CLIENT PRIVACY NOTICE

Aester Limited (Aester) is a boutique corporate service provider (CSP) licensed with the Bermuda Monetary Authority (BMA) and committed to prioritising our customers' business needs through meticulous attention to detail and bespoke services.

This Privacy Notice is intended to inform individuals, public authorities and organisations who are clients of Aester or may become clients of Aester of how we use personal information (including sensitive personal information).

This Privacy Notice is a live document and will be kept under review and updated, as required, to comply with Bermuda law and any new guidance from the Privacy Commissioner, and/or the Minister responsible for information and communication technologies policy and innovation.

1. ABOUT PIPA

1.1 The Personal Information Protection Act 2016 (PIPA) came into full effect on 1 January 2025. All individuals, private entities and public authorities that use personal information in Bermuda (whether by automated means or as part of a structural filing system) are subject to legislative obligations to protect that information. Part of those obligations involve the provision of a Privacy Notice to individuals before or at the time of the collection of their personal information.

1.2 PIPA requires that organisations use personal information only for the specific purposes provided in their privacy notices or for purposes that are related to those specific purposes unless such use occurs:

(a) with the consent of the individual whose personal information is used;

(b) when necessary to provide a service or product required by an individual;

(c) where required by any rule of law or by the order of the court;

(d) for the purpose of detecting or monitoring fraud or fraudulent misuse of personal information; or

(e) for the purposes of scientific, statistical or historical research subject to the appropriate safeguards for the rights of individuals.

Importantly, PIPA and the rights established for data subjects will not apply so as to:

(a) affect any legal privilege;

(b) limit the information available by law to a party to any legal proceedings; and

(c) limit or affect the use of information that is the subject of trust conditions or undertakings to which a lawyer is subject.

Organisations are expressly permitted to use personal information where it is reasonable to protect or defend the organisation in any legal proceeding.

PIPA further will not apply to:

- **Personal information contained in a court file and used by a judge of any court in Bermuda or used as part of judicial administration or relating to support services provided to the judges of any court in Bermuda, but only where such personal information is necessary for judicial purposes.**
- **Personal information contained in a personal note, communication or draft decision created by or for an individual who is acting in a judicial, quasi-judicial, or adjudicative capacity.**

There are also a number of scenarios involving the use of personal information which will also be excluded from the regulatory scope of PIPA entirely or subject to exemptions.

If a provision of PIPA is inconsistent or in conflict with a provision of another statute, the provision of PIPA will prevail unless PIPA is inconsistent with or in conflict with a provision of the Human Rights Act 1981, in which case, the Human Rights Act 1981 prevails.

2. KEY DEFINITIONS

2.1 The term Client in this Client Privacy Notice refers to any individual, public authority or private organisation that has engaged or potentially may engage Aester's services.

The following definitions are established by PIPA and adopted by Aester in this Privacy Notice:

(a) **business contact information**: an individual's name, position name or title, business telephone number, business address, business e-mail, business fax number and other similar business information. PIPA does not apply to the use of business contact information for the purpose of contacting individuals in their capacity as an employee or official of an organsation.

(b) **KYC** is an abbreviation for the compliance term 'Know Your Client'. Aester, as a CSP, is responsible for combating Money Laundering (**ML**) and Terrorist Financing (**TF**) by identifying risk profiles for potential clients via Customer Due Diligence (**CDD**) processes.

(c) **PEP (i.e. politically exposed person**) is a person who is or has, at any time in the preceding year either:

(i) been entrusted with prominent public functions (e.g. Member of Parliament, Government Minister, Member of higher level of judicial body); or

(ii) a prominent function by an international organisation (e.g. Ambassador); or

(iii) is an immediate family member (includes spouse, partner, children, children's spouse or partner, and parents) of such a person; or

(iv) is a known close associate of such a person (includes business partners and individuals who hold joint ownership in any legal entity as well as partners outside the family unit such as significant others).

(d) **personal information** (**PI**): means any information about an identified or identifiable individual.

(e) **sensitive personal information**: means any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information* or genetic information**.

* **biometric information** means any information relating to the physical, physiological or behavioral characteristics of an individual which allows for their unique identification, such as facial images or fingerprint information.

** **genetic information** means all personal information relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual resulting, in particular, from an analysis of biological sample from the individual in question.

