ROYAL UNIBREW

General Data Protection and Data Ethics Strategy

Version 1.0
October 2022

General Data Protection and Data Ethics Strategy

1. Introduction

The increasing digitalization implies the collection of massive amounts of personal data in order to improve and adapt products and services as well as improve performance internally and externally. This involves risks of unlawful and unauthorized access to and use of personal data and gives rise to ethical dilemmas when using data.

This policy represents the Royal Unibrew Group ("Royal Unibrew") strategy on information security and data protection and describes how data ethics is considered and included in the use of data and in the design and implementation of technologies, especially new technologies, used for processing of data within Royal Unibrew.

Royal Unibrew will adopt specific guidelines, processes, and procedures to ensure that data, systems and information assets are used in accordance with legislation and the policies of Royal Unibrew. Such guidelines are communicated in the relevant parts of the organization to ensure that employees understand and comply with this policy and such guidelines.

2. Scope

This Policy applies to all employees and entities in Royal Unibrew. External consultants, collaborators and suppliers that handle data for or in collaboration with Royal Unibrew are also covered by this Policy.

3. Risk, Transparency and Compliance

Royal Unibrew acknowledges and has a clear conception of its liability for any processing of personal data under its responsibility and instructions. Accordingly, Royal Unibrew aims to secure that any processing of personal data under Royal Unibrew's responsibility will take place in accordance with applicable data protection legislation.

All processing of personal data must be transparent, as the trust of employees, customers, business partners and other third parties with whom Royal Unibrew interacts is of major importance to Royal Unibrew.

Data protection risks are closely related to IT risks in terms of their risks and consequences to the business and the likelihood of occurrence.

In line with the overall business objectives of Royal Unibrew, Royal Unibrew aims to achieve a high degree of compliance and a low risk of unintended events, including unauthorized or unlawful processing and accidental loss, destruction or damage of personal data.

4. Organization and governance

Management of data protection and information security is a part of and is integrated in Royal Unibrew's processes and overall structure and protection of personal data must be considered in the designing of processes and systems.

Royal Unibrew has implemented an IT Business Continuity Plan (IT-BCP) defining the strategy for Royal Unibrew’s organizational management and handling of IT emergency situations. The IT emergency work must limit the consequences of loss of information and systems caused by disasters and security breaches.

Information Security Committee

An information security management system is established to ensure structured management and protection of the organization's data. The information security management system includes organization, policies, guidelines, and procedures, planned activities, responsibilities, processes, and resources.

Overall decisions concerning the information security management system are made by the Information Security Committee (ISC), which consists of the following members:

- CFO - Chairman
- CIO
- CHRO
- Group General Counsel

The ISC meets half-yearly or when necessary. Any existing or potential data security breaches or events relating to data security will be addressed and appropriate actions taken according to the information security management system.

The management system must be appropriate and sufficient and ensure continuous improvement of information security and data protection. The ISC's work comprises continuously approving risk assessments, action plans, training, policies, and guidelines.

The ISC is responsible for ensuring that the various functions have the appropriate skills for the tasks to be solved or to assess whether further training or training in the field should be initiated. The ISC’s decisions will be implemented and handled by the responsible Royal Unibrew employees described in the Roles and Responsibilities section below.

By the end of every year, the ISC will evaluate the impact of the management system's overall efforts and subsequently optimize and correct accordingly.

Roles and responsibilities

The overall responsibility in relation to processing of personal data within Royal Unibrew lies with the Executive Board. Group measures in relation to data protection are decided by the Executive Board, and apply within Royal Unibrew Group with relevant reservations for local legislation.

The Corporate Risk Manager is responsible for the organization's risk management and reports risks to the Executive Board.

The General Managers in subsidiaries of Royal Unibrew are responsible for the subsidiary they manage.

The CIO ensures that the IT function conducts risk assessments of the relevant data and information assets and reports the overall IT risk picture to the Corporate Risk Manager.

