during or after the event. Alteo shall ensure that the Personal Data are processed lawfully, including, but not limited to, ensuring that the below requirements are catered for:

(i) Consent has been obtained from the Data Subject;
(ii) Withdrawal is possible at any time;
(iii) Name of third parties who will have access to the data is disclosed, if applicable.

5. ADMINSTRATIVE PROVISIONS

5.1 POLICY SUMMARY

Document Name	Alteo Group Data Protection Policy
Document responsibility	Group Data Protection Officer
Effective Date	24th June 2022
Approval Level	3
Approval Authority	Board of Directors of Alteo Limited

5.2 DISTRIBUTION LIST

Policy		Tick as Appropriate
Agricultural; Industrial; Property CEOs		✓
Executives		✓
Heads of Department		✓
Employees	Staff	✓
	Workers	✓
	Casuals	✓
Unions		✓
Job Contractors		✓
Service Providers		✓
Clients		✓
Other Stakeholders		✓

5.3 RELATED POLICIES

Policy	Owner
Terms of Reference – Data Protection Committee	GDPO
Employee Data Privacy Notice	GDPO
Privacy Notice_Corporate	GDPO
Privacy Notice_AEL	GDPO
Privacy Notice_ARVL	GDPO
Privacy Notice_Agri/Indus	GDPO
Data Breach Management Policy	GDPO
Information Technology and Security Policy	Head of IT & Innovation
Data Retention and Disposal Policy	GDPO

CCTV Policy	GDPO

5.4 REVIEWS

Version history				
Version	Approved by	Revision date	Description of change	Author
1.0	Board of Alteo Limited	N/a	N/a	N/a

SCHEDULE 1: GLOSSARY OF KEY TERMS

Business Unit shall mean the different clusters of Alteo, being:
- Corporate;
- Property (divided into Property Development and Golf and Anahita Residence and Villas); and
- Agricultural and Industrial.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of eprsonal data relatin to hum or her.

Controller means the natural or legal person 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.

Data Protection Act 2017 means the law which governs the protection of personal data in Mauritius.

Data Protection Commissioner ("**Commissioner**") heads the Data Protection Office.

Data Protection Office means the Mauritian public office under the aegis of the Ministry of Technology, Communication and Innovation. It is led by the Data Protection Commissioner who enjoys wide range of enforcement powers to ensure that the principles of data protection are observed.

Data Subject (Individual) 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.

Employee(s) means any person who is employed by any of the entities of the Alteo Group.

GDPR means General Data Protection Regulations (EU) 2016/79 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data.

Personal Data means 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 to an identifier such as 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.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing means any operation or set of operations performed on personal data or sets of personal data, whether 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.

Processor means a natural or legal person which possesses personal data on behalf of the Controller.

Special Categories of Data in relation to a data subject means personal data pertaining to:

(i) his racial or ethnic origin;
(ii) his political opinion or adherence;
(iii) his religious or philosophical beliefs;
(iv) his membership of a trade union;
(v) his physical or mental health or condition;
(vi) his sexual orientation, practices or preferences;
(vii) his genetic data or biometric data uniquely identifying him;
(viii) the commission or alleged commission of an offence by him;
(ix) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or
(x) such other personal data as the Commissioner may determine to be sensitive personal data.

END OF POLICY DOCUMENT

APPENDIX I

	Company	Date of Incorporation	Business Registration Number
1	Alteo Limited	13/09/2017	C17150285
5	Alteo Properties Ltd	12/09/2002	C06043109
6	Anahita Centre for Excellence Limited	20/10/2006	C06066238
7	Anahita Residences & Villas Limited	15/03/2007	C07069638
8	Anahita Golf Ltd	19/07/2005	C06057532
9	Anahita Estates Limited	19/08/2004	C06052344
10	Domaine de L'Etoile Ltd	20/09/2002	C06043241
11	Alteo Agri Ltd	18/04/1913	C06000012
12	Alteo Refinery Ltd	18/06/2008	C08081346
13	Alteo Milling Ltd	05/12/1995	C07015690
14	Alteo Energy Ltd	20/06/1997	C07018131
15	Alteo New Energy Ltd	16/08/2016	C16140875
16	Alteo Planters Services Ltd	04/03/2011	C11101159
17	Consolidated Energy Co. Ltd	02/08/1996	C06016819
18	Compagnie Usinière de Mon Loisir Ltée	14/12/1995	C07015755
19	Deep River – Beau Champ Milling Company Limited	08/05/1995	C06014643
20	Eastern Energy Company Limited	23/09/1996	C06017036
21	Island Basket Ltd	12/08/2020	C20174121
22	Island Fresh Ltd	09/12/1999	C07023445
23	Refinest Limited	21/01/2009	C09085968
24	Schoenfeld Co. Ltd	18/01/2005	C07054148
25	Usinest Limited	05/04/1995	C06014451