

# Privacy Policy of Bourbon Vanilla Ltd

## Introduction

Bourbon Vanilla Ltd (hereinafter referred to as “The Company,” “we,” or “us”) is committed to protecting the privacy of our employees, clients, suppliers, and all data subjects we interact with. We comply with the obligations set forth under applicable data protection laws, including the Data Protection Act 2017, regarding the collection, use, processing, and retention of personal and special categories data.

This Privacy Policy outlines how we collect, use, store, and retain your data, as well as the principles that guide these processes. It applies to all data held by the Company, regardless of the form, media, or manner in which it was acquired or retained.

## Scope

This policy applies to all employees, agents, affiliates, consultants, and third-party service providers who may handle or have access to personal or sensitive data on behalf of Bourbon Vanilla Ltd.

All individuals involved in data processing or handling within the Group are responsible for familiarizing themselves with this policy and ensuring its strict compliance.

## Personal Data we collect

Personal data means any information relating to a data subject, as such term is defined under the Data Protection Act 2017. Personal data includes, but is not restricted to:

- Personal contact details (name, address, contact number, email address)
- Gender and date of birth
- Medical information
- Morality Certificate
- Employment information such as social security, passport or visa number or the identification of information required to confirm eligibility for employment by a government entity.
- Curriculum Vitae

- Signature
- Citizenship
- Photographs
- Video and audio recordings
- Biometrics information (fingerprint images)

Personal data such as medical information, morality certificate or biometrics pertain to special categories of data according to the requirements under the Data Protection Act 2017 and as such are subject to enhanced security measures as required by the applicable law.

## Use of Personal Data

We may use your personal information in the ways outlined below, as well as in any additional ways that advance our legitimate interests or are required or permitted under applicable law:

- Performance of a contract
- Reporting to management
- Recruiting and employment
- Tenders award procedures
- Due diligence procedures
- To deliver services to you
- To reply to your requests
- Data analysis
- To personalize your experience (Your information helps us respond better to your individual needs)
- Website- to know your preferences
- Contacting you with information about our products and services
- Sending you important notices

## Retention of Personal Data

The Company retains data for as long as required to effectively conduct our operations and comply with legal requirements. The retention periods are outlined in the **Data Retention Schedule** in Annex A. After the retention period, personal data is securely deleted or anonymized.

## Data Duplication

The Company seeks to minimize data duplication, but in certain cases, it may be necessary to retain duplicate records for business or operational reasons. This policy applies to all data, including duplicates.

## Data Sharing Within the Taylor Smith Group

By engaging with any companies within the Group, you acknowledge and agree that your personal data may be shared among companies within the Taylor Smith Group for purposes such as administrative efficiency, customer support, and service delivery.

All Group entities adhere to this Privacy Policy to ensure consistent privacy and data protection standards.

## Disclosure of Personal Data

We may disclose your Personal Information to the extent permitted by applicable law or with your consent:

- When it is required by law
- To comply with the law (Judicial proceedings, court order, law enforcement, exercise our legal rights, defend against legal claim, request from public and governmental authorities)
- When there is an investigation or in prevention, against illegal activities
- When there is a suspected fraud
- When there is a potential threat to safety of any person
- For the purposes set out in this Privacy Policy, to our affiliates.

- For promotional purposes
- To our third-party service providers to provide service on our behalf, facilitate our service or perform related services
- To all Companies in the Taylor Smith Group

## Third Party

The privacy practices and data protection policies of third parties are not covered by this Policy and cannot be controlled. Please read and refer to the third party's privacy and data retention policy when you submit personal information to such a third party. In circumstances, we disclose your personal data to third parties for the purposes described in this policy, they are bound by contractual obligation not to disclose or use the information for any other purpose.

If you choose to provide personal information of a third party (such as name, email and telephone number) to the Company, you represent and warrant that you have permission from the third party to do so (e.g. Marketing material or Job referrals).

## Your Rights

The Company is committed to complying with regulations with respect to your rights. It is your responsibility as a data subject to ensure that the information you give us is kept up to date and is accurate. The Company takes all reasonable steps to discard or update any inaccurate data without delay.

You have certain rights in respect to how we use your personal data. These are:

- You have the right to request a copy of the personal information we have about you as far as practical; unreasonable request, or information that is difficult or time consuming to retrieve, may be subjected to charges.
- to ensure that your personal data that we have is up-to-date, accurate and complete. However, it is your responsibility to submit correct and updated data to the Company and our responsibility is to update the data as provided by you.

- to have your personal data erased if the personal data collected, for the purposes for which it was collected, is no longer necessary, unless we are required by law to retain it. Where this right is exercised on our Office 365 solutions, such data will be deleted on live systems and a "Right to be forgotten" tag will be marked to the backed-up file in question. The file will be beyond use and deleted when its 10 years cycle in the backup system has lapsed.
- to withdraw your consent whenever the Company processes your personal data based on your consent, subject to applicable laws.
- to object to the processing of your personal data and if you think that your data protection rights are being breached you have the right to contact the applicable supervisory authority to register a complaint.

