HAQQ INC.

TERMS OF SERVICE

&

PRIVACY POLICY

&

DATA PROCESSING AGREEMENT (DPA)

Table of Contents

BOOK I. INTRODUCTION & DEFINITIONS

A. Welcome

Welcome to the HAQQ legal technology and client relationship management ecosystem (the "Ecosystem"). Access and use of this Ecosystem and its modular services (each a "Product" or collectively the "Products") are governed by these Terms and Conditions (the "Terms").

HAQQ Inc. ("HAQQ", "Company", "we", "our") may amend these Terms at any time by posting updated versions on the Platform. Continued use constitutes binding acceptance. If you do not agree, you must immediately cease use.

These Terms apply to every visitor, registered User, Subscriber, and Beneficiary accessing the Ecosystem, whether as an individual practitioner, firm, or organizational license holder. By creating a MyHAQQ User ID, subscribing to any Product, or otherwise using the Services, you expressly acknowledge that you have read, understood, and agreed to be legally bound by these Terms and our Privacy and Data Protection Policies.

You further acknowledge and agree that:

1. The Ecosystem is provided as a modular and subscription-based set of services, each subject to the general provisions of these Terms and, where applicable, the specific provisions governing the Product in which you are enrolled.
2. Access to the Ecosystem does not grant you any ownership rights in its underlying software, code, trademarks, or proprietary materials, which remain exclusively vested in HAQQ and its licensors.
3. Your rights under these Terms are limited to a non-transferable, non-exclusive right to access and use the Ecosystem in accordance with the permitted purposes outlined herein.
4. The Ecosystem is designed to meet applicable professional, regulatory, and technical standards (including SOC2, GDPR, and other recognized frameworks), but the accuracy, completeness, and compliance of any Data or Content that you input remains your responsibility.
5. The Ecosystem is continually evolving. HAQQ may introduce new Products, discontinue or modify existing Products, or change the nature of services provided under the Ecosystem at its sole discretion, subject always to applicable law and fair notice requirements.

Your continued access and use of the Ecosystem signify your acceptance of these Terms as a binding contractual agreement between you and HAQQ.

B. Binding Effect

These Terms, together with the HAQQ Privacy Policy and any incorporated annexes, schedules, or supplemental agreements expressly referenced herein (collectively, the "Agreement"), constitute the entire, complete, and exclusive understanding and agreement between you, the registered user (the "User" or "you"), and HAQQ Inc. ("HAQQ", "Company", "we", "our") with respect to the subject matter hereof.

This Agreement supersedes and extinguishes all prior or contemporaneous proposals, communications, representations, warranties, negotiations, or agreements, whether oral, written, or implied, relating to the subject matter of the Ecosystem and the Services. No statement, promise, condition, inducement, or representation of any kind made by HAQQ or any of its representatives that is not expressly set forth in this Agreement shall be of any force or effect.

In the event of a conflict or inconsistency between these Terms and:

The HAQQ Privacy Policy, the provisions of the Privacy Policy shall prevail with respect to the collection, processing, and protection of Data;

Any annex, schedule, or Product-specific supplement, the terms of the annex, schedule, or supplement shall prevail with respect to the relevant Product, provided that such annex, schedule, or supplement expressly states that it modifies or overrides these Terms; and

Any separate written agreement duly executed between HAQQ and the User, the executed written agreement shall prevail with respect to the matters expressly covered therein.

The Agreement is binding upon you individually and, where you are acting on behalf of an organization, upon such organization as a legal entity. By accepting these Terms, you represent and warrant that you are duly authorized to bind such organization to this Agreement.

C. Definitions

Acceptable Use: The lawful and policy-compliant use of the Ecosystem.

Administrator Access: Elevated privileges to create, delete, or manage accounts.

Ecosystem: Collectively, all Products, modules, services, and features available from HAQQ.

Platform: The digital interface granting access to the Ecosystem.

Products: Functional components including MyHAQQ ID/Auth, Data Protection/Compliance, e-Firm, Legal AI, e-Client, Directory, Customization Services, Elite Support, and Data Migration.

Public Content: Expressive materials shared through public community and public social functions and made public by the owner of Public Content (posts, images, videos, forum entries, etc.).

Services: The functionalities and tools delivered under each Product.