5. Training and awareness

It is of the utmost importance that employees, who as a part of their job within the Royal Unibrew Group, process personal data or are engaged in designing, purchasing, or implementing technologies for the processing of personal data, understand their responsibility. Royal Unibrew will encourage this sense of responsibility through education and training targeted to the relevant groups of employees.

Royal Unibrew ensures that employees, receive education and training in the handling of personal data and data ethics described in this Policy at least once a year.

If Royal Unibrew finds that certain employees need additional training or more frequent training than described above, Royal Unibrew ensures that such employees receive the targeted training deemed necessary to ensure compliance with this policy.

6. Data ethics

When the Royal Unibrew Group processes personal data or designs, purchases or implements technologies, especially new technologies, entailing processing of personal data, principles for data ethics must be assessed and included in the considerations during the design process and/or prior to the purchase or implementation of the processing activity or the technology used for the processing of personal data.

The following principles for data ethics must be considered:

- **Necessity**: Only personal data which is necessary to fulfill the purpose of the processing activity shall be collected and processed. For example, it shall be considered whether it is possible to achieve the purpose of the processing with anonymized data instead.
- **Legality**: The processing of personal data shall, at all times, comply with applicable legislation. For example, the processing of personal data requires a specific legal basis according to the General Data Protection Regulation (“GDPR”).
- **Ethical design**: Technologies for the processing of personal data, especially new technologies, shall be designed to respect principles of data ethics, including the principles laid down in this policy and the general processing principles as laid down in

the GDPR. For example, technologies shall be designed to ensure correct and timely deletion of personal data in accordance with the Royal Unibrew Group's retention periods.

- **Consequences:** The consequences of the processing activity and the technology used for the processing activity shall be considered, especially where new technology is used for the processing of personal data. In such case, the consequences for the individuals, both in short term and long term, shall be considered.
- **Expectations:** Personal data shall be processed in ways that are consistent with the intentions, expectations and understanding of the disclosing party. Thus, personal data may not be processed for new purposes which are incompatible with the purposes for which the personal data was originally collected.
- **Security:** A sufficient level of security shall be implemented in and around technologies used for processing of personal data. The security measures shall include technical as well as organisational measures, and the sufficient level of security shall be assessed based on a risk assessment of the specific processing activity and the technology used for the processing of personal data.
- **Transparency:** Personal data shall always be processed in a way that ensures transparency, especially where algorithms are used for the processing. Furthermore, when the processing activity includes automated decision making for decisions which have legal or similarly significant effects, the results shall be subject to human review.
- **Respect for human rights:** Processing of personal data and the design of technologies used for processing of personal data shall ensure that human rights are respected. For example, processing of personal data or use of technologies for the processing of personal data may not be biased with a risk of discrimination, marginalisation or stigmatisation against individuals.
- **Proportionality:** Personal data shall be processed only for purposes which are proportional taking into account the rights of the individuals, including the right of privacy. Thus, a proportionality assessment shall always be carried out before beginning new processing activities or implementing or designing technologies for the processing of personal data. If the proportionality assessment shows that the processing is not proportional, the processing activity may not be initiated.
- **Accountability:** Royal Unibrew Group shall be able to demonstrate that this policy is complied with. Thus, the considerations relating to these principles for data ethics shall be documented in relation to all processing activities, designs or choice of technologies.

7. Cooperation with relevant authorities

Royal Unibrew will cooperate with the relevant Data Protection Authorities (DPAs). Royal Unibrew undertakes to follow any advice and recommendation of the relevant DPAs regarding any issues relating to the processing of personal data at Royal Unibrew.

Royal Unibrew will establish procedures ensuring that the relevant DPAs are notified in case of data protection breaches as defined in the GDPR.

8. Communication

This policy is made available and communicated to relevant stakeholders. Royal Unibrew ensures that this policy is available to employees, e.g., on the intranet, with the purpose of

ensuring the employees' access to the applicable principles for data ethics for Royal Unibrew. This policy will be attached to agreements and other relevant documents to external parties when relevant.

Version	Approved	Date	Changes
1.0	Board of Directors	November 2022	N/A