(f) **use** and **using:** in relation to personal information and sensitive personal information, means carrying out any operation on personal information, including collection, obtaining, recording, holding, storing, organising, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or otherwise making available, combining, blocking, erasing or destroying it.

3. PRIVACY OFFICER

Aester has appointed as its Privacy Officer, the Group Privacy Officer generally responsible for attendance to privacy matters on behalf of the BeesMont Group of Companies, of which Aester is an affiliate. The Privacy Officer has primary responsibility for communicating with the Privacy Commissioner and individuals should

they have any questions or concerns about how Aester uses personal information or if they wish to exercise any of the rights of Individuals established by PIPA. Their contact information is provided below:

Group Privacy Officer
privacyofficer@beesmont.bm

4. TYPES OF PERSONAL INFORMATION WE COLLECT:

4.1 *Identity Information*: Aester is required under Bermuda's regulatory regime to obtain PI to perform or consider performing services we have been engaged or requested to provide (Services). This PI includes, but is not limited to, documentation in relation to the identity and address of the ultimate beneficial owners (UBOs), shareholders and directors of the Company (together known as KYC) which may include, but is not limited to: name, passport information with photograph, date of birth, place of birth, citizenship, utility invoice including residential address, bank statement including residential address, driver's licence including photograph, class of licence, and residential address; court cases and convictions, any negative press about the individuals and politically exposed person (PEP) status.

4.2 *Contact Information*: This may include your postal address, email address, home address, and your mobile and home telephone numbers, though Aester will generally use your business contact information.

4.3 *Financial Information*: This may include your source of wealth and source of funding (which may include, but is not limited to, details of your assets, employment history, shareholdings and your beneficial interest in assets, your bank details and your credit history).

4.4 *Information we collect or generate about the Company, its officers, directors, shareholders and beneficial owners*: This includes files including a register of officers and directors, share register, register of members and a minute book(s) with company records to be used by us in the provision of the Services and the consideration of the performance of our general business obligations and requirements.

5. HOW WE COLLECT PERSONAL INFORMATION:

We use the following different methods to collect personal information.

5.1 Collected directly from the Client, such as:

(a) provided by your engagement of our services;

(b) information included in forms and documents;

(c) information gathered through client due diligence, carried out as part of our compliance with regulatory requirements (e.g. passport, driver's licence, marriage certificates); or

(d) by way of correspondence with us by phone, email, letter, social media, or otherwise.

5.2 Collected via disclosure by public source, such as:

(a) public records (e.g. legal notices, published court schedules, Court judgments, warning and decision notices issued by regulators);

(b) searches on the Registrar of Companies portal;

5.3 Collected via disclosure by third-party, such as:

(a) press releases and other media publications such as articles published online;

(b) public listings on stock exchanges and regulatory websites such as the Registrar of Companies;

(c) entities in which you or someone connected to you has an interest;

(d) courts, tribunals;

(e) your legal and/or financial advisors or banking institutions; or

(f) credit reference agencies and financial crime databases for the purposes of complying with our regulatory requirements.

6. HOW AESTER USES THE COMPANY'S PERSONAL INFORMATION

The purposes for which Aester uses Clients' PI can vary depending on the services Aester has been engaged to provide.

Generally, Aester will use personal information for the following purposes:

6.1 *Lawful Entry into Contract*: using PI necessary to take steps at the request of the potential clients with a view to entering into contract such as:

(a) client due diligence and verification of identity;

(b) performance of conflict checks;

(c) attendance to initial meetings/calls; and

(d) negotiation of and entry into engagement terms with clients and file opening.

6.2 *Performance of Contract*: using PI necessary to perform the contract with the Company. Sometimes this involves Aester using the services of third-party organisations located in Bermuda and/or overseas. Pursuant to PIPA, the Administrator will remain responsible for ensuring compliance with privacy regulations with regard to third-party vendors.

6.3 *Exercising Legal Rights and Meeting Legal Obligations*: using PI pursuant to a law which authorises or requires such use. We have set out some practical examples below:

(a) To meet regulatory thresholds for compliance and due diligence;

(b) To administer requests, enquiries, or complaints received from clients or a party in connection with a client pursuant to the legal right such as afforded by PIPA; and

(c) To adhere to legislation regulating the work of a corporate service provider.

6.4 Consent: using PI based on the consent of the Client, for example "opting-in" to receive marketing materials or to receive event invitations.

