STAFF PRIVACY NOTICE

This Staff[1] Privacy Notice informs individuals who are Staff of BeesMont Law Limited (**BeesMont**) or may become Staff of BeesMont of how the firm uses staff personal information (including sensitive personal information).

This Staff 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 US

BeesMont Law Limited 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 regulated by the Bermuda Bar Council.

2. ABOUT PIPA

The Personal Information Protection Act 2016 (**PIPA**) came fully in force in Bermuda on 1 January 2025. As of that time, 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) became 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.

PIPA requires that organisations use personal information only for the specific purposes provided for 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 do 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

[1] Staff in this context includes all employees, part-time workers, consultants and other persons who are engaged by the law firm in an ad hoc administrative capacity or as students, pupils, interns etc as well as agency workers who provide services to the law firm on behalf of a third party organisation.

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 or 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 a number of other scenarios involving the use of personal information which are 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

PIPA establishes the following new statutory definitions which are followed by BeesMont 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, staff member or official of an organisation.

- **publicly available information** is personal information about an individual which either:

  (a) the individual knowingly makes or permits to be made available to the public;

  (b) which is legally obtained or accessed from government records that are available to the public; or

  (c) which is legally obtained or accessed from information required by law to be made available to the public.

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 BeesMont in order to determine whether the firm or any of its lawyers has ever represented an individual or a group of parties with an interest which is adverse to that of the candidate for employment/ engagement/appointment as a member of Staff.

Due Diligence BeesMont, as a regulated entity, is responsible for combating Money Laundering (**ML**) and Terrorist Financing (**TF**) by identifying risk arising from the employment and engagement of individuals and further have a duty to our clients to ensure that our staff are fit and adequately skilled to execute and discharge their duties. BeesMont undertakes vetting exercises (**Due Diligence**) as part of its activities to meet these obligations.

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 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), is 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 individuals who hold joint ownership in a legal entity).**staff**: means the individuals working for BeesMont in the capacity of employees, contract workers, consultants, part-time workers, and other persons who are engaged by the law firm in an ad hoc administrative capacity or as students, pupils, or interns.

Relevant employee as defined in Regulation 18(2) of the Proceeds of Crime (AML/ATF) Regulations 2008 as an employee who at any time in the course of his duties has or may have access to any information which may be relevant to determining whether any person is engaged in money laundering or terrorist financing. For the purposes of Regulation 18, “relevant employee” includes an individual working on a temporary basis whether under a contract of employment, contract for services or otherwise.

4. OUR PRIVACY OFFICER

Our Privacy Officer has primary responsibility for communicating with the Privacy Commissioner and for liaising with members of staff or the public if they have any questions or concerns on how we use personal information. Our Privacy Officer may be contacted via privacyofficer@beesmont.bm.

5. WHAT STAFF PERSONAL INFORMATION WE COLLECT

We regularly use different kinds of staff personal information, such as:

- **Standard Identity Information**, which may include:
  - name; and
  - date of birth.
- **Due Diligence Information**, such as:
  - a copy of a government-issued driving licence, such licences can contain personal information and sensitive personal information such as first name, surname, date of birth, license number, signature, registered address, medical donor status, sex and biometric information (facial photograph) of the cardholder;
  - a copy of a utility invoice or bank statement can contain personal information such as first name, surname, account number, service address, meter number, and bank information of the account holder;
  - a copy of a passport information page, such passport information page can contain personal information and sensitive personal information such as first name, surname, passport number, nationality, date of birth, sex, place of birth, issuing authority, registration as a Bermudian and the facial photograph of the passport holder;
  - the results of background checks and formal police records reports, such results and reporting can contain personal information and sensitive personal information by providing details pertaining to claims, court cases and convictions; and
  - PEP status information, such as personal information and sensitive personal information evidencing the type of PEP and corresponding risk level assigned to BeesMont engaging with individuals who are a PEP or are otherwise linked to a PEP.
- **Contact Information**, such as:
  - preferred email address;
  - residential address;
  - emergency contact name (first name and surname) and telephone number; and
  - mobile and home telephone numbers.
- **Professional Headshot:**
  - biometric information (facial photograph).
- **Social Events:**
  - On occasion, if you attend events (whether in an official or social capacity or during staff team-building or holiday events) BeesMont may obtain photos of you directly or from a third party (such as a client, industry association or another member of the firm). BeesMont will obtain your consent prior to publishing your biometric information on any publicly available platform.

- **Human Resources Information**:
  - banking institution;
  - bank account number;
  - social insurance number;
  - payroll tax information;
  - university and professional designation documentation
  - reference letters;
  - curriculum vitae / resume;
  - vacation day requests;
  - contractual terms of appointment / employment / engagement,
  - medical practitioner's notes regarding fit for work status, ,
  - compensation information,
  - information on pension forms such as:
  - information about offspring and/or spouse,
  - next of kin,
  - information on health insurance forms,
  - leave requests per Employment Act 2000, and
  - concerns, complaint and grievance information.

