

LEGAL & DATA PROTECTION

Data Processing Agreement

This Data Processing Agreement ("DPA") governs the processing of personal data by Hubfolio on behalf of your organisation in accordance with Article 28 of Regulation (EU) 2016/679 (GDPR).

DATA CONTROLLER (CUSTOMER)**[Customer Organisation Name]**

Represented by its authorized officers.

As identified in the Hubfolio account registration.

DATA PROCESSOR (HUBFOLIO)**Space in the Making AB**

Corporate Reg. No: 559033-9825

Smedsbacksgatan 7, SE-115 39 Stockholm, Sweden

Contact: hello@hubfolio.ai

1. Parties and Roles

The Customer acts as Data Controller for the personal data entered into Hubfolio. Space in the Making AB acts as Data Processor and processes personal data strictly upon the Customer's documented instructions, solely for the purpose of delivering the Hubfolio software platform.

2. Purpose and Scope of Processing

The Processor shall process personal data solely to provide, maintain, and support the Hubfolio services: portfolio oversight, project and service management, tender packages and contractor bids, document management, milestone tracking, inbound invoice verification, workflow notifications, and human-in-the-loop AI assistance.

3. Categories of Data Subjects and Personal Data

Data subjects: Authorized user staff, client representatives, project managers, architectural consultants, general contractors, sub-contractors, and equipment suppliers.

Data categories: Full names, business email addresses, telephone numbers, employer company, role assignments, audit log entries, timestamped approvals, and any personal information voluntarily contained within uploaded architectural drawings, contracts, or site inspection photos. No special categories of data (GDPR Art. 9) are collected or required.

4. Confidentiality

The Processor ensures that all personnel authorized to process personal data have committed themselves to strict confidentiality agreements or are under an appropriate statutory obligation of confidentiality. Access is restricted strictly on a need-to-know basis.

5. Technical and Organizational Security Measures (TOMs)

The Processor implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including: (a) database-level multi-tenant separation (Row-Level Security) preventing cross-organisation data exposure; (b) mandatory Multi-Factor Authentication (MFA) for all system accounts; (c) encryption in transit (TLS 1.2 or higher, TLS 1.3 preferred) and AES-256 encryption at rest; (d) private object storage accessed exclusively through short-lived cryptographic URLs; and (e) immutable audit logging of critical actions and sign-offs.

6. Sub-processors and Notification Protocol

The Controller provides general authorization for the sub-processors listed in Schedule 1 below. The Processor shall notify the Controller by email at least thirty (30) days prior to engaging or replacing any sub-processor. The Controller retains the right to object on legitimate data protection grounds within this 30-day notice period.

7. International Data Transfers

Personal data is hosted within primary facilities situated in the European Union / European Economic Area. Any transfer outside the EU/EEA shall only take place under recognized adequacy decisions or the European Commission's Standard Contractual Clauses (SCCs), accompanied by supplementary technical safeguards.

8. Assistance with Data Subject Requests

Taking into account the nature of processing, the Processor assists the Controller through technical capabilities to respond to data subjects exercising their rights (access, rectification, erasure, restriction, and portability) and assists with Data Protection Impact Assessments (DPIAs) when required.

9. Personal Data Breach Management

The Processor shall notify the Controller without undue delay and at the latest within seventy-two (72) hours upon becoming aware of any confirmed personal data breach affecting the Controller's data, providing necessary forensic details to facilitate compliance with GDPR Articles 33 and 34.

10. Audits and Inspections

The Processor shall make available to the Controller all information necessary to demonstrate compliance with this DPA and contribute to reasonable security questionnaires or audits conducted by the Controller or an independent auditor mandated by the Controller, upon reasonable written notice.

11. Termination and Data Deletion Protocol

Upon termination of the underlying subscription, the Controller may export all project records and documentation. Within thirty (30) days following agreement termination, the Processor shall irrevocably delete or return all personal data from production systems, with automated backups purged in accordance with standard disaster recovery retention cycles, unless retention is mandated by applicable EU or Swedish statutory laws.

12. Governing Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of Sweden. Any dispute arising out of or in connection with this DPA shall be submitted to the exclusive jurisdiction of the Stockholm District Court (Stockholms tingsrätt).

SCHEDULE 1

Approved Sub-processors

Sub-processors authorized under Clause 6. All sub-processors are bound by GDPR Article 28 data protection terms.

ENTITY & INFRASTRUCTURE	FUNCTION	HOSTING LOCATION	SAFEGUARDS
Lovable Cloud (Amazon Web Services)	Application hosting, database, user accounts & file storage	EU (Ireland)	AES-256 at rest, TLS 1.2+ in transit, database-level access control
Cloudflare, Inc.	Website delivery, network security & DDoS protection	Global network, SCCs	TLS encryption; no storage of Hub content
Lovable Emails (with its email delivery provider)	Account & service email (invitations, sign-in codes, notifications)	EU/US, SCCs	Only recipient address and message content
Resend	Receiving supplier invoices sent to the Invoice inbox	US, SCCs	Only the received email and its attachments; signed delivery
Lovable AI Gateway	Routes AI requests to the model providers below	EU/US, SCCs	Only the document or text a user asks AI to read; retention per provider terms
Google (Gemini models)	AI-assisted document reading & suggestions	EU/US, SCCs	Only content sent for that request; client data not used to train models
OpenAI (GPT models)	AI-assisted document reading & suggestions	US, SCCs	Only content sent for that request; client data not used to train models

FOR THE DATA CONTROLLER:

Company:

Name:

Title:

AUTHORIZED SIGNATURE & DATE

FOR SPACE IN THE MAKING AB (PROCESSOR):

Company: **Space in the Making AB**

Name: **Helena Boberg**

Title: **Chief Executive Officer / Founder**

AUTHORIZED SIGNATURE & DATE