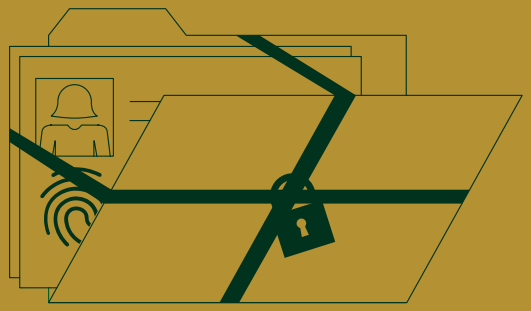

RECORDS MANAGEMENT & PERSONAL DATA PROTECTION POLICY

INTRODUCTION AND PURPOSE

This policy covers both records management and personal data protection. A key part of running a highly successful, professional and attractive company is knowing how and where to store and keep business relevant documents, contracts and data. Carlsberg India Private Limited ("CIPL"/"Company") together with any subsidiary of CIPL from time to time ("CIPL Group") is therefore committed to establishing and maintaining records management practices, and to collecting and storing personal data, in a way that meets our business needs as well as the legal requirements deriving from relevant laws and regulations.

Records generally contain such business relevant information as is needed for Carlsberg to be able to run its business and to comply with relevant laws and regulations and can be in all formats or media, including documents, photos and e-mails. See also "Records" in the Glossary below.

The CIPL Group collects personal data about people and business partners with whom it deals in order to carry out our business and related services. No matter how personal data is collected, recorded, used or processed (e.g. on a computer or on paper), we must always ensure compliance with applicable personal data protection regulations in order to retain the trust of those people and business partners.

The purpose of this policy is to establish a framework for effective records management and compliant personal data processing in order to mitigate legal and business risks and optimize the way we do business.

Detailed guidance on practical implementation, roles and responsibilities, and compliance with this policy will be provided in specific Records Management and Personal Data Protection Manuals. The principles shall be integrated in relevant local procedures.

SCOPE

This policy applies to the management, employees and contract workers of all entities in the CIPL Group.

REQUIREMENTS

All managers and employees are responsible for ensuring immediate escalation to CIPL Legal and the relevant functional responsible manager, as set out in the "Roles and Responsibilities" section below, of all actual or potential personal data and records management risks that could have a material impact on the CIPL Group.

1. RECORDS MANAGEMENT

The creation and management of records is an integral part of the CIPL Group's activities, processes and systems. The business efficiency of the Group depends on the accessibility and protection of our records. Records must therefore be managed and controlled in accordance with the principles set out below.

1.1. Regardless of formats or media, records must be stored in a way that ensures that the CIPL Group can manage and control its records in a safe and efficient way. In order to ensure this, records must be:

- Managed in accordance with applicable legal requirements and business needs. Records Retention Plans must be developed throughout the Group.
- Retrievable when required at any time during the retention period.
- Protected from unauthorized access, changes, loss and destruction.
- Not kept in separate individual filing systems.
- Made available in digital form wherever possible.
- Properly classified, indexed and controlled:
    - Records that are classified as confidential must be protected with additional security controls.
    - All records must be named/labelled appropriately in order to ensure easy retrieval.
    - Additions to and comments on records must be traceable and, if made in a finalised record, version control and an audit trail must be available.

1.2. All CIPL Group IT and physical systems that contain, manage and provide access to records must have an owner and meet the following minimum standards:

- Back-up routines, continuity and recovery plans must be established and documented.
- Migration and preservation activities/strategies must be undertaken without loss of data in order to ensure the accessibility and usability of records throughout the storage period.
- Systems must be routinely monitored and evaluated in order to identify any risks to the accessibility or integrity of records.

1.3. The disposal of records must be carried out in a systematic and authorized way in accordance with approved retention periods and must be documented.

1.4. In addition to the above requirements, vital records must be protected and regularly monitored and controlled according to their value, and relevant recovery/emergency procedures for effective use must be established.

2. PERSONAL DATA PROTECTION

When collecting or processing any type of personal data, the CIPL Group must respect the privacy of its employees, contractors, vendors, suppliers and consumers, and of other third parties with which we do business. Personal data includes, but is not limited to name: address,
e-mail address, date of birth, private and confidential information, as well as sensitive personal information.

The CIPL Group fully endorses the following six principles for handling personal data:

2.1. **Lawfulness:** The processing of personal data must only be permitted if the data subject has given prior consent or if it is allowed under applicable
law at the place of processing (see definition of processing in glossary). Consent must be given in writing or by other legally allowed means in the relevant country.

