



DATA PROTECTION & PRIVACY

GLOBAL POLICY



CONTEXT

This policy outlines the framework for compliance with applicable data protection laws and regulations, ensuring that Carlsberg operates with integrity and in accordance with legal requirements.

In the EU and UK, regulations like the General Data Protection Regulation (GDPR), UK GDPR and national privacy laws set clear rules on how personal data must be handled. In Canada, we follow the Personal Information Protection and Electronic Documents Act (PIPEDA), while in APAC, our businesses adhere to laws such as China's Personal Information Protection Law (PIPL) and Vietnam's Decree on Personal Data Protection.

As privacy laws evolve and expectations for transparency and control grow, we uphold a consistent, high standard of data protection across all Carlsberg entities. This policy defines Carlsberg's global principles for data protection and privacy, ensuring compliance while strengthening the trust of our employees, customers, and partners.

OUR COMMITMENT

We at Carlsberg have always strived for better – better brews, pioneering innovation, respecting our planet and championing ethical business. This policy commits Carlsberg to conducting business ethically and with the utmost integrity in all its operations worldwide.

We believe that responsible data handling isn't just about compliance—it's good business and part of Carlsberg's long-standing commitment to integrity and trust. For generations, we have built our reputation through quality, innovation, and responsible business practices. As we continue our digital transformation, we uphold strong data protection and privacy principles to drive long-term growth, responsible innovation, and respect for our employees, customers, and partners. We do not tolerate misuse, negligence, or unfair data practices—because protecting personal data means protecting the trust that has defined us for generations.

WHO DOES THIS APPLY TO?

This policy applies to everyone at Carlsberg, including managers, employees, and contract workers for:

1. All entities in the Carlsberg Group.
2. Joint venture entities where Carlsberg is a majority shareholder.



THE CORE PRINCIPLES OF THIS POLICY


We follow key global privacy principles like lawfulness, fairness, transparency, purpose limitation, and accountability, to ensure personal data is handled responsibly. This means we only collect and use data for legitimate purposes, keep it to a minimum, and put safeguards in place to protect it from misuse or unauthorised access. Failing to uphold these principles can lead to fines, legal actions against our business, and reputational damage, weakening trust in Carlsberg. Beyond business, misuse of personal data can harm individuals, exposing them to identity theft, fraud, and distress. Following privacy principles is paramount to protect our business and the people who trust us.

REQUIREMENTS

At Carlsberg, we want to handle personal data responsibly and in line with our global privacy principles and the Code of Ethics and Conduct. We expect everyone to follow these requirements in their daily work.


1. LAWFULNESS & PURPOSE LIMITATION

- 1.1.** We always have a business or legal reason to collect personal data and never gather it “just in case”.
- 1.2.** We expect you to use personal data only for a legitimate business purpose and never to use it beyond its original intent.
- 1.3.** We expect you to ensure that you always have the legal right to use someone’s data, whether through their consent or another basis under the local law.

 **Your Action:**
Be extra careful when using sensitive data such as health, religion, social security numbers. Do not collect it without consultation with your Data Protection Responsible.


2. TRANSPARENCY & FAIRNESS

- 2.1.** We want to be open and honest about how we use personal data.
- 2.2.** We ensure people know what data we collect, why we collect it, and how it will be used by providing clear privacy notices on our websites.
- 2.3.** We expect you to use data in ways that are fair and aligned with individual expectations and our privacy notices.

 **Your Action:**
Familiarise yourself with the privacy notices in your market and ensure that your use of personal data aligns with them.


3. DATA MINIMISATION & ACCURACY

- 3.1.** We keep personal data collection to the minimum necessary.
- 3.2.** We expect you to collect only what is needed for the task at hand and ensure the information remains accurate and relevant.

 **Your Action:**
Collect only the data you truly need. If you request personal data, be prepared to justify why each piece of information is required.


4. RETENTION & DELETION

- 4.1.** We want to ensure that personal data is not kept longer than necessary.
- 4.2.** We expect you to delete or anonymise personal data when it is no longer needed, in line with Carlsberg’s data retention policies.

 **Your Action:**
If your team stores personal data records, schedule regular reviews to remove outdated data instead of keeping it indefinitely.

5. RESPECT FOR INDIVIDUAL RIGHTS

- 5.1.** We respect people’s rights to their personal data provided under local laws.
- 5.2.** We expect you to help ensure data requests — such as accessing, correcting, or deleting their personal data—are handled promptly and in line with legal requirements.

 **Your Action:**
If someone contacts you about their privacy rights, inform the Data Protection Responsible right away so their request can be handled correctly.

REQUIREMENTS (CONT)

6. DATA SECURITY

- 6.1.** We want to protect personal data from unauthorised access, loss, or misuse.
- 6.2.** We expect you to follow security measures, such as using strong passwords, restricting access to shared folders, locking screens and reporting any potential data breaches immediately.



Your Action:

When working on projects involving personal data, ensure that access to project files is restricted on a need-to-know basis and only granted to those who must have it.