Please contact us at [dpo@taylorsmith.mu](mailto:dpo@taylorsmith.mu) if you wish to exercise any of the above rights.

## Protecting your Personal Data

The security of your personal data is important for us. We use appropriate methods to protect your personal data. The Company is compliant with the basic privacy and security principles such as access control to different categories of personal data, clear screen policy, clean desk policy, and lockable document storage cabinets. Wherever practical, we ensure that data is encrypted during transit and storage and that access to this data is strictly limited to a minimum number of individuals and subject to confidentiality obligations.

We also train our employees on privacy and security protection to raise awareness of personal data protection and to ensure the security of your personal data. Our personnel having access to your personal data are bound by a non-disclosure agreement with the Company.

The Company only retains your personal data for a reasonable period and until the purpose for which the data was collected is achieved, including for the purpose of satisfying any legal, accounting, or reporting requirements. It is our policy to destroy personal information once we are no longer required to retain it by law or business.

In certain circumstances, we may anonymize your personal data (so that it is no longer associated with you) for research or statistical purposes.

## Children's Personal Data

The Company is sensitive with regards to children's personal data, which is considered sensitive data. Children's personal data is collected with prior consent from their parents or guardians, for purposes outlined in that consent, for example, to be published in our newsletter or on our website or otherwise displayed within the organization. The Company is involved in activities including TS foundation, Welfare, CSR program and Company events, where Children's personal data may be collected. The Company will be using or disclosing the data only as permitted by law, with the clear consent of the parents or guardians of the child or as required for the child's protection. If we accidentally collect personal data of a child without verified prior permission from the parent or guardian, we will endeavor to delete the data at the earliest practicable opportunity.

## Transfer of information outside Mauritius

Your personal data we collect may be processed or accessed outside Mauritius where the Company or its affiliates, service providers or business partners are situated. In this case, we take appropriate safeguards to ensure that the personal data is treated securely in accordance with this policy and applicable laws. We use encryption where appropriate. The Company uses a wide range of legal procedures, such as standard contractual clauses with those parties to ensure data is processed in a secure manner.

## ANNEX A - Data Retention Schedule

The information listed in the retention schedule below is intended as a guideline and may not contain all the records the Group may be required to keep in the future.

<b>A. ACCOUNTING AND FINANCE</b>	
Record Type	Retention Period
Annual Plan and Budgets	5 Years
Financial Activities (Accounts Payable Ledgers, Accounts Receivable Ledgers and Interim Financial Statements)	7 Years

<b>B. CONTRACTS</b>	
Record Type	Retention Period
Contracts and Related Correspondence Including emails (including any proposal that resulted in the contract and all other supportive documentation)	10 Years after expiration or project completion
Electronic records of progress sets	10 Years after expiration or project completion
Client Data (KYC, Due Diligence, Profile, Invoices)	10 Years after expiration or project completion

<b>C. EMPLOYEE RECORD</b>	
Record Type	Retention Period
Recruitment records for candidates	2 years
Employee Personal File/Management/Payroll	10 Years after termination of employment contract
Pension Details	60 Years
Health and Safety training records	30 Years

**D. CORRESPONDENCE**

Most correspondence (external and internal) should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a particular contract would be retained as long as the contract (10 years after project completion). It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project file.

**E. ELECTRONIC MAILS/DOCUMENTS**

Electronic mail will not be kept for more than 7 years unless the said mail contains documents and/or data for which a longer retention period is provided by this Policy. In such case, the electronic mail should be labeled as ‘never delete’ or ‘10 years’.

All employees are required to properly sort and label the retention period of their specific document/file/folder depending on the subject matter.

The backup retention period is 10 years for both electronic mail and documents.

<b>F. LEGAL FILES AND PAPERS</b>	
<b>Record Type</b>	<b>Retention Period</b>
Legal Memoranda and Opinions (including all subject matter files)	10 years after close of matter
Litigation Files	10 years after expiration of appeals or time for filing appeals

Retention periods in the present Data Retention Schedule may be extended under exceptional circumstances where:

- **Ongoing Investigations:** When investigations by relevant authorities are ongoing and the personal data in question may be required to demonstrate compliance with legal or regulatory demands.
- **Legal Proceedings:** When personal data is necessary for the exercise or defense of legal rights in current or anticipated legal proceedings, disputes or other form of resolution processes.

## Contact us

If there are any questions regarding this Privacy Policy, do not hesitate to contact us on [dpo@taylorsmith.mu](mailto:dpo@taylorsmith.mu) or if you have any complaints or concerns about privacy and want to contact the Data Protection Officer (DPO) of the Company.

## Review

This Policy is subject to change at the sole discretion of Taylor Smith Group. Updates may be made from time to time without prior notice.

## Proprietary Rights

This policy is the property of Taylor Smith Group and may not be reproduced, distributed, or used without prior written permission.

Policy	Reference	Version	Revision	Last updated
Privacy Policy	DPO/2024/01	Version 2	Revision 1	February 2025

*The most recent policy will be updated on this page.*