Subscription Fees: Payments owed by you for use of the Products.

Third Party: Any individual or entity not a party to this agreement, including service providers, affiliates, regulators, or other Platform users.

User Data: All personal information, records, files, metadata, logs, and structured or unstructured information processed through the Platform, including personally identifiable information ("PII"), case/matter files, billing records, and CRM datasets.

Your Content: Public Content generated or uploaded by you.

BOOK II. MYHAQQ USER ID & AUTHENTICATION SERVICE

A. Registration & Eligibility

To access and utilize the Ecosystem and its Products, you must first register for a **MyHAQQ User ID**. Registration constitutes a legal act by which you agree to be bound by these Terms and, where applicable, to bind the organization you represent.

1. Age and Capacity Requirements
    a. You must be at least eighteen (18) years of age.
    b. You must have full legal capacity under the laws of your jurisdiction.
    c. Where you act on behalf of a company, firm, or institution, you warrant that you have the necessary authority to bind such entity to these Terms.
2. Accuracy of Registration Details
    a. You must provide complete, current, and accurate information, including your full legal name, verified email address, and any other details required by HAQQ.
    b. You agree to update such information promptly to ensure it remains accurate and complete at all times.
3. Verification and Authentication
    a. HAQQ may require you to undergo additional verification steps, which may include, without limitation: multi-factor authentication, identity document verification, or confirmation through professional credentials.
    b. Failure to complete verification requirements may result in restricted access or denial of registration.
4. Account Approval, Suspension, and Termination
    a. HAQQ reserves the right, in its sole discretion, to approve or reject any registration request without obligation to provide reasons.
    b. Accounts created with false, misleading, or incomplete information may be suspended or terminated without notice.
    c. HAQQ may also suspend or terminate accounts if the User has previously been banned from the Ecosystem or has violated these Terms.
5. Single Account Principle
    a. Unless explicitly permitted in writing by HAQQ, you may not create multiple accounts for the same individual or organization.
    b. Accounts are non-transferable and may not be assigned, licensed, or sold to third parties.
6. Assumption of Responsibility

a. You acknowledge and accept full responsibility for all activities conducted under your MyHAQQ User ID, regardless of whether such activities are authorized by you.
b. Any liability arising from misuse of your account, whether by you or by a third party to whom you granted access, shall rest solely with you.

BOOK III. DATA PROTECTION, HOSTING & COMPLIANCE

A. General Principles

HAQQ acknowledges the fundamental importance of privacy, confidentiality, and data security in the provision of its Services. To that end, HAQQ is committed to processing all Data in strict compliance with the principles and obligations imposed by: (i) the European Union's General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"); (ii) the Lebanese Law No. 81 of 2018 on Electronic Transactions and Personal Data ("Lebanese Data Protection Law"); (iii) recognized industry standards including but not limited to the American Institute of Certified Public Accountants (AICPA) SOC2 framework; and (iv) any other applicable data protection and privacy legislation in the jurisdictions in which HAQQ operates (collectively, the "Applicable Data Protection Laws").

For purposes of these Terms:

1. Roles of the Parties
    a. You, as the User, determine the purposes and means of processing Data entered into or generated within the Ecosystem. Accordingly, you shall be regarded as the **Data Controller**.
    b. HAQQ processes Data on your behalf strictly in accordance with your instructions, except as otherwise required by Applicable Data Protection Laws. HAQQ shall therefore be regarded as the **Data Processor**.
    c. In circumstances where HAQQ determines purposes and means of processing Data for its own legitimate business operations (such as billing, fraud detection, internal product development, or compliance with legal obligations), HAQQ shall act as an **Independent Controller** for such processing activities.
2. Processing Principles

    HAQQ processes Data in accordance with the following principles, each of which mirrors the requirements of GDPR Article 5 and SOC2 Trust Services Criteria:

    a. **Lawfulness, Fairness and Transparency**: Data is processed on a lawful basis, communicated transparently through these Terms and our Privacy Policy.
    b. **Purpose Limitation**: Data is collected and processed only for specified, explicit, and legitimate purposes communicated to you, and not further processed in a manner incompatible with those purposes.
    c. **Data Minimization**: Data collected is limited to what is adequate, relevant, and necessary in relation to the purposes for which it is processed.

d. **Accuracy**: Reasonable measures are taken to ensure Data is accurate and, where necessary, kept up to date.
e. **Storage Limitation**: Data is retained no longer than necessary for the purposes set forth in these Terms, unless longer retention is required by law.
f. **Integrity and Confidentiality**: Data is processed in a manner ensuring appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, using technical and organizational measures aligned with SOC2 controls.
g. **Accountability**: HAQQ maintains records, policies, and audit trails evidencing its compliance with Applicable Data Protection Laws.