2.2. **Purpose:** Personal data must only be collected for specified, explicit and legitimate purposes, and must not be further processed contrary to such intended purposes.

2.3. **Data limitation:** Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

2.4. **Accuracy:** Personal data must be accurate and, where necessary, kept updated. Appropriate and reasonable steps must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed are erased or rectified without delay.

2.5. **Storage restriction:** Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed.

2.6. **Security:** Personal data must be processed in a manner that ensures appropriate security using suitable technical and/or organizational means. Personal data must be protected against unauthorized or unlawful processing, accidental loss, destruction or damage.

ROLES AND RESPONSIBILITIES

Body/function/individuals	Roles and responsibilities
CIPL Board of Directors (BoDs)	Responsible for policy approval.
CIPL Legal	Policy owner with overall responsibility to CIPL BoDs for records management and personal data protection issues and for ensuring that material records management and personal data protection risks in the CIPL Group are duly attended to and communicated to CIPL BoDs / Audit Committee, as relevant.
CIPL IT Manager	Functionally responsible for developing, implementing and maintaining the Personal Data Protection Compliance Programme. This includes ensuring that associated documents and the compliance programme are kept up to date as well as monitoring and addressing identified risks.
CIPL Managing Director and CIPL heads of functions / Local Management	Responsible for ensuring that this policy is implemented and adhered to, and that all relevant employees are made aware of the policy and its requirements. To the extent this policy requires notification and/or escalation to a representative of the Carlsberg Group, outside of the CIPL Group, a representative nominated by CSAPL (Singapore) Holdings Pte. Ltd. shall be copied in such notification and/or escalation.
CIPL IT Manager	Responsible for ensuring that relevant IT systems are compliant with this policy.
CIPL Legal	Responsible for supporting local implementation and operation of this policy and the associated Personal Data Protection Compliance Programme. This includes ensuring that relevant local legislation is implemented in regard to personal data protection and local records retention plans and procedures, if retention periods are different from the corporate retention plan
CIPL IT Manager	Functionally responsible for supporting implementation of the policy by providing guidance, training, monitoring and control. Performs assessments of records management practices under the policy (i) on demand, (ii) based on audit findings or (iii) based on risk evaluations.
CIPL Legal	Responsible for taking over the ownership of all records deemed to be historically significant at the end of the retention period in accordance with the historical archives procedures.
Management, employees and contract workers of all entities in the CIPL Group	Responsible for adhering to this policy.

GLOSSARY

Data subject
The person to whom the personal data relates.

Personal data
Any information relating to an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly. Identifying information includes both directly and indirectly identifying information, such as name, photo, identification number, location data, online identifier and bank account number.

Processing
Any operation or set of operations performed on personal data by any method. Any use of personal data, both electronically and manual, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Records
Records contain such business relevant information as is needed for CIPL to be able to run its business and to comply with relevant laws and regulations, including information created, received and maintained by the CIPL Group as evidence or as an asset in pursuit of legal rights and obligations or in the transaction of business. Records can be in all formats or media, including documents, e-mails, photos, videos, social media and physical objects.

Records Retention Plan
A list of approved records, systems, retention periods, classification and record owners.

Vital records
Records that are irreplaceable if lost or destroyed, and (i) if lost, would have severe consequences for the CIPL Group in terms of loss of money, reputation or heritage or (ii) are essential to the continued operation of the Group.

DEVIATIONS

No exemptions from this policy can be granted unless there are exceptional circumstances or the policy is obviously not applicable. All requests for exemptions must be made in writing to the policy owner. The policy owner must assess and decide on each request individually in alignment with the CIPL Managing Director. Exemptions must be duly logged and documented.

POLICY REVISION

This policy must be reviewed and approved at least every two years. It may be amended at any time with the approval of CIPL BoDs. In the event of any discrepancies between the English version of this policy and a translated version, the English version will be binding.

ASSOCIATED POLICIES AND MANUALS

- Records Management Manual
- Personal Data Protection Manual

CONTACT

For more information, please contact the Policy Owner.

GOVERNING LAWS

This Policy shall be subject to applicable Indian Law(s).

ENGLISH

June 2018

Carlsberg India Private Limited
Regd. Office : 04th Floor, Rectangle No.1, Commercial Complex D4, Saket, New Delhi-110017, India
Corporate Office : 3rd Floor, Tower-A, Paras Twin Towers, Sector-54, Gurugram, Haryana-122002, India