|  |
| --- |
|  |
|  |
| Personal Data Protection Manual |

Contents

[Introduction 4](#_Toc531870184)

[Scope 4](#_Toc531870185)

[Governance Structure 4](#_Toc531870186)

[**1.** The Data Protection organization at Group level 4](#_Toc531870187)

[**1.1. Local Data Protection Organization** 5](#_Toc531870188)

[1.1.1. Management 5](#_Toc531870189)

[1.1.2. Local Data Protection organization in the EU/EEA markets 5](#_Toc531870190)

[1.1.3. Local Data Protection Organization outside the EU/EEA markets 5](#_Toc531870191)

[Processing of personal data 6](#_Toc531870192)

[**2.** What is personal data? 6](#_Toc531870193)

[**3.** The Concept of “processing” 6](#_Toc531870194)

[Principles for processing personal data 6](#_Toc531870195)

[**4.** The overall key principles 6](#_Toc531870196)

[**5.** Data subject rights 7](#_Toc531870197)

[**6.** Transfer of data and the use of processors 7](#_Toc531870198)

[**7.** incidents and breaches 7](#_Toc531870199)

[**8.** Training 8](#_Toc531870200)

[**9.** More information 8](#_Toc531870201)

[Roles and responsibilities 9](#_Toc531870202)

[Monitoring and control 11](#_Toc531870203)

[Glossary 11](#_Toc531870204)

[Deviations 11](#_Toc531870205)

[Associated policies, manuals and other 11](#_Toc531870206)

[Contact 11](#_Toc531870207)

[Manual revision history 11](#_Toc531870208)

[Appendix 1 12](#_Toc531870209)

[Introduction 12](#_Toc531870213)

[The scope and structure 12](#_Toc531870214)

[Personal data and processing 13](#_Toc531870215)

[**1.** Personal Data according to GDPR 13](#_Toc531870216)

[**1.1. What is personal data?** 13](#_Toc531870217)

[**1.2. What is “processing” of personal data?** 13](#_Toc531870218)

[Data Protection organization 15](#_Toc531870219)

[The Carlsberg GDPR Compliance framework 15](#_Toc531870220)

[What is the Carlsberg GDPR compliance framework? 15](#_Toc531870221)

[**1.** The Carlsberg GDPR House 16](#_Toc531870222)

[**2.** The Overall Key Principles for Processing Personal Data 16](#_Toc531870223)

[**2.1.** **Lawfulness, Fairness and Transparency** 17](#_Toc531870224)

[**2.2. Purpose limitation** 18](#_Toc531870225)

[**2.3. Data minimization** 18](#_Toc531870226)

[**2.4. Accuracy** 19](#_Toc531870227)

[**2.5. Storage limitation (Retention)** 19](#_Toc531870228)

[**2.6. Integrity, confidentiality and security** 19](#_Toc531870229)

[**2.7. Accountability** 19](#_Toc531870230)

[**3.** Data subject rights 20](#_Toc531870231)

[**4.** Working with third parties 21](#_Toc531870232)

[**5.** Transfer requirements 21](#_Toc531870233)

[**6.** Data breach 22](#_Toc531870234)

[**7.** Contact 22](#_Toc531870235)

Introduction

Carlsberg Group (“Carlsberg”) processes personal data about people as part of its business operations. No matter how personal data is collected or obtained, Carlsberg must always ensure compliance with applicable personal data protection regulations in order to retain the trust of those people Carlsberg processes personal data about.

Scope

Carlsberg has implemented a Records Management & Personal Data Protection Policy (“the Policy”) that commits all parts of Carlsberg to ensure compliance with the Policy, the Personal Data Protection Manual (“the Manual”) and applicable data protection laws at all times.

Protecting personal data is the responsibility of everyone, and Carlsberg requires that all employees, business partners and other parties, which Carlsberg interacts with, are committed to protect personal data according to the applicable laws and agreements.

This Manual covers the global Carlsberg approach to protecting personal data and in Appendix 1 more specifically compliance under the GDPR within the EU/EEA countries.

The principles, concept and requirements and the like must be read, interpreted and understood in the context of local law that may vary from country to country.

Governance Structure

# The Data protection ORGANIZATION at GROUP level

The personal data protection organization in Carlsberg consists, at Group level, of the Head of Data Protection (“HDP”) in Group Legal, reporting to the General Counsel, and the Data Protection Manager (“DPM”) reporting to the HDP.