3. Processor Obligations

HAQQ undertakes, as Data Processor:

a. To process Data only on documented instructions from you, the Controller, including with respect to international transfers, unless required to do so by law;
b. To ensure persons authorized to process Data are bound by confidentiality obligations;
c. To implement and maintain appropriate technical and organizational security measures in line with SOC2 and ISO 27001;
d. To assist you in fulfilling your obligations to respond to data subject rights requests under GDPR and equivalent laws;
e. To notify you without undue delay of any personal data breach;
f. To make available information necessary to demonstrate compliance and to allow for audits in accordance with Section 3.11.

4. User (Controller) Obligations:

As Controller, you undertake:

a. To ensure that all Data you submit to the Ecosystem has been collected lawfully and with appropriate consents or legal bases;
b. To comply with your obligations toward data subjects under Applicable Data Protection Laws, including informing them of how their Data will be processed through HAQQ;
c. To refrain from using the Ecosystem to process categories of Data not permitted under law (including sensitive data such as biometric identifiers or health records) unless HAQQ has explicitly agreed in writing to such processing;
d. To indemnify HAQQ for any claims, fines, or liabilities arising from your failure to comply with these obligations.

5. Cross-Jurisdictional Application

Given the cross-border nature of the Ecosystem, Users acknowledge that Data may be processed in multiple jurisdictions, including outside their country of residence. HAQQ ensures that all such transfers are protected by adequate safeguards, including but not limited to Standard Contractual Clauses (SCCs) adopted by the European Commission, or equivalent legal frameworks in other jurisdictions.

B. Categories of Data Processed

For the purposes of fulfilling its obligations under these Terms and in the ordinary course of providing the Ecosystem and its Products, HAQQ may process the following categories of Data on behalf of the User:

1. Identity Data
    a. Includes personal identifiers such as first and last names, residential and business addresses, telephone numbers, verified email addresses, government-issued identification numbers (including but not limited to passports, national identity cards, bar association IDs, and professional license numbers), and other identifiers reasonably necessary to establish or verify User identity.
2. Professional Data
    a. Includes information relating to the User's professional status and affiliations, such as educational background, certifications, professional licenses, job titles, organizational roles, firm or employer details, practice areas, bar membership, and other professional identifiers.
3. Case and Matter Files
    a. Includes any legal documents, contracts, pleadings, memoranda, case evidence, client communications, discovery materials, exhibits, or similar records uploaded, generated, or stored by the User in connection with case or matter management within the Ecosystem.
    b. The User acknowledges that HAQQ does not determine the content of such files and disclaims all liability for the lawfulness, accuracy, or completeness of such data, which remains solely the User's responsibility as Controller.
4. CRM Data
    a. Includes client and contact information, relationship management records, billing and invoicing data, timekeeping entries, matter notes, correspondence logs, interaction histories, and related customer relationship management details maintained within the Ecosystem.
5. Authentication Data
    a. Includes usernames, hashed passwords, credential tokens, multi-factor authentication ("MFA") secrets or confirmations, security challenge responses, and session identifiers generated or required for the purpose of granting and managing access to the Ecosystem.

b. Authentication Data is subject to encryption both in transit and at rest in accordance with HAQQ's SOC2-compliant security measures.

