Procedure owner: Group CEO
Approver: Board of Directors

Group Policy – Data Protection

1. Purpose and Scope

This Group Policy - Data Protection reflects the obligations imposed by European and national data privacy legislation, defines the main principles regarding processing of personal data in the Group and establishes Group data protection accountability framework.

This policy shall apply to Boozt AB and any subsidiary in which Boozt AB directly or indirectly owns more than 50% of the voting shares or in which the power of control is possessed and exercised by or on behalf of Boozt AB.

This policy shall take precedence over any internal policies or procedures of the Group regarding data protection in case of a conflict. The terms used in the policy have the same meaning as in the General Data Protection Regulation (GDPR), unless explicitly stated otherwise.

This policy does not replace applicable EU legislation and national laws. The regulations and laws shall take priority if compliance with this policy would result in a violation of national law. The content of this policy must also be observed in the absence of corresponding national laws.

2. Main Principles

The Group shall process personal data in accordance with the following fundamental principles:

2.1. Processing must be lawful, fair, and transparent

The Group shall process personal data in a lawful, fair, and transparent manner. In particular, the processing may only take place if and insofar as the legal ground exists and has been identified by the Group company processing personal data before data has been collected for such purpose. The Group company processing personal data shall, in a clear and concise manner, inform people whose personal data it processes about the type of personal data that is collected, the sources of such data, the purpose and the legal grounds for such collection. Such information shall be readily accessible and available when personal data is first collected from the data subject to enable the data subject to make an informed and conscious decision whether to provide personal data to the Group company.

2.2. Personal data shall only be processed for specific, explicit, and legitimate purposes

The Group shall process personal data for specified, explicit, and legitimate purposes, and shall not process it further in a manner incompatible with those purposes. In particular, the Group company shall ensure that that it processes personal data in compliance with applicable data protection legislation and in accordance with general principles of law. The processing shall be

sufficiently defined to enable the implementation of any necessary data protection safeguards and delimit the scope of the processing operation. In addition, the processing purposes shall be sufficiently unambiguous and clearly expressed to prevent any hidden processing.

2.3. Personal data undergoing processing shall be adequate, relevant, and not too extensive in relation to the purpose

The Group shall process personal data only to the extent necessary for the explicit purpose applicable for that processing, while always considering the protection of individuals' privacy.

2.4. Personal data undergoing processing shall be accurate

The Group undertakes to keep personal data accurate and reasonably up to date as commercially possible. The Group entity shall provide data subjects whose personal data it processes with accessible ways to verify the validity and correct inaccuracies of such personal data.

2.5. Personal data shall not be processed for longer than is necessary for the purpose of processing of the personal data.

The Group shall have procedures in place that set out principles and rules for data retention and which apply to all Group companies subject to this Policy. The Group will ensure that these data retention rules are aligned with the requirements and standards for data retention set out in applicable laws. The Group company may only retain personal data for as long as it is needed for the purpose of processing of the personal data. When personal data is no longer necessary to fulfil the explicit purpose in question, which legitimised its original collection and processing, the Group company shall permanently delete such data, unless it is prevented from doing so under applicable laws.

2.6. The Group shall process personal data with a view of safeguarding integrity, confidentiality, and security

The Group shall ensure appropriate technical and organizational measures are in place to protect the data against accidental or unlawful destruction, accidental loss, alteration or corruption, unauthorized disclosure, or access, and unauthorized or unlawful processing. The measures shall include both proactive and reactive approach to data privacy and security. A risk assessment process is used to establish a risk baseline and to periodically identify new or changed risks to personal information and to develop and update responses to such risks. The personal data shall be processed in accordance with Boozt Group security policies and procedures which the Group undertakes to maintain, in particular, Group IT Policy, Group Policy – Information Security, Group Procedure – IT User Access Management, Group Procedure – IT Incident Management, Group Procedure – IT Disaster Recovery Plan and Group Procedure - IT End User Guidelines.

2.7. The Group will ensure data protection by design and default

The Group aims to ensure that the protection of personal data is taken into account in any technical or commercial project, including any requirement to comply with other applicable local law. In particular, this should apply to developing, designing, selecting, and using applications,

services and products that are based on the processing of personal data or that process personal data to fulfil their task.