All markets in Carlsberg shall appoint a Data Protection Responsible (“DPR”) who is responsible to local management for compliance with applicable local data protection regulation and the Policy and Manual. As IT systems are an integral part of ensuring data protection compliance, GBS will not only have a dedicated DPR but also representatives at Group level. This is further illustrated below:



Figure 1: The Data Protection organization at Group Level.

## **Local Data Protection Organization**

### Management

Management in all markets and in the global functions (ISC and GBS) are responsible for ensuring compliance locally with the Policy, the Manual, and relevant data protection regulations. Management shall ensure that there is a local data protection organization in place as described below.

### Local Data Protection organization in the EU/EEA markets

The local data protection organization in the EU/EEA markets will typically be anchored in Finance (See appendix 1).

Subject to approval from the General Counsel, markets or global functions may deviate from this proposed standard organization to reflect the specific market setup (e.g. clusters of markets or markets with small sales organizations only).

### Local Data Protection Organization outside the EU/EEA markets

The local data protection organization outside the EU/EEA markets shall have a local DPR and support function representatives as will be required, given the specific risk profile and applicable data protection regulation.

The DPR will typically be anchored in Legal. Other organizational structures and the roles and responsibilities will beagreed upon on a case-by-case basis by local management and the General Counsel.

Processing of personal data

# What is personal data?

"Personal data" means any information that relates to an identified or identifiable individual (“Data Subject”). Such information may be names, email addresses, initials, payroll information etc.

Some types of personal data are considered *sensitive personal data*. Special attention must be given if sensitive personal data is being processed.

Personal data that has been anonymized is not considered personal data.

# The Concept of “processing of personal data”

The concept of “processing of personal data” may in some jurisdictions be understood broadly and in others narrowly. Each box in the figure below may be seen as a form of “processing”.



Figure 2: The figure shows examples of the broad concept of “processing of personal data”

Principles for processing personal data

# The overall key principles

Carlsberg is committed to protecting the personal data that Carlsberg processes, for example data on employees, business partners, customers and consumers. Carlsberg shall protect personal data that Carlsberg uses in the course of its business in line with relevant local laws and the following key principles[[1]](#footnote-1) for processing personal data in Carlsberg.

The principles are described below:



Figure 3: The six overall key principles for processing personal data.

These principles constitute Carlsberg’s general approach to data protection which shall be subject to local legal requirements.

# Data subject rights

Carlsberg will fulfil the rights of the data subjects under applicable local data protection requirements[[2]](#footnote-2).

# Transfer of data and the use of processors

All data exchange of personal data within Carlsberg shall be governed by the Intra Group Agreement which is the agreement for both data transfers and data processing. Carlsberg has applied for the Binding Corporate Rules to substitute the data transfer part of Intra Group Agreement and all Carlsberg entities shall upon approval of the application (app. by 2020) undertake to adhere to the Binding Corporate Rules Procedure.

All processing of personal data by an external party requires a relevant data processing agreement, unless it is not a requirement according to applicable international and local law outside EU/EEA.

# incidents and breaches

Carlsberg is committed to protecting all personal data in the best possible way, but acknowledges at the same time that technical and/or human errors/acts/omissions can occur or malicious or intentional acts of e.g. Carlsberg employees or third parties can happen. A personal data breach means that personal data in Carlsberg’s possession is compromised through unauthorized access or accidental deletion or corruption. In order to manage a potential personal data breach in an efficient manner, Carlsberg has established relevant personal data breach procedures which should be followed in the event of a personal data breach.

If you suspect that a personal data breach has occurred or is likely to occur, the local DPR must be contacted immediately.

# Training

All Carlsberg employees working with personal data shall be provided training in complying with applicable data protection requirements.

Training programs shall be ongoing and include training in the Manual and any local regulations and procedures. Where possible, training should be built into existing training programs. New employees shall receive adequate training in protection of personal data no later than three months after commencing their role unless more immediate training is required.

# More information

You can also visit the Compass SharePoint site to access all company general and functional policies including the Records Management & Personal Data Protection Policy. You may also visit the Group Legal Personal Data Protection SharePoint site.