6. System Metadata
    a. Includes automatically collected technical information such as Internet Protocol (IP) addresses, browser types, device identifiers, operating system versions, access dates and times, geographic location data derived from IP or device, log files, error logs, activity trails, and performance diagnostics.
    b. Such metadata is collected for the purposes of ensuring platform security, improving system performance, generating anonymized analytics, and complying with applicable regulatory or audit obligations.
7. Special Categories of Data
    a. HAQQ does not intentionally collect or process special categories of personal data as defined under Article 9 of the GDPR, including but not limited to data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric identifiers, health information, or data concerning sex life or sexual orientation.
    b. If the User elects to input such special categories of data into the Ecosystem in connection with Case and Matter Files or other functionalities, the User acknowledges and agrees that:
        i. the User, as Controller, remains solely responsible for ensuring an adequate legal basis for processing such data under Applicable Data Protection Laws; and
        ii. HAQQ shall implement appropriate security measures but disclaims liability for processing such data absent explicit written agreement authorizing such processing.
8. Derived Data
    a. Includes data generated by HAQQ's systems as a byproduct of processing User inputs, such as anonymized usage statistics, aggregated performance metrics, or system learning models (including outputs used to improve AI functionalities within the Ecosystem).
    b. Derived Data shall be deemed the property of HAQQ, provided always that it is irreversibly anonymized and does not identify the User or any data subject.

C. Purposes of Processing

HAQQ processes Data exclusively for the following purposes, each of which shall be deemed lawful, necessary, and proportionate under Applicable Data Protection Laws:

1. Account Registration and Authentication
    a. To establish and maintain a MyHAQQ User ID, verify identity, and authenticate credentials.

   b. Lawful Basis: Processing is necessary for the performance of a contract to which the User is party (GDPR Art. 6(1)(b)), and for HAQQ's legitimate interest in ensuring secure access control.
2. Service Provision Across All Products
   a. To deliver functionalities of the Ecosystem including, without limitation, e-Firm case management, Legal AI advisory tools, e-Client communications, Directory listings, Customization Services, Elite Support, and Data Migration.
   b. Lawful Basis: Processing is necessary for the performance of a contract (GDPR Art. 6(1)(b)).
3. Client Relationship Management (CRM)
   a. To enable Users to manage client relationships, maintain contact records, track interactions, and support professional workflows within the Ecosystem.
   b. Lawful Basis: Processing is necessary for the legitimate interests of Users in managing client relations (GDPR Art. 6(1)(f)) and for the performance of a contract.
4. Billing and Subscription Management
   a. To generate invoices, process payments, manage subscriptions, and enforce applicable fees or taxes.
   b. Lawful Basis: Processing is necessary for the performance of a contract and to comply with legal obligations related to accounting and taxation (GDPR Art. 6(1)(b) and 6(1)(c)).
5. Security Monitoring and Incident Response
   a. To detect, prevent, investigate, and respond to unauthorized access, misuse, fraudulent activity, or security incidents affecting the Ecosystem.
   b. Lawful Basis: Processing is necessary for HAQQ's legitimate interests in ensuring the integrity and security of its systems (GDPR Art. 6(1)(f)) and to comply with legal obligations relating to information security and breach notification (GDPR Art. 6(1)(c)).
6. Compliance with Legal and Regulatory Obligations
   a. To comply with statutory, regulatory, and professional obligations, including anti-money laundering (AML), counter-terrorism financing (CTF), sanctions compliance, tax reporting, court orders, and requests from competent authorities.
   b. Lawful Basis: Processing is necessary for compliance with a legal obligation (GDPR Art. 6(1)(c)).
7. Continuous Product Improvement and AI Training
   a. To improve the performance, reliability, and features of the Ecosystem, including training and refinement of Legal AI tools.

b. Data used for this purpose is aggregated, pseudonymized, or anonymized to ensure it cannot reasonably be linked back to an identifiable User or data subject.
c. Lawful Basis: Processing is based on HAQQ's legitimate interests in developing and enhancing its services (GDPR Art. 6(1)(f)), subject always to strict safeguards ensuring data minimization and anonymization.

8. Support and Troubleshooting
    a. To provide technical support, resolve service issues, and handle user inquiries.
    b. Lawful Basis: Processing is necessary for the performance of a contract (GDPR Art. 6(1)(b)).
9. Audit, Risk, and Compliance Assurance
    a. To maintain records, generate audit trails, and produce evidence of compliance with SOC2, GDPR, and other regulatory frameworks.
    b. Lawful Basis: Processing is necessary for compliance with legal obligations and for HAQQ's legitimate interests in upholding industry standards (GDPR Art. 6(1)(c) and 6(1)(f)).

