Appendix O
for “Rules of procedure for
the Board of Atrium Ljungberg AB”

Personal Data Policy
Atrium Ljungberg AB

(Resolved at the Board meeting on 12/06/2024)

Purpose

Atrium Ljungberg AB and its subsidiaries (which are jointly referred as the ‘Company’ in this document) process and handle personal data in accordance with the General Data Protection Regulation, and adopt policies and guidelines for processing and protecting personal data.

Responsibility

Atrium Ljungberg’s Board of Directors adopts the Company’s Personal Data Policy.

This policy is to be revised regularly and adopted by the Board at least once a year. The Personal Data Protection Officer is the document owner and responsible for this policy.

Organisation

Personal Data Protection Officer

Atrium Ljungberg does not need to have a Data Protection Officer as defined by the General Data Protection Regulation, as it does not conduct operations in which any substantial amount of personal data is processed. However, Atrium Ljungberg shall have a Personal Data Protection Representative who is responsible for ensuring that personal data is processed correctly and that there is adequate protection for such data. The Personal Data Protection Officer must always be asked if there are any questions that relate to the processing and protection of personal data.

The IT-architect is responsible for matters relating to information security and serves as the Personal Data Protection Representative.

Personal data processing requirements

Personal data shall be processed with due regard for the privacy of the data subject. The minimisation principle shall apply to all personal data processing, meaning that at any given time as little personal data as possible shall be used to achieve the purpose of the personal data processing. All personal data the Company collects must be correct, relevant and up-to-date, and there must be a clear purpose, reason and legal basis for processing this data.

Information

Every time the Company collects new personal data or updates existing personal data, the data subject must be informed of who the personal data controller is, the complete purpose and legal basis for the processing. Complete information on the Company's processing of personal data shall be available for data subjects via the Company's website.

As far as internal staff and agency workers are concerned, each line manager is responsible for informing them about the processing of personal data for their employment or recruitment.

Sensitive personal data

In addition to the statutory requirements, sensitive personal data may only be collected to comply with the company's obligations or to exercise its rights as an employer.

Impact analysis

A risk analysis shall be performed before introducing any measures that involve new or revised processing of personal data that could risk the privacy of the data subject. This analysis must also propose suitable routines and measures to address any risks that have been identified. The initiator of the change is responsible for initiating the risk analysis and shall contact the Personal Data Protection Representative if they have need for any support.

Agreements that include the processing of personal data must always be reviewed and approved by the Personal Data Protection Officer.

Retention period

A maximum retention period must be set for all personal data. This should be set as short as possible to protect the privacy of the data subject whist still taking the requirements and needs of the Company into account.

Deletion

Any personal data that does not meet the requirements in this policy or that has reached its maximum retention period shall be deleted.

Protection

Personal data shall be processed and stored in such a way that it is protected from unauthorised access, alteration or deletion. High standard encryption shall be used for electronic storage or transmission.

Corrections

Checks and routines shall be in place to ensure that any inaccurate or misleading personal data that are identified or become known are managed in such a way that they are immediately deleted or corrected without delay.

Rights of data subjects

Personal data must always be processed in a way that safeguards the rights of the data subjects in accordance with the General Data Protection Regulation. There shall be a clear path of contact for data subjects to contact the Company.

Incident management

A process for reporting and handling personal data breaches that fulfils mandatory reporting to the Swedish Data Protection Authority and to the data subject must be documented.

Record

There must be a central record of all personal data processing activities within the group.

Suppliersand partners

The company must have personal data processing agreements with all suppliers that process or store personal data on behalf of the company, setting out requirements to provide adequate protection of this personal data.

Processing shall take place within the EU

Personal data processing shall take place within the EU/EEA or within countries approved by the European Commission. Exceptions to this can only be made through transfer mechanisms approved by the European Commission and any such processing must be approved by the Head of Technology Development and Digitalisation.

Periodic checks

Processes must be in place for reporting and monitoring compliance with the Personal Data Policy and associated guidelines.

Regular monitoring, documentation and reporting of the level of compliance throughout the Group must be carried out as an integral part of day-to-day operations. The Personal Data Protection Officer is responsible for ensuring that monitoring and reporting are carried out at least once a year.

Reporting must include the following, at minimum:

- Follow-up of the effectiveness of checks, including assessment data.
- Reporting of incidents/deviations from the policy, along with a description.
- Action(s) with a description of what will be achieved by the action(s) and when the action(s) will be taken to address the incident/deviation
- Follow-up of outstanding actions and completion reporting