7. IN SELECT SITUATIONS, WE MAY ALSO USE PI FOR THE FOLLOWING PURPOSES:

7.1 **Supervisory Adherence**: using PI to comply with an order made by a court, individual or a body having jurisdiction over us.

7.2 **Disclosures to/from Public Authorities**: using PI collected from, or disclosed to, a public or regulatory authority which is authorised or required by a statutory provision to provide the PI to or collect it from us. Practical examples include:

(a) Disclosing PI as part of making an application to a regulator for the incorporation of a company or acquiring a specific licence to do business in Bermuda.

(b) Making disclosures under the Proceeds of Crime Act 1997.

7.3 **Appropriate Use of Public PI**: using publicly available information for the purpose that is consistent with the purpose of its public availability. For example, PI collected from LexisNexis and Google searches in the course of completing our due diligence while onboarding the Company and/or individual.

7.4 **Emergency**: Using PI as necessary to respond to an emergency that threatens the life, health or security of an individual or the public.

7.5 **Debt Collection** using PI as necessary in order to collect a debt owed to our organisation or for our organisation to repay any money owed to the individual.

7.6 **Protection or Defence of the Organisation**: using PI as a reasonable means to protect or defend our organisation in any legal proceeding.

8. HOW AESTER SHARES THE COMPANY'S PI:

8.1 We may disclose Client PI with our staff however the extent of their use is contractually limited to the performance of their duties, the terms of our engagement agreements and adherence to Bermuda law.

All staff are required to adhere to our cybersecurity and privacy standards and regulated by our contractual protections in place to protect PI and confidential information. All staff (students, employees, part-time workers, consultants and other persons who are engaged by Aester in an ad hoc administrative capacity, interns, as well as agency workers who provide services to Aester on behalf of a third-party organisation) are required to execute confidentiality agreements to preserve confidentiality and the privacy of Clients.

8.2 We may further share Client PI with:

(a) our consultants and service providers (such as C-Suite roles staff contracted on service contracts, financial institutions with whom Aester or the client transact, outsourced compliance partners, information technology providers and, when necessary, with other affiliated members of BeesMont Group);

(b) other entities we have a reliance agreement with for the purposes of Anti-Money Laundering and Anti-Terrorist Funding compliance. In such cases we will include you in the communication;

(c) our own advisors, such as auditors, accountants, and any external legal advisors which we may instruct from time to time; and.

(d) regulators who hold jurisdiction over us such as the Bermuda Monetary Authority, the Financial Intelligence Agency, the Bermuda Police Service or the Registrar of Companies.

9. INTERNATIONAL TRANSFERS OF COMPANY PI:

9.1 We have controls in place to maintain the security of our information and information systems.

9.2 Appropriate controls (such as restricted access) are in place on our computer systems.

9.3 The Administrator seeks to protect the PI in its custody or control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal. Confidentiality and security are not assured when information is transmitted through email or other wireless communication. The Administrator will not be responsible for any loss or damage suffered as a result of a breach of security and/or confidentiality when information is transmitted by email or wireless communication. We will take your use of a particular mode of communication as permission for us to communicate with you using the same method of communication unless otherwise instructed by you. Where requested, we will transmit confidential documents via secure file sharing.

9.4 As a condition of employment, the Administrator's employees are required to follow all applicable laws and regulations, including in relation to data protection law. Unauthorised use or disclosure of confidential client information by an employee is prohibited and may result in disciplinary measures.

9.5 Your PI may be transferred to or accessed from countries that may not have data protection laws equivalent to those of Bermuda or your country.

9.6 Unless we have your consent to transfer your PI, the transfer is necessary for the performance of the contract, for the establishment, exercise or defence of legal claims, or is otherwise permitted by applicable data protection and privacy laws, we will only transfer your PI to a country considered by us to have comparable levels of data protection and privacy laws. If such a country does not have equivalent privacy laws, the Administrator will seek to ensure it has the appropriate safeguards in place such as binding corporate policies and procedures, standard contractual data protection clauses approved by

applicable supervisory authorities, an approved employee code of conduct, and/or an approved certification mechanism.

10. YOUR RIGHTS UNDER PIPA:

PIPA fully came into force in Bermuda on 1 January 2025. Under PIPA you have the general right of access to the PI which we hold about you as set forth below.