D. Lawful Basis

All processing of Data within the Ecosystem shall be undertaken in strict conformity with Applicable Data Protection Laws and shall be grounded on one or more of the following lawful bases:

1. Performance of a Contract
    a. Processing is necessary for the conclusion and performance of the contractual relationship between HAQQ and the User.
    b. This includes, without limitation, activities required for account registration, authentication, provision of Products and Services, subscription management, billing, and technical support.
    c. Where processing is required for the fulfillment of these Terms, refusal to provide the necessary Data may prevent HAQQ from delivering the Services or may render continued use of the Ecosystem impossible.
2. Compliance with Legal Obligations
    a. Processing may be necessary for HAQQ to comply with mandatory legal and regulatory requirements to which it is subject, including but not limited to:
        i. Record-keeping, tax, and financial reporting obligations;
        ii. Obligations relating to anti-money laundering (AML), counter-terrorism financing (CTF), and sanctions compliance;
        iii. Statutory data retention requirements under Lebanese law or other applicable regimes;

iv. Responding to lawful requests from courts, regulators, or other competent authorities.

b. Where such obligations exist, HAQQ shall process Data only to the extent necessary to achieve compliance and shall notify the User, unless prohibited by law, of any legally binding request for disclosure.

3. Legitimate Interests
   a. Processing may be carried out on the basis of HAQQ's legitimate interests, provided such interests are not overridden by the fundamental rights and freedoms of data subjects.
   b. Legitimate interests include, but are not limited to:
      i. Ensuring the security, integrity, and availability of the Ecosystem;
      ii. Preventing fraud, misuse, or unauthorized access;
      iii. Monitoring performance and usage patterns to ensure stable and reliable services;
      iv. Protecting HAQQ's legal rights and enforcing these Terms;
      v. Improving and innovating HAQQ's Products and Services, provided any Data used for such improvement is fully anonymized or pseudonymized possible.
   c. Users may object to processing based on legitimate interests by submitting a request to **info@haqq.ai**, in which case HAQQ will assess whether its compelling interests override the User's objection.
4. Consent
   a. In limited circumstances, HAQQ may rely on the explicit consent of the User or relevant data subjects.
   b. Consent will only be sought where processing cannot be justified under any of the other lawful bases described herein. Examples include, but are not limited to:
      i. Activation of optional features (e.g., AI personalization modules, integration with third-party marketing or analytics tools);
      ii. Participation in voluntary surveys, research, or pilot programs;
      iii. Use of Cookies and similar technologies for non-essential tracking or profiling.
   c. Where consent is the lawful basis:
      i. HAQQ will ensure that such consent is freely given, specific, informed, and unambiguous;
      ii. Users may withdraw consent at any time, without prejudice to the lawfulness of processing carried out prior to withdrawal;
      iii. Withdrawal of consent may affect the availability of certain optional features but shall not affect the general availability of the Ecosystem.

E. Data Subject Rights

In accordance with Applicable Data Protection Laws, including but not limited to the GDPR and the Lebanese Data Protection Law, Users and data subjects whose Data is processed through the Ecosystem retain the following rights. HAQQ shall facilitate the exercise of these rights in cooperation with the User (as Controller) and subject to the terms of this Agreement:

1. Right of Access
    - Data subjects have the right to obtain confirmation as to whether or not their Data is being processed and, if so, to access such Data together with information regarding:
        - The categories of Data processed;
        - The purposes of processing;
        - The recipients or categories of recipients to whom Data has been or will be disclosed;
        - The envisaged period for which the Data will be stored; and
        - The existence of rights available to the data subject under this Section.
2. Right of Rectification
    - Data subjects have the right to request the correction of inaccurate or incomplete Data.
    - Users, as Controllers, bear the primary obligation to ensure Data input into the Ecosystem is accurate and up to date. HAQQ shall, upon instruction, promptly implement corrections requested by the User.
3. Right to Erasure ("Right to be Forgotten")
    - Data subjects may request the deletion of their Data where:
        - The Data is no longer necessary for the purposes for which it was collected;
        - Consent (where applicable) has been withdrawn;
        - Processing is unlawful; or
        - Erasure is required to comply with a legal obligation.
    - HAQQ shall execute such requests only upon the documented instruction of the User, except where HAQQ acts as Independent Controller in respect of its own processing obligations.
4. Right to Restriction of Processing
    - Data subjects may request the temporary suspension of processing where:
        - The accuracy of