7. ACCOUNTABILITY

- 7.1.** We expect you to be aware of privacy requirements in your workplace and to complete all mandatory privacy trainings.
- 7.2.** Whether you are procuring vendor services or launching a new website, you are responsible for initiating necessary privacy assessments and maintaining the evidence of data protection compliance.



Your Action:

When initiating a new project involving the use of personal data, reach out to your Data Protection Responsible for compliance consultation and be ready to explain and document the intended data processing.



HOW TO REPORT A BREACH

REPORTING DATA BREACHES

We expect you to immediately report any real or suspected data breaches to the IIT and your Data Protection Responsible.

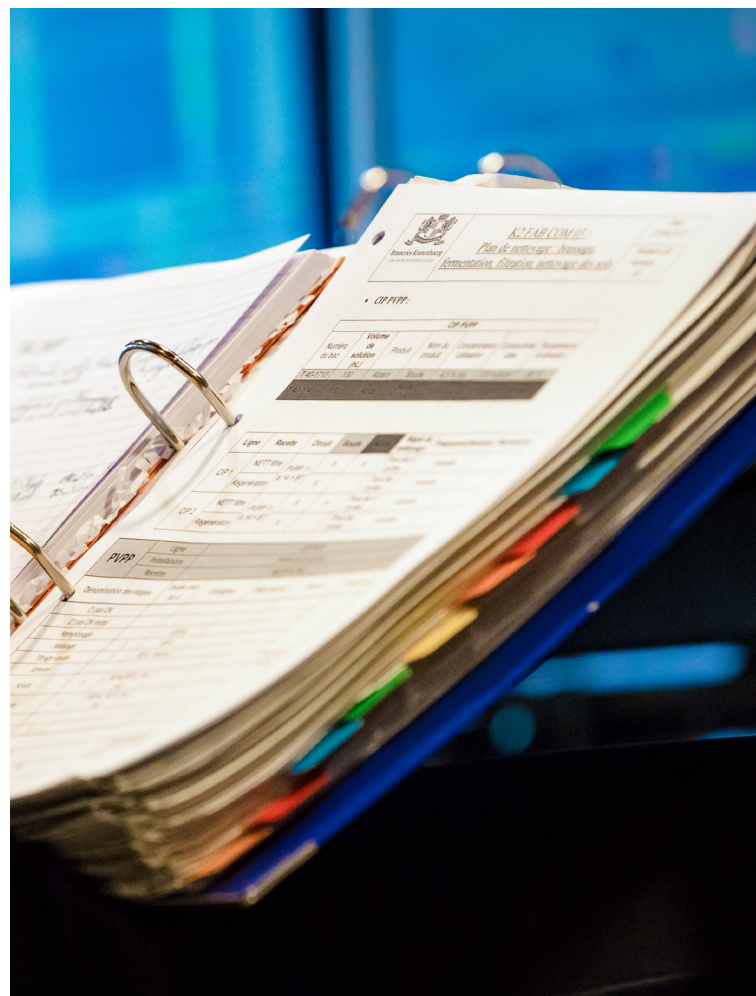
REPORTING POLICY VIOLATIONS

We expect you to ask questions, seek guidance and report any suspected violations regarding compliance with this policy to your manager, your local Data Protection Responsible or the Head of Legal.

ANONYMOUS REPORTING

Alternatively, our Speak Up whistleblowing phone line and web reporting tool can be accessed anonymously by employees, by those in our value chain and the communities in which we operate. Where matters are brought to us, we are committed to protecting the rights of those reporting them. We do not tolerate any reprisal against anyone who raises a matter in good faith or has assisted in an investigation.

[The Speak Up Manual](#) contains more information about how cases are investigated.



DEFINITIONS & KEY TERMS

Carlsberg

In this policy, "Carlsberg" refers to any business unit, subsidiary, or joint venture within the Carlsberg Group where Carlsberg holds a majority shareholding or exercises management control.

Data Breach

A data breach is any incident where the security of personal data has been compromised or is likely to be compromised, or there is an unauthorised or accidental disclosure of or access to personal data. Examples include loss of an unencrypted laptop containing sensitive health records of Carlsberg employees, a malicious insider altering customer personal data and financial records or a ransomware that encrypts employee personal records.

Individual

The individual that can be identified by the personal data, or to whom the personal data relates. For example employees, contractors, consumers, and contact persons at our customers, business partners, vendors, suppliers or other third parties.

Personal Data

Any information or a combination of information that can identify or relates to an individual. For example names, contact details, photos, videos and voice recordings, identification number, private and confidential information, location data, online identifiers, bank account number and other financial information, work-related information, consumer/customer patterns, habits and profiles, user accounts, as well as information about health and criminal records. Personal data can be in all formats or media, including documents, emails, photos, videos, social media and physical objects. Data collected via online tracking technologies such as cookies and tracking pixels is also considered personal data in many markets where Carlsberg operates.

