DATA PROCESSING AGREEMENT (DPA)

This Data Processing Agreement ("DPA") is entered into by and between:

Custodia RMS ("Processor") and the Customer (as defined in the Terms of Service) ("Controller").

This DPA is intended to ensure that the processing of personal data by the Processor is compliant with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1. Definitions

"Personal Data" means any information relating to an identified or identifiable natural person (e.g., names, emails, phone numbers).

"Processing" means any operation performed on personal data, such as collection, storage, analysis, or disclosure.

"Sub-processor" means a third-party service provider engaged by the Processor to perform parts of the Platform's services (e.g., hosting, email, analytics).

2. Scope and Purpose of Processing

The Controller engages the Processor to provide the Custodia RMS Platform. The Processor will process personal data provided by the Controller (or its staff/contractors) solely for the purpose of providing the Platform's management and compliance services, as described in the Terms of Service.

3. Obligations of the Processor

The Processor agrees to:

Instructions: Process personal data only on the documented instructions of the Controller.

Confidentiality: Ensure that all personnel authorised to process the data are bound by confidentiality obligations.

Security: Implement appropriate technical and organisational measures to protect data against unauthorised access, loss, or destruction (see Section 4).

Sub-processors**:** Maintain a list of Sub-processors. The Processor may engage Sub-processors to provide services but ensures that they provide the same level of data protection as required by this DPA.

Data Integrity**:** Ensure that the personal data remains accurate and kept up to date where provided by the Controller.

4. Technical and Organisational Measures

The Processor shall implement a combination of technical and organisational measures to ensure a level of security appropriate to the risk, including:

Encryption**:** Use of encryption for data in transit and at rest.

Access Control**:** Restricting access to personal data to only those employees who require it to perform their duties.

Regular Audits**:** Regular monitoring of security logs and infrastructure (Hetzner, Scaleway).

Data Breach Notification**:** The Processor shall notify the Controller without undue delay (and in no later than 48 hours) after becoming aware of any personal data breach that affects the Controller's data.

5. Data Subject Rights

The Processor will assist the Controller in responding to requests from "Data Subjects" (e.g., a staff member or tenant) who exercise their rights under the UK GDPR (such as the right to access, delete, or rectify their data), provided that the Controller remains responsible for the ultimate fulfilment of these requests.

6. Data Retention and Deletion

The Processor will retain personal data only for as long as necessary to provide the Platform services.

Upon termination of the service, the Processor will delete or return all personal data held on its systems, unless required by law to retain such data for a specific period.

The Controller is responsible for exporting their data (e.g., via the Platform's export tool) prior to account termination.

7. Audit Rights

The Processor shall make available to the Controller all information necessary to demonstrate compliance with this DPA and shall allow for and cooperate with the Controller's audits or inspections of the Platform's processing activities.

8. International Transfers

The Processor shall not transfer personal data outside the UK/EEA unless it ensures that the destination country has adequate data protection laws or uses standard contractual clauses (SCCs) approved by the UK government.