3. Group Accountability Framework

Data protection legislation includes an accountability principle, which requires the Group to demonstrate that the Group complies with the data protection principles. The Group demonstrates compliance through the measures and commitments set out below.

3.1. Leadership and Culture

The Group undertakes to establish, maintain, and promote a proactive, positive culture of data protection compliance. Group Management bears the responsibility for implementing a corporate privacy culture that is in line with corporate strategy, legal and regulatory requirements, and business ethics.

The Group shall conduct an internal analysis to determine whether or not a Data Protection Officer shall be appointed in the Group. Such internal analysis should be updated when necessary for example if the Group undertakes new activities or provides new services that might fall within the cases listed in Article 37(1) of the GDPR. The Group may choose to voluntarily appoint a Data Protection Officer in which case Articles 37-39 of the GDPR will apply as if the designation had been mandatory. The Group should consider such Data Protection Officer as a Group function and provide the Data Protection Officer with the necessary resources, including human resources, to carry out its tasks and duties.

Irrespective of the appointment of a Data Protection Officer, the Group Management shall ensure that data protection liaisons with a good knowledge of past, ongoing, and planned projects, developments and processes are appointed in every department that is involved in processing of personal data in order to maintain high privacy awareness and support the data protection function within the Group in ensuring compliance with this Policy and applicable laws. Group Management considers data protection and information governance issues and risks reported by the data protection liaisons.

3.2. Consistency with Laws and Regulations

Policies and procedures that govern data protection and informational security are maintained and revised based on the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and notices are revised to conform with the requirements of applicable laws and regulations.

The Group shall establish and maintain internal policies and procedures that clearly set out the organisational structure for managing data protection and information governance, as well as clear reporting lines and information flows between relevant groups. Each Group company must ensure that the data protection and information governance staff have clear responsibilities, as well as authority, support, and resources to carry out their responsibilities effectively.

3.3. Training and Awareness

The Group shall maintain a comprehensive privacy awareness program about the Group's processing of personal data. The privacy awareness program shall include an in-depth training for all employees and contractors who have access to personal data which covers privacy and security topics, legal and regulatory considerations, and incident response for all employees depending on their roles and responsibilities. The Group shall strive to maintain a more specialised training for the frontline staff.

3.4. Protection of rights

The Group makes sure that there are rules and procedures in place for identifying and dealing with requests and complaints from data subjects, including an internal escalation process that ensures the any inquiry or complaint receives proper attention.

3.5. Record Management

The Group company processing personal data, whether as a data controller or a data processor, has to maintain a complete record of processing activities in accordance with Article 30 of the GDPR. Where the Group company refers to any legal ground for processing of personal data, the Group entity is required to maintain internal records and documentation to justify the existence of such ground for the processing operation in question. The Group may adopt additional policies and procedures that govern the format of such record-keeping.

4. Implementation and Compliance

4.1. Implementation of Main Principles

The main principles shall be implemented as described in this policy. The Group CEO is responsible for the implementation of this Policy. The Board of Directors has overall responsibility for data protection in the Group.

4.2. Monitoring of Compliance

The Group CEO shall monitor compliance with the Policy. The Legal Department or, if appointed for the Group, the DPO reports any deviations of this Policy to the CEO.

4.3. Deviation Handling

Deviations from main principles and/or procedural action steps can be exceptions or breaches. A deviation can either be permitted, and is then referred to as an exception, or not permitted, and is then referred to as a breach.

Exceptions shall not be granted unless exceptional conditions exist. The Group CEO shall address any request for exception in writing to the Board of Directors. The Board of Directors shall assess and decide on each request individually. The assessment shall take both local and Group-wide risks into consideration. Exceptions shall be documented and stored by the Group Legal Department.

The Group CEO shall immediately report any significant or material breach to the Board of Directors with a copy to the Group Legal Department. The Board of Directors shall initiate appropriate actions and/or decide whether sanctions are required.

5. References

- Group IT Policy
- Group Policy – Information Security
- Group Procedure – IT User Access Management
- Group Procedure – IT Incident Management
- Group Procedure – IT Disaster Recovery Plan
- Group Procedure - IT End User Guidelines.

6. Revision log

Volume – Valid from	Revision Category (New/Update/Wording/None)	Description of main revisions
16.12.2022	New	New