Use of Personal Data

Any handling of personal data, both electronically and manually, such as collection, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, processing, disclosing by transmitting, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

ROLES & RESPONSIBILITIES

ROLES / NAME	RESPONSIBILITIES
ExCom Policy Sponsor – Group CFO	<ul style="list-style-type: none"> The Global Policy Sponsor is a senior leader who provides strategic oversight, ensures resources are allocated, and champions the policy at the executive level. Approves and provides oversight over all exceptions and variations.
Global Policy Owner – Group General Counsel and CCO	<ul style="list-style-type: none"> Global Policy Owner is accountable for the overall lifecycle of a policy, ensuring alignment with the organisation's strategy, compliance requirements, and operational needs. Approves and provides oversight over all exceptions and variations.
Policy Subject Matter Expert – Head of Data Protection	<ul style="list-style-type: none"> The Policy SME provides in-depth expertise on the policy's subject matter, supporting its development, implementation, and ongoing maintenance. Defines and delivers an annual risk-based policy activity plan and training toolkit. Responsible for monitoring adherence and providing guidance on exceptions.
Group IIT Privacy Operations & IIT Digital Marketing	<ul style="list-style-type: none"> Supports Policy SME in developing and implementing processes to operationalise policy requirements and manages digital privacy solutions. Embeds personal data retention and deletion, and privacy by design controls into global IT systems and websites.
Corporate, Regional and Local IIT Function	<ul style="list-style-type: none"> Ensures that IT systems and processes owned by the IIT Function are compliant with this policy. Defines and implements cyber security and data security controls across Carlsberg.
Managing Directors, Functional heads at CCO/Region	<ul style="list-style-type: none"> Ensures implementation of the policy locally or in their function, adapting it to local requirements whilst maintaining alignment. Accountable for the appointment of Data Protection Responsible. They set the "tone from the top" by promoting a culture of integrity.
Head of Legal	<ul style="list-style-type: none"> Accountable for compliance with the policy and local data protection laws. Responsible for providing legal advice, regulatory horizon scanning and implementing necessary actions in response to changes in local data protection laws. Ensures appointment of a competent Data Protection Responsible and provides support and oversight.
Data Protection Responsible (DPR)	<ul style="list-style-type: none"> Ensures compliance within their function or market by implementing global processes operationalising policy requirements, and developing local processes to comply with the local data protection requirements. Provides day-to-day data protection advice to Carlsberg employees, completes necessary privacy assessments and reviews, and maintain compliance records in line with the accountability principle.
All business units, managers, employees and contractors working for and behalf of Carlsberg	<ul style="list-style-type: none"> Responsible for understanding and complying with the policy in their day-to-day work. Responsible for cooperating with the DPR by participating in data mappings, privacy assessments and responding to follow-up questions in a timely manner to ensure compliance with the accountability obligation. Informed about policy updates and trained on how to comply effectively. In doubt, always contact their local DPR or Head of Legal who shall, if needed, verify with the Head of Data Protection.

HOW WE MONITOR

We monitor adherence to this policy through a structured internal controls assessment programme, conducted in partnership with our internal controls team.

As part of our risk management approach, risks are mapped and self-assessed annually to identify potential areas for improvement. Additionally, a prioritised internal audit programme, along with targeted deep dives and spot checks, provides independent assurance of compliance. Ensuring compliance with global privacy principles is a shared responsibility, and failure to adhere to this policy may result in disciplinary action.

EXCEPTIONS & DEVIATIONS

LOCAL POLICY DEVIATIONS

In addition to this policy, all Carlsberg Group entities must comply with any applicable local data protection laws that may impose additional or stricter requirements. Where such requirements apply, local entities may introduce supplementary policies (policy extensions) to ensure compliance. Local policies must be provided for review to the Policy Subject Matter Expert.

OTHER EXCEPTIONS

Other than the above, exceptions to this policy shall not be granted, unless exceptional conditions exist, or the policy is not applicable. Any request for an exception shall be put in writing to the Global Policy Owner. The Global Policy Owner shall assess and decide on each request individually. Exceptions shall be duly logged and documented.

POLICY REVISION

This policy must be revised annually as a minimum. It may be amended as needed with the approval of the relevant ExCom Policy Sponsor. In the event of any discrepancies between the English version of this Policy and a translated version, the English version is binding.





ASSOCIATED STANDARDS & MANUALS

- [Data Privacy & Data Protection Manual](#)
- [Data Ethics Policy](#)
- [Information Security & Acceptable Use Policy](#)

SUPPORTING TOOLS & RESOURCES

- [Data Protection for Business Hub](#)
- [Data Protection for DPRs Hub](#)
- [DPR Network Hub](#)
- [Global Privacy Notice for Carlsberg Employees](#)
- [Global Privacy Notice for Customers, Partners & Visitors](#)

CONTACT

For more information, please reach out to the Head of Data Protection or your local [Data Protection Responsible](#).

Version: 1

Effective Date: 1 May 2025

Next Review Date: 1 May 2026

Policy Owner: Ulrik Andersen, Group General Counsel and CCO

Approved By: Ulrica Fearn, Group CFO

Carlsberg Breweries A/S

J.C. Jacobsens Gade 1

1799 Copenhagen V

Denmark

