Operative Date: 1 January 2025

CLIENT PRIVACY NOTICE

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

This Client 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, the Minister responsible for information and communication technologies policy and innovation and/or Bermuda Bar Council.

1. ABOUT US

BeesMont Law is a leading boutique Bermuda corporate/commercial law firm. We are registered with Barristers & Accountants AML/ATF Board pursuant to Section 30B of the Proceeds of Crime (Anti-Money Laundering and Anti-terrorist Financing Supervision and Enforcement) Act 2008 and are regulated by the Bermuda Bar Council. Our offices are located at 73 Front Street (3rd Floor) in Hamilton, Bermuda.

2. ABOUT PIPA

The Personal Information Protection Act 2016 (**PIPA**) is due to come fully in force in Bermuda on 1 January 2025. Once the legislation comes fully into effect, all individuals, private entities and public authorities that use personal information in Bermuda (whether by automated means or as part of a structured filing system) will be subject to new 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.

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:

- with the consent of the individual whose personal information is used;
- when necessary to provide a service or product required by an individual;
- where required by any rule of law or by the order of the court;
- for the purpose of detecting or monitoring fraud or fraudulent misuse of personal information; or
- 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:

- **affect any legal privilege;**
- **limit the information available by law to a party to any legal proceedings; and**

- **limit or affect the use of information that is the subject of trust conditions or undertakings to which a lawyer is subject.**

Organisations will be 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; and**
- **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 number of other 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 in the Human Rights Act 1981, in which case, the Human Rights Act 1981 prevails.

3. KEY DEFINITIONS

When we use the term "**Client**" in this Client Privacy Notice, it is referring to any individual, public authority or private organisation that has engaged or potentially may engage our legal services.

PIPA establishes the following new statutory definitions which are adopted by BeesMont Law and are referred to in this Privacy Notice:

- **personal information**: means any information about an identified or identifiable individual.
- **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 behavioural 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 a biological sample from the individual in question.

- **use** or **using**: in relation to personal information and sensitive personal information, means carrying out any operation on personal information, including collecting, obtaining, recording, holding, storing, organising, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or

otherwise making available, combining, blocking, erasing or destroying it.

- **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 organisation.

Other terms which you may not be familiar with that are commonly used in law firm practice are:

conflict check is a standard process conducted by law firms in order to determine whether the firm or any of its lawyers has ever represented a party or parties with an interest which is adverse to that of the potential client.

Hansard is the traditional name of the transcripts of parliamentary debates in Bermuda. Often, these debates provide insight into the interpretation of legislation and policy position of the Bermuda Government and therefore is used as a reference by attorneys in managing advisory practice.

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

Officers of the Court all barristers and attorneys who are enrolled and called to the Roll of the Court are entitled to practice as a barrister or attorney in Bermuda. Such persons are deemed to be an Officers of the Court.

PEP (i.e. politically exposed person) is a person who is or has, at any time in the preceding year either been entrusted with prominent public functions (e.g. Member of Parliament, Government Minister, Member of higher level judicial body) or a prominent function by an international organisation (e.g. Ambassador), has an immediate family member (includes spouse, partner, children, parents) of such a person or is a known close associate of such a person (includes business partners and joint ownership in legal entity).

4. OUR PRIVACY OFFICER

We have appointed a Group Privacy Officer generally responsible for attendance to privacy matters on behalf of the BeesMont Group of Companies. The Group Privacy Officer has primary responsibility for communicating with the Privacy Commissioner and individuals should they have any questions or concerns about how we use 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

5. WHAT CLIENT PERSONAL INFORMATION WE COLLECT

We regularly collect and use different kinds of client personal information, such as:

- **Identity Information**: personal identification information which may include your name, passport, driving licence or other photographic identity details, utility invoice, driver's licence with photograph, and personal information relating to claims, court cases and convictions, PEP status information.