6. HOW DO WE COLLECT STAFF PERSONAL INFORMATION

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

- Collection directly from the current /prospective Staff member, such as that:
  - provided via your voluntary engagement with our corporate LinkedIn account for the BeesMont Group of Companies; or
  - included in general or on-boarding forms such as pension forms, health insurance forms and related documents; or
  - gathered through Due Diligence carried out as part of our compliance with regulatory requirements and verification of information provided in a CV/resume; or
  - by way of correspondence with us by phone, e-mail, letter or otherwise.
- Collection via disclosure by public source, including publicly available information, such as:
  - public records (e.g. legal notices, Court judgments, warning and decision notices issued by regulators); or

- press releases and other media publications;
- search results from public as well as legal and compliance-focused search engines and platforms, such as Lexis Nexis, Google, and financial crime databases.

- Collection via disclosure by a third party:
  - entities in which you or someone connected to you has an interest;
  - 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);
  - Government departments (such as Department of Social Insurance or the Office of the Tax Commissioner);
  - your financial institutions; or
  - enforcement agencies, such as the Bermuda Police Service.

7. HOW WE USE STAFF PERSONAL INFORMATION

The purposes for which we use Staff personal information can vary.

Generally, we use personal information for the following purposes:

- **Contractual Relationship**: using personal information necessary (1) to take steps at the request of potential staff with a view to entering into a contract (2) for the performance of a contract to which the individual is a party and (3) the use of the personal information is necessary in the context of an individual's present, past or potential employment relationship with the organisation., such as:
  - performance of conflict checks and other forms of Due Diligence;
  - verification of previous career experience, educational qualifications and professional designations;
  - attendance to initial meetings/calls;
  - negotiation of and entry into contractual terms;
  - provision of compensation
  - enrolment on health insurance and pension plans; and
  - deductions from compensation for health insurance, pensions, and statutory payroll tax and social insurance.
- **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:
  - enrolment on health insurance and pension plans; and
  - deductions from compensation for statutory payroll tax and social insurance.

- facilitation of Practising Certificates and other regulatory documentation for attorneys of BeesMont;
- to adhere to health and safety regulations;
- for administration of requests, enquiries or complaints received from Staff pursuant to a legal right such as the right to rectify personal information in PIPA.
- to adhere to supervision of Bermuda Bar Council, the Bar Professional Conduct Committee and Barristers & Accountants AML/ATF Board.

- **Adherence to Policies & Procedures in alignment with legislation**
- **Consent:** using personal information based on the consent of a Staff member, for example the use of images of Staff in photos used by BeesMont for marketing.

In select situations, we may also use personal information for the following purposes:

- **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 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 to the Bermuda Monetary Authority when adding an employee as an officer of the Company; or
  - making disclosures under the Proceeds of Crime Act 1997.
- **Workplace Investigation**: Where a security breach incident occurs, BeesMont has the ability to request our third-party security vendor to produce a report verifying which key cards were used to access the premises at the time of the breach. The security vendor does not hold personal information about Staff, but upon receipt of the report, BeesMont could potentially identify the Staff member that has been assigned the key card(s) in question. This information may then be shared with regulatory authorities and enforcement agencies. It should be noted that it is not the regular practice of BeesMont to request a security report to be generally issued by our third party vendor and BeesMont would only do so in these certain or similar circumstances.
- **Appropriate Use of Publicly Available Information:** using publicly available information for a purpose that is consistent with the purpose of its public availability.
- **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 by an individual 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.
- **Marketing Materials:** BeesMont may publish photographs of Staffon our website and / or the social media account of the BeesMont Group of Companies after you have provided your consent

for the respective purpose.

8. HOW WE SHARE STAFF PERSONAL INFORMATION

We may share Staff personal information with:

- Other members of staff;
- Third-party service providers such as:
    - insurance providers;
    - pension providers; or
    - compliance partners.
    - social media platforms such as:
    - LinkedIn;
    - Facebook; or
    - Beta Technologies (the third party vendor responsible for BeesMont's website design, IT and infrastructure)
    - MidSea (the third party vendor responsible for BeesMont's Due Diligence)
    - Oxygen (the third party vendor responsible for BeesMont's telephone systems)
    - BeFunky (third party software used for online photo editing).

We may also share Staff personal information with HR support from time to time, our own advisers, such as auditors and accountants, and any external legal advisors which we may instruct from time to time.

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

- Regulators;
- Law enforcement agencies;
- Governmental departments and institutions; and/or
- Tribunals

9. RIGHTS OF STAFF UNDER PIPA

PIPA provides 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. This aspect of our Privacy Notice provides a general overview of these rights:

The right of access to personal information

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

- personal information about yourself which is in 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.

The right to access medical records

We would highlight that PIPA provides organisations with the ability to refuse to provide access to personal information if:

- 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; and
- if such disclosure would be likely to prejudice the physical or mental health of that person.

In such cases, 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 may refuse to provide access to your personal information where:

- The personal information is protected by 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.

We will not provide access to 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.

If we are reasonably able to redact the confidential information of the organisation or of a third party that is of a commercial nature; or the personal information which would reveal personal information about another individual; or the personal information that would reveal the identity of an individual who has in confidence provided an opinion about another individual; or information which would be likely to prejudice the physical or mental health of the individual from the personal information about the individual who requested it, we shall then provide the requester with the access to their personal information after redacting the former information.

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 should 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.

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

You 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'.

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.

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

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

- for the purposes of advertising, marketing, or public relations; and
- 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 to cease using your personal information for the purposes of advertising, marketing or public relations, we will cease, or not begin using your personal information for such purposes.
- On receiving a request to cease using your personal information where the use of it is causing or

is likely to cause substantial damage or substantial distress to yourself or to another individual, we will 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.

Effective 2 April 2025