Roles and responsibilities

|  |  |  |  |
| --- | --- | --- | --- |
| Roles |  | Role description | Level of responsibility |
| ExCom |  | Responsible for Policy approval. | Global |
| General Counsel |  | Policy owner with overall responsibility to ExCom for personal data protection issues and for ensuring that personal data protection risks in the Group are duly attended to and communicated to ExCom/the Audit Committee/the Supervisory Board, as relevant. | Global |
| Head of Data Protection  |  | Manual owner and responsible for the implementation of data protection, including the implementation of the Records Management & Personal Data Protection Policy and Personal Data Protection Manual throughout the Group. | Global |
| Local Data Protection Responsible |  | Responsible towards local management for ensuring the local day to day compliance with the requirements set out in the Policy and this Manual. | Local |
| Management of local entity and Group functions |  | Responsible for ensuring that the Policy and this Manual are implemented and adhered to, and that all relevant employees are made aware of the Policy and the Manual and their requirements. | Local |
| Management of Corporate and Local IT |  | Responsible for ensuring that relevant IT systems are compliant with the Policy and this Manual. | GlobalLocal |
| Local Legal Counsel |  | Responsible for supporting local implementation and operationalization of the Policy and this Manual.  | Local |

Monitoring and control

The effectiveness of this manual shall be monitored and controlled by managers, and as part of internal audit programs and any audit findings acted on.

Glossary

HDP: Head of Data Protection

DPM: Data Protection Manager

DPR: Data Protection Responsible

DPC: Data Protection Contact

Deviations

Deviations from this Manual must be approved by the Manual Owner.

Associated policies and other

* + - * + Records Management & Personal Data Protection Policy
				+ Information Security and Acceptable Use Policy
				+ Security Policy
				+ Data Breach Procedure
				+ Intra Group Agreement

Contact

For more information, please reach out to your local DPR or the HDP.

Manual revision history

|  |  |  |
| --- | --- | --- |
| Version | Publication date | Approval of revisions |
| 0.9 | December 2018 | HDP/ General Counsel |

Appendix 1

GDPR - Additional Requirements in

the EU/EEA markets

Introduction

This Appendix covers **only** the **Carlsberg entities that operate in the EU/EEA countries**. This Appendix sets out mandatory requirements, additional to the Manual, for protecting personal data more specifically under the GDPR.

The scope and structure

The Appendix is divided into three main areas:

1. Personal Data and Processing
2. Data Protection Organization
3. The Carlsberg GDPR Compliance Framework

personal data and processing

# Personal Data according to GDPR

## **What is personal data?**

In conjunction with the definition in the Manual under section 2 the GDPR applies to the use of all personal data that is processed electronically or manually.

Personal data includes three groups 1) non sensitive data, 2) sensitive data and 3) criminal records. Under EU law sensitive data comprises: racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data and sex life or sexual orientation. When processing sensitive data or criminal records, Carlsberg must ensure adherence to the special GDPR requirements hereon e.g. explicit consent and higher security levels.

## **What is “processing of personal data”?**

The concept of “processing of personal data” is understood broadly in GDPR and covers all the following types of ways of processing personal data:

* Recording
* Organization
* Structuring
* Adaptation or alteration
* Retrieval
* Consultation
* Use
* Disclosure by transmission
* Distribution or otherwise making available
* Alignment or combination
* Restriction or destruction
* Archives or clouds, and
* Deletion

Carlsberg must adhere to the applicable key processing requirements described above in respect to all stages of the personal data life cycle. Examples of processing of personal data with a specific purpose as part of one or more of business processes in Carlsberg, are given below:

* + Carlsberg *may collect* personal data, when Carlsberg recruits candidates for vacant positions.
	+ Personal data *may be recorded* when Carlsberg records employee activities performed as part of complaint handling processes.
	+ The personal data *will be stored by Carlsberg* or service providers in systems, archives, clouds etc. for the purpose of keeping the data for business purposes.
	+ The data might *be transferred or shared internally* in Carlsberg, or externally with third parties, to achieve the purposes of the processing.

It is important to note that any processing that is outsourced to service providers is still considered processing that Carlsberg, as controller, is responsible for.

* + When the data is no longer needed *it will be deleted or anonymized* by Carlsberg, and if it has been share with externals, Carlsberg must request the externals to delete this accordingly.

Data Protection organization

Carlsberg entities in the EU/EEA markets are required to establish a local data protection governance. The local data protection organization in the EU/EEA markets will typically be anchored in Finance as illustrated in the figure below:



Figure 4: The local data protection organization in the EU/EEA markets.

The CARLSBERG Gdpr Compliance framework

# What is the Carlsberg GDPR compliance framework?

The Carlsberg GDPR compliance framework in the EU/EEA markets falls into seven main areas:

1. The Carlsberg GDPR House
2. The overall Key Principles for Processing Personal Data
3. Data Subject Request
4. Working with Third Parties
5. Transfer Requirements
6. Data Breach
7. Contact

# The Carlsberg GDPR House

The Carlsberg GDPR house consists of three elements:

1. **The Data Inventory:** The Data Inventory should for each Carlsberg entity comprise and maintain a record of all personal data processing activities in each functions. This record is necessary for Carlsberg to maintain an overview of the personal data that is processed throughout the Carlsberg Group in the EU/EEA markets.
2. **Governance:** The Governance related to policies, manuals and procedures that apply to each entity in the EU/EEA markets. Governance must ensure that relevant policies, manuals, standard operating procedures (“SOP”) are in place, and that Carlsberg at all times can demonstrate that policies, manuals, SOPs and guidelines are generated and followed as part of the day-to-day business.
3. **Embedding**: Embedding includes in Carlsberg training and creating general awareness into the application and adherence to the GDPR.