- **Contact Information**: This may include your postal address, email, home address and your mobile and home telephone numbers.
- **Financial Information**: sources of wealth and your assets (which may include details of your assets, sources of wealth, shareholdings and your beneficial interest in assets, your bank details and your credit history).
- **Advisory Matter Information:** personal information pertaining to the advisory matter that we have been engaged to advise upon and/or provide representation in respect of, which may include sensitive personal information such as photos and/or recordings. In certain types of advisory matters, it is more common for law firms to use greater amounts of sensitive personal information in order to assist advise and represent a client's interests.

  For example, advice concerning employment, immigration, human rights and constitutional protections, personal injury typically uses greater amounts of sensitive personal information. In particular, it is possible we may also use the personal information and sensitive personal information of the family members of a Client as may be relevant to the legal service to be provided. For example, a person granted a work permit by the Department of Immigration to be gainfully employed in Bermuda may have sponsored dependents and advice sought on changing employers could involve advising on the legal positioning of those family members in addition to the client themselves.

  Certain types of advice to private organisations, such as regarding corporate mergers and acquisitions, may also use greater amounts of personal information and sensitive personal information. For example, information about the current and former staff and employees of the relevant organisations, claims history, disciplinary history, vendor management history, client records and relationship management, recruitment and HR activities are often considered.
- **COVID-19 Health Information:** personal information relevant for COVID-19 contact tracing.

6. HOW DO WE COLLECT CLIENT PERSONAL INFORMATION

We use different methods to collect Client Personal Information, such as:

- Collection directly from the Client, such as that personal information which is:
  - included in forms and documents; or
  - gathered through client due diligence, carried out as part of our compliance with regulatory requirements (e.g. passport, drivers licence, marriage certificates); or
  - by way of correspondence with us by phone, e-mail, letter or otherwise.
- Collection via disclosure by public source, such as:
  - public records (e.g. legal notices, Hansard, published court schedules, Court judgments, warning and decision notices issued by regulators);
  - press releases and other media publications; or
  - Registrar of Companies search.

- Collection via disclosure by a third party:
    - entities in which you or someone connected to you has an interest; or
    - courts, tribunals, independent offices (such as the Office of the Human Rights Commission, Information Commissioner's Office and the Office of the Privacy Commissioner) and quasi-judicial bodies (such as Labour Relations, Ombudsman and the Department of Workforce Development); or
    - your legal and/or financial advisors; or
    - your financial institutions; or
    - credit reference agencies and financial crime databases for the purposes of complying with our regulatory requirements.

7. HOW WE USE CLIENT PERSONAL INFORMATION

The purposes for which we use Client personal information can vary depending on the legal services that we have been engaged to provide.

Generally, we use personal information for the following purposes :

- **Lawful Entry into Contract**: using personal information necessary to take steps at the request of potential clients with a view to entering into a contract such as:
    - performance of conflict checks;
    - performance of KYC collection, inclusive of identification of PEP status;
    - attendance to initial meetings/calls);
    - negotiation of and entry into engagement terms with client and file opening; and
    - any subsequent conflict checks in connection with any new advisory matters;
- **Performance of Contract**: using personal information necessary to perform the contract we have with a Client for the provision of legal services.
- **Exercising Legal Rights and Meeting Legal Obligations**: using personal information pursuant to a law which authorises or requires such use. We have set out some practical examples below:
    - to meet regulatory thresholds for compliance, and due diligence;
    - to adhere legislation regulating Court procedure and the conduct of Officers of the Court;
    - for administration of requests, enquiries or complaints received from clients or a party connection to a client pursuant to a legal right such the up-coming new right to rectify Personal Information in PIPA
    - to adhere to supervision of Bermuda Bar Council and the Bar Professional Conduct Committee:
- **Consent:** using personal information based on the consent of a Client, for example Clients "opting in" to receive marketing materials or legal updates on an area of law or to send you event invitations.