10.1 You have the right to request and we generally will be required to provide:

(a) personal information about yourself which is in our custody or under our control;

(b) the purposes for which your personal information has been and is being used by us; and

(c) the names of the persons or types of persons to whom and circumstances in which your personal information has been and is being disclosed.

We may refuse to provide access to your personal information if:

(a) the personal information is protected by any legal privilege;

(b) the disclosure of the personal information would reveal confidential information of the organisation or of a third party that is of a commercial nature and is not unreasonable to withhold the information;

(c) the personal information is being used for a current disciplinary or criminal investigation or legal proceedings, and refusal does not prejudice the right of the individual to receive a fair hearing;

(d) the personal information was used by a mediator or arbitrator, or was created in the conduct of a mediation or arbitration for which the mediator or arbitrator was appointed to act under an agreement or by a court;

(e) the disclosure of the personal information would reveal the intentions of the organisation in relation to any negotiations with the individual to the extent that the provision of access would be likely to prejudice the negotiations; or

(f) If such disclosure would be likely to prejudice the physical or mental health of that person and the request of an individual involves access to personal information of a medical or psychiatric nature relating to themselves or personal information kept for the purposes of, or obtained in the course of, the carrying out of social work in relation to themselves. In such a case, an organisation must, if requested to do so by the individual, provide access to such personal information to a health professional who has expertise in relation to the subject matter of the record, and the health professional shall determine whether disclosure of the personal information to the individual would be likely to prejudice the physical or mental health of that individual.

Aester must refuse to provide access to requested personal information where:

(a) the disclosure of the personal information could reasonably be expected to threaten the life or security of an individual;

(b) the personal information would reveal personal information about another individual; or

(c) the personal information would reveal the identity of an individual who has in confidence provided an opinion about another individual and the individual providing the opinion does not consent to disclosure of his identity,

Unless it is reasonable in all the circumstances to provide access.

In some circumstances, we may redact certain information, and, in such cases, we are required to provide you with access to the remainder of the personal information after such redaction has occurred.

Redact or **redaction**: the process of removing or blanking out certain information in a record before disclosure to a data subject.

10.2 The right to request the rectification of your personal information

If you believe that personal information concerning you which is under our control has an error or omission, you will be able to make a written request for a correction to the same.

If there is an error or omission in personal information that your correction request has identified, we will be required to correct your personal information as soon as reasonably practicable and where we have disclosed the incorrect information to other organisations, we will be required to send a notification containing the corrected information to each organisation to which the incorrect information has been disclosed, if it is reasonable to do so.

Aester must obtain the consent of the writer of an opinion, including a professional or expert opinion, before making a correction to or otherwise altering such opinion. If consent is not provided, the organisation must still note what is contained in the written request to change any error or omission in the opinion in a manner that links that request with that opinion.

10.3 The right to request that we erase your personal information.

10.4 You have the right to request Aester to erase or destroy your personal information where that personal information is no longer relevant for the purposes of its use. The right to erasure is also known as the 'right to be forgotten'.

Upon receiving such a request, Aester is required to erase or destroy the personal information that you have identified in your request or provide you with written reasons as to why the use of such personal information is justified.

10.5 The right to request the cessation of the use of your personal information.

You will have the right to request us to cease, or not to begin, using your personal information:

(a) for the purposes of advertising, marketing, or public relations; and

(b) where the use of that personal information is causing or is likely to cause substantial damage or substantial distress to yourself or another individual.

On receiving a request described in subsection (a) above, we will be required to cease or not begin using your personal information for the purposes of advertising, marketing, or public relations. On receiving a request described in subsection (b) above, we will be required to either cease, or not begin, using the personal information that you have identified in your request, or provide you with written reasons as to why the use of such personal information is justified.

11. CHANGES TO OUR PRIVACY NOTICE

We reserve the right to, at our discretion, change, modify, add to, or remove portions from, our Privacy Notice. We will of course notify you of any changes where we are required to do so.

Should you have any general questions pertaining to the development of privacy law in Bermuda, please contact the Bermuda Privacy Regulator:

The Office of the Privacy Commissioner for Bermuda

Maxwell Roberts Building
4th Floor
1 Church Street
Hamilton HM11
Bermuda Telephone: +1 441 543 7748
Email: PrivCom@privacy.bm