GDPR in Carlsberg is visualized in the below figure called “the Carlsberg GDPR house”:



Figure 5: The Carlsberg GDPR house.

# The Overall Key Principles for Processing Personal Data

The Carlsberg GDPR Compliance Framework sets out one extra key principles in addition to the six principles mentioned in the general part of the Manual above. The seven principles are shown below:



Figure 6: The seven key principles in the EU/EEA markets

The meaning attached to the key principles, however, differs from country to country.

Hence, in the EU/EEA markets, the seven principles must therefore be read, understood and interpreted in accordance with the GDPR as well as additional local data protection laws.

The extra key principle that applies under GDPR is “accountability”. The principles are further addressed below in the GDPR context:

## **Lawfulness, Fairness and Transparency**

**Lawfulness:** Carlsberg has identified an appropriate lawful basis (or bases) for processing of personal data

**Fairness:** Carlsberg has considered how the processing may affect the individuals concerned and can justify any adverse impact

**Transparency:** Carlsberg comply with the transparency obligations of the right to be informed.

Before processing personal data, it must be ensured that Carlsberg has a lawful basis (a “legal basis”) for processing the personal data. The relevant local DPR will give guidance as to what is required in a particular market.

This means that before Carlsberg processes personal data, it must be assessed if the processing of the personal data is allowed. The legal basis will typically depend on:

* + - * + the purpose for which Carlsberg is collecting the personal data, and
				+ the character of the personal data (if it is sensitive or special categories of personal data)

The processing of personal data can be based on one or more of the below legal bases:



Figure 6: The legal bases for processing personal data.

In addition to the legal bases, Carlsberg must ensure that the processing in general complies with the GDPR in whole as well as additional local data protection laws.

Under the GDPR, transparency means (among other things) that when personal data is processed about an individual, the person must before the processing begins, be notified about the processing of their personal data, including the purpose, data retention periods, etc. This applies regardless of whether the data subject is an employee or a person external to Carlsberg such as a consumer, a supplier or a website visitor.

Before processing personal datayou mustverify that the data subjects, about whom Carlsberg is processing personal data, have been or will be provided with the required information.

## **Purpose limitation**

Carlsberg shall process the personal data for the specified, explicit and legitimate purpose(s) under which the personal data was originally collected and not processed for further processed in any manner that is incompatible with this purpose or those purposes.

## **Data minimization**

Carlsberg shall only process personal data which is adequate, relevant and limited to what is necessary in relation to the purpose(s) for which the personal data was processed.

Carlsberg should not process more personal data than Carlsberg needs to achieve the purpose(s) in question. Furthermore, Carlsberg should not include irrelevant details of personal data.

If Carlsberg process data than is actually necessary for the given purpose, this is likely to be unlawful (as most of the lawful bases have a necessity element) as well as a breach of the data minimization principle. Individuals will also have the right to request erasure of such data in this regard.

## **Accuracy**

Carlsberg shall take all reasonable steps to ensure that personal data stored and processed is not incorrect or misleading and, where necessary, kept up to date; having regard to the purposes for which the personal data is processed, erased or rectified. This must be done without delay.

According to this principle Carlsberg may need to keep the personal data updated, although this will depend on what Carlsberg is using it for.

## **Storage limitation (Retention)**

Carlsberg shall not keep personal data for longer than is necessary for the purpose(s) for which the personal data are processed. When Carlsberg no longer has a legitimate purpose for storing or processing personal data, such personal data must be deleted or anonymized.

Thus, Carlsberg must establish and implement retention and deletion periods for personal data being processed by Carlsberg.

However, the standard for when personal data is considered truly anonymized is normally a very strict standard. In practice this would e.g. mean that if Carlsberg was to make an aggregated report on employee salaries based on anonymized data, all identifiers such as names, initials etc. must be deleted from the data set.

## **Confidentiality and security**

This principle means that Carlsberg must have appropriate security to prevent the personal data from being accidentally or deliberately compromised.

Carlsberg must ensure that technical, organizational and physical security measures are applied at the locations processed for storing and processing personal data.