In select situations, we may also use personal information for the following purposes connected to the legal service:

- **Supervisory Adherence**: using Personal Information to comply with an order made by a court, individual or a body having jurisdiction over us.
- **Disclosures to/from Public Authorities**: using Personal Information collected from, or is disclosed to, a public authority which is authorised or required by a statutory provision to provide the personal information to, or collect it from us. Practical examples include:
    - disclosing Personal Information as part of making an application to regulator for the incorporation of a company or acquiring a specific licence to do business in Bermuda;
    - disclosing Personal Information and Sensitive Personal Information to the Department of Immigration as part of an immigration application or appealing an immigration-related decision;
    - making disclosures under the Proceeds of Crime 1997.
- **Appropriate Use of Public Personal Information:** using publicly available for a purpose that is consistent with the purpose of its public availability. We have set out some practical examples below:
    - using personal information from public Court judgments, court schedules and information obtained from the Registry of the Supreme Court to advance legal argument and advice;
    - using personal information from Hansard, reports and decisions issued by public authorities to advance legal argument and advice.
- **Emergency:** using personal information necessary to respond to an emergency that threatens the life, health or security of an individual or the public.
- **Debt Collection:** using Personal Information as necessary in order to collect a debt owed to our organisation or for our organisation to repay to the individual money owed.
- **Protection or Defence of Organisation**: using Personal Information as reasonable to protect or defend our organisation in any legal proceeding.

8. DISCLOSURE OF CLIENT PERSONAL INFORMATION

We may disclose Client personal information 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.

As we are a hybrid law firm, we employ and engage attorneys who advise Bermuda-based Clients from both Bermuda and overseas. They are required to adhere to our cybersecurity and privacy standards and are regulated by our contractual protections in place to protect personal information and confidential information. All staff (students, employees, consultants) are required to executed confidentiality agreements to preserve confidentiality and the privacy of Clients.

We may further share Client personal information with our consultants and service providers (such as C-Suite roles and attorneys contracted on service contracts, information technology providers, event hosting service providers, or our own advisors, auditors and accountants and financial institutions with whom we or

you transact) in connection with the provision of services, outsourcing, regulatory adherence or client relationship development. These organisations and individuals are also contractually required to keep Client information confidential and are not permitted to use it for any purposes other than for the proper provision of their duties / services and in accordance with Bermuda law.

We may also share the personal information of clients (as well as the representatives of clients) in the form of the obtaining and collecting of photos at our corporate hosting events and the publication of the same as part of our wider digital branding.

Depending on the nature of the advisory matter and/or the Bermuda law regulating us or the Client, we may also disclose personal information to:

- Parties to transactions or litigation (including law firms acting for other parties);
- Court Registries, their staff and members of the judiciary in the context of litigation;
- Other professional service providers such as organisations providing background information services;
- Regulators;
- Law enforcement agencies;
- Governmental institutions; and/or
- Tribunals.

9. RIGHT OF CLIENTS UNDER PIPA

Once fully in force, PIPA will provide individuals with a number of statutory rights in relation to their personal information which is held by organisations. These rights are subject to a number of statutory exemptions and the request process is also subject to a statutory timeframe.

The remainder of this section provides a general overview of these data subject rights:

(A) The general right of access to personal information

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

- personal information about yourself which is our custody or under our control;
- the purposes for which your personal information has been and is being used by us; and
- 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:

- the personal information is protected by any legal privilege;

- 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 it is not unreasonable to withhold that information;

- 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;

- 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;

- 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 those negotiations.

- 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.

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

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

- the personal information would reveal personal information about another individual; or

- 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 be able to **redact** certain information, and, in such cases, we are require 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.

(B) 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.

An organisation 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.

(C) The right to request the erasure or destruction of your personal information

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

Once PIPA is fully in force, on receiving such a request we will be 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.

(D) 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 to another individual.

On receiving a request described in sub-section (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 sub-section (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.

10. CHANGES TO OUR PRIVACY NOTICE

We reserve the right, at our discretion, to 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