



British American Tobacco Kenya plc

Data Protection Policy

1. INTRODUCTION

Article 31 of the Constitution of Kenya dictates that every person has a right to privacy. To further give effect to this Article, the Data Protection Act 2019 (“the Act”) was passed in November 2019 to govern the collection and processing of personal data. Responsible, purposeful, secure, transparent and time-bound processing of data subject’s personal data is fundamental for the protection of the individual’s rights.

At British American Tobacco Kenya plc (“BAT” or “the Company”), we have a responsibility to ensure that we use personal data in accordance with the law.

2. PURPOSE AND SCOPE OF THIS POLICY

This Policy is intended to provide minimum standards with respect to the protection of personal data that we collect, process and store and will cover the use of personal data about all individuals, including consumers, employees, customers and other third parties, that deal with BAT and its affiliated companies.

Importantly, the Policy ensures that British American Tobacco Kenya plc:

- Complies with local and, to the extent applicable, international laws and regulations on data protection.
- Protects the rights of its employees, consumers, customers and business partners.
- Fosters transparency in how it collects, processes and stores people’s data.
- Safeguards itself from the risks of data breaches.

The terms used in this Policy are explained in detail in Appendix 1.

Every member of BAT has a duty to maintain the confidentiality and trust of the data subjects that share their personal data with the Company. Compliance with the Policy is mandatory and any breach of this Policy and related policies and procedures may result in disciplinary action.

The Data Protection Officer is responsible for overseeing the implementation and review of this Policy and can be contacted through Data_Protection@bat.com.

3. DATA PROTECTION PRINCIPLES

I. Right to privacy

BAT shall endeavor to protect the privacy of the data subject, by anonymising where possible and in consistency with the purpose for which the data is being processed, to hide the identity of the data subject.

II. Lawfulness and Fairness

Collection of personal data shall be for a lawful reason for which BAT shall explain the specific purpose to the data subject. Before processing of data, the lawful basis relied upon shall be documented.

Processing of personal data will be lawful if at least one of the following conditions are met:

- a. The data subject has given their consent for one or more specific purposes.
- b. Processing is necessary for the performance of a contract to which the data subject is a party to.
- c. To comply with a legal obligation as prescribed by statute.
- d. Where processing is necessary for public interest.
- e. Processing is necessary for BAT to pursue a legitimate interest without prejudicing the rights and dignity of the data subject.

III. Legitimate purpose

BAT shall ensure that the data collected is used for legitimate purposes and shall seek to minimise any privacy impact to the data subject.

IV. Purpose limitation

Processing and control of data shall be limited to the purpose for which it was collected. Data shall only be collected for a specified, explicit and legitimate purpose. The data collected shall be adequate, relevant, and limited to what is necessary for processing. Employees and agents of BAT shall not process data for a new purpose that is not compatible with the original purpose. Where a new purpose is required, BAT shall first notify and obtain a fresh consent of the data subject.

V. Data minimisation

A member or agent of BAT will ensure that they collect only personal data that is required for the legitimate purpose of collection.

VI. Storage limitation

To the extent possible, all efforts shall be made to ensure that personal data is not stored in a way that identifies the data subject.

Further, BAT shall ensure that personal data is not stored for longer than is necessary in respect of the purpose for which it was collected (except where there is a legal, audit or tax obligation that requires holding of the records).

BAT employees appreciate that longer storage period beyond the retention period may lead to data breaches and increase storage costs. Employees and agents of BAT shall be required to regularly review the personal data they process to ascertain whether or not they are due for destruction.

A member or agent of BAT will ensure that personal data is destroyed, deleted or anonymised where such data is no longer needed for the performance of their duties and or has been held for longer than the applicable retention period, which periods shall be reviewed and updated by the Company from time to time.

Compliance with the Records Management Policy and retention periods shall be observed at all times when dealing with personal data.

VII. Data security

Personal data shall be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification, or disclosure of data.

VIII. Data migration

BAT being part of a group of companies, is likely to share data with its affiliate companies. By dealing with BAT, you agree for BAT to share your data with such of its affiliates outside Kenya for storage, processing and or control. BAT shall ensure that the entity and country of transfer has in place laws or measures that ensure an individual's data is protected against loss, breach etc.

4. RIGHTS OF THE DATA SUBJECT

BAT shall respect the rights of the data subject under the Act, which include:

- a. **Right to be informed:** on the reason for collection of their personal data including the purpose for which and how their personal data will be processed.
- b. **Right of access:** the right to receive a copy of the personal data BAT holds including an understanding of how the data has been processed.

- c. **Right to withdraw consent:** where the lawful basis relied upon to collect personal data is the data subject's consent, the data subject reserves the right to withdraw such consent at any time without reason. Withdrawal of consent shall not impact the information processed when consent was still in effect.
- d. **Right to rectification:** the right to have inaccurate personal data corrected.
- e. **Right to erasure (right to be forgotten):** the right to ask BAT to delete or destroy the data subject's personal data where: consent has been withdrawn (where applicable); data is no longer required for BAT to perform its tasks; the holding of the personal data is not in the best interest of the data subject; objection to processing.
- f. **Right to restrict processing:** the right to restrict processing where there is reason to believe that: the personal data is inaccurate; the processing was unlawful, and the data subject prefers restriction of processing over erasure; BAT legitimate interests for processing doesn't override those of the data subject.
- g. **Right to data transfer:** to the extent permissible, the right to receive or ask BAT to transfer to a third party, a copy of the data subject's personal data in a structured, commonly used machine-readable format.
- h. **Right to object to direct marketing:** the right to request that we do not process the data subject's personal data for direct marketing purposes.
- i. **Right to be notified of a personal data breach:** the right to be notified of a personal data breach which is likely to result in a high risk to the data subject's rights, freedoms or dignity.
- j. **Right to complain:** the right to lodge a complaint to the Data Commissioner.

5. COMPLIANCE WITH AUDIT

The Board may conduct periodic audits to ensure compliance with this Policy. All employees shall cooperate with such audits and any outcomes, including remediation plans.

6. INTERPRETATION

In circumstances in which the terms of this Policy differ from newly enacted laws, regulations or standards governing the Company, the law, regulation or standard will take precedence over these policies and procedures until these policies and procedures are amended to conform to the law, regulation or standard.

7. RELATED DOCUMENTS

- 7.1 Records Management Policy
- 7.2 Standards of Business Conduct

8. REVIEW

This policy shall be reviewed every two years by the Audit Committee who shall recommend any proposed changes to the Board for approval.

9. POLICY APPROVAL

This Policy was approved by the Board on 3rd December 2021.

APPENDIX

Definition of terms

Consent	means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject
Data subject	means an identified or identifiable natural person who is the subject of personal data
Data controller	means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.
Data processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller
Sensitise data or sensitive personal data	means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject
Personal data	means any information relating to an identified or identifiable natural person
Processing	means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as: a) collection, recording, organisation, structuring; b) storage, adaptation or alteration; c) retrieval, consultation or use; d) disclosure by transmission, dissemination, or otherwise making e) available; or f) (e) alignment or combination, restriction, erasure or destruction.