Such measures may include the locking of premises, access control, implementation of alarm systems and fire prevention and protection systems.

Furthermore, Carlsberg must ensure that personal data is not disclosed to any unauthorized individuals, including employees of Carlsberg who do not have a purpose for processing the personal data.

In Carlsberg, this must be ensured through the use of encryption technologies, training programs, access restrictions, contractual clauses with third parties etc.

## **Accountability**

Accountability means that Carlsberg is responsible for complying with the GDPR, and Carlsberg must be able to demonstrate that Carlsberg is compliant.

This means that Carlsberg must establish clear accountability and traceability of Carlsberg’s storage and processing of personal data. This can e.g. be achieved by assigning roles and responsibilities for use of the personal data in question or through use of system logging, self-auditing or review of log files.

# Data subject rights

Carlsberg must facilitate the rights of the data subjects under applicable data protection requirements. It is essential that Carlsberg supports data subjects in exercising these rights. In the EU/EEA markets data subjects have the rights to request the following:



# Working with third parties

Carlsberg engages a number of suppliers in providing services that entail that the supplier will process personal data on behalf of Carlsberg. In these situations Carlsberg will be considered the data controller, and the supplier will be considered a data processor.

A data controller is the entity that determines the purpose and means of processing personal data. For instance Carlsberg will be data controller in respect of personal data processed on employees as part of the internal HR administration.

A data processor is an entity that is engaged by the data controller to process personal data on behalf of the data controller and in accordance only with the instructions of the data controller. If Carlsberg engages a payroll service provider to process payments to Carlsberg’s employees, the payroll service provider will be a data processor.

Prior to Carlsberg engaging a data processor, Carlsberg must:

* verify that the supplier will be able to protect the personal data (due diligence);

A data processing agreement is a set of contractual clauses that ensure that external suppliers engaged by Carlsberg to process personal data on behalf of Carlsberg are legally obliged to protect the personal data in question and only use the personal data as instructed by Carlsberg.

* ensure that the supplier provides sufficient guarantees to protect the personal data, and
* that a data processing agreement is entered into between Carlsberg and the supplier.

It will always be Carlsberg’s responsibility that the personal data is sufficiently safeguarded by processors and any failures at a supplier to protect personal data can result in a significant risk to Carlsberg.

In some situations, Carlsberg may provide personal data to third parties, including affiliates within the Carlsberg Group that are not engaged by Carlsberg to process personal data on behalf of Carlsberg. This would e.g. be the case if Carlsberg is legally required to provide personal data on its employees to local tax authorities. In these situations Carlsberg will still be considered data controller, but the third party will also be considered data controller as the third party processes the personal data for its own purposes.

# Transfer requirements

Transferring personal data – or simply sharing it – with others internally or externally must only take place under very specific circumstances, where the following requirements apply:

1. A legal basis is required for transferring or sharing personal data to third parties that also act as a data controller.
2. Personal data must not be shared informally or casually.
3. The purpose of the transfer/sharing must be in line with the purpose for which the personal data was collected.
4. The data transferred must be limited to what is necessary to achieve the purpose.
5. Transferring personal data to third parties that also acts as a data controller such as suppliers, affiliates within Carlsberg, or authorities requires a legal basis. It should therefore be verified that either of the legal basis described above apply to the transfer of personal data.

# Data breach

In order to manage a potential personal data breach in an efficient manner, Carlsberg has established relevant personal data breach procedures which should be followed in the event of a personal data breach.

If you suspect that a personal data breach has occurred or is likely to occur, the local DPR must be contacted immediately.

# Contact

For more information, please reach out to your local DPR and please do contact the local DPR to enquire about how to:

* Proceed before starting a new processing of personal data
* Ensure that Carlsberg’s data processing record (Data inventory) is updated correctly
* Proceed before notifying data subjects
* Proceed if you receive a request or complaint from a data subject
* Proceed if you have any questions related to the secure transfer of personal data before the transfer or type of transfer is initiated, and
* Proceed if you want to transfer or share personal data with externals (e.g. engaging a new data processor or a data controller).

|  |  |  |
| --- | --- | --- |
|  |  | November 2018Carlsberg Breweries A/S100 Ny Carlsberg Vej1799 Copenhagen VDenmark |

1. If a local market data protection regulation requires a higher standard, such higher standard shall be followed. Your local Data Protection Responsible will guide you as to the relevant key principles. [↑](#footnote-ref-1)
2. The data subject rights applicable under GDPR are set out in Appendix 1. [↑](#footnote-ref-2)