ROYAL UNIBREW

General Data Protection and Data Ethics Policy

Version 1.3
November 2026

General Data Protection and Data Ethics Policy

1. Introduction

Digitalisation and the increasing use of data and technology create opportunities to improve products, services and internal processes, but also create risks of unlawful and unauthorized access to and use of personal data and give rise to ethical questions about how personal data and technology are used.

This General Data Protection and Data Ethics policy ("Policy") sets out the overarching principles for data protection and data ethics in the Royal Unibrew Group ("Royal Unibrew"). It applies to the processing of personal data and describes how data ethics is considered and included in the use of data and in the design, implementation and use of technologies used for processing of personal data within Royal Unibrew.

This Policy is supplemented by the Information Security Policy that governs information security, the Guidelines for use of Generative AI that govern the responsible use of Artificial Intelligence, and specific guidelines, processes and procedures that provide more detailed requirements for the responsible and compliant use of data and technology.

All relevant policies, guidelines, processes and procedures are communicated to the organisation to ensure that data, systems and information assets are used in accordance with applicable legislation and the policies of Royal Unibrew, and to promote understanding of and compliance with the applicable requirements.

2. Scope

This Policy applies to all Royal Unibrew entities and to all employees, including permanent and temporary employees. This Policy also applies to external persons working for or on behalf of Royal Unibrew, such as consultants, collaborators and suppliers who process personal data for or on behalf of Royal Unibrew.

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 must ensure 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 lawful, fair and transparent. Royal Unibrew must identify, assess and manage data protection risks, taking relevant information security and business risks into

account. Appropriate measures must be implemented to prevent unauthorised or unlawful processing and accidental loss, destruction, disclosure of, access to or damage of personal data.

4. Organization and governance

Data protection and data ethics are integrated into Royal Unibrew's governance, processes and systems. Data protection must be applied and considered when processes and systems involving personal data are designed, introduced or changed.

Royal Unibrew manages data protection, data ethics and information security through Royal Unibrew's governance framework that includes policies, guidelines, defined roles and responsibilities, risk assessments, controls, training, incident management and reporting, with oversight by the Information Security Committee. The effectiveness of the framework is regularly reviewed and identified weaknesses or risks must be addressed as appropriate.

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
The Information Security Committee (ISC) provides governance and oversight of data protection and data ethics under this Policy in addition to its responsibilities under the Information Security Policy and makes overall decisions concerning the management and protection of data. Material data protection and data ethics risks, incidents and compliance matters must be reported to the ISC, so that appropriate actions can be taken.

The ISC's work comprises continuously approving risk assessments, action plans, training, policies, and guidelines. The ISC's composition and working procedures are set out in the Information Security Policy.

Roles and responsibilities
Royal Unibrew Executive Management has overall responsibility for compliance with this Policy and for ensuring that appropriate resources are available. Group measures in relation to compliance with this Policy is decided by the Royal Unibrew Executive Management and apply within Royal Unibrew Group with relevant reservations for local legislation.

General Managers in subsidiaries and separate entities of Royal Unibrew are responsible for implementing this Policy within the subsidiary or entity they manage and for ensuring compliance with applicable local legislation. General Managers shall report material incidents and cases of non-compliance to the ISC.

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 ISC.

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 are trained to comply with this Policy at least once a year.

If Royal Unibrew finds that certain employees need additional risk-based and role-specific training or more frequent training than described above, Royal Unibrew ensures that such employees receive such training as deemed necessary to ensure compliance with this Policy.

6. Data ethics

Data ethics must be considered when Royal Unibrew processes personal data or designs, purchases or implements technologies, especially new technologies and AI. 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 assessment must be proportionate to the nature, context, purpose and risks of the activity or technology.

The following principles for data ethics must be considered:

- **Necessity**: Only personal data which is necessary to fulfil the purpose of the processing activity shall be collected and processed. For example, it shall be considered whether the purpose of the processing can be achieved using anonymised data instead.
- **Lawfulness**: The processing of personal data shall at all times comply with applicable legislation. For example, the processing of personal data requires a valid 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 set out in this Policy and the general processing principles under the GDPR. For example, technologies shall support correct and timely deletion of personal data in accordance with Royal Unibrew's applicable retention requirements.
- **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.
- **Reasonable expectations:** Personal data shall be processed in ways that are consistent with the reasonable expectations of the individuals concerned. Personal

data shall not be processed for new purposes which are incompatible with the purposes for which it was originally collected.

- **Security:** Appropriate technical and organisational security measures shall be implemented for technologies used to process personal data. The appropriate level of security shall be determined based on a risk assessment of the specific processing activity and the technology used for the processing of personal data and in accordance with the Information Security Policy.
- **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. Processing activities and technologies shall not create unjustified risks, or risks 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 shall be able to demonstrate compliance with this Policy. Relevant considerations, assessments and decisions shall be documented in relation to all processing activities, designs or choice of technology.

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 and within the applicable statutory time limits.

8. Communication

This Policy is made available and communicated to employees and other 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 protection and 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

1.1	Board of Directors	November 2023	Editorial changes and updates
1.2	Board of Directors	November 2024	Update of ISC meeting frequency
1.2	Board of Directors	November 2025	None
1.3	Board of Directors	November 2026	Updated to align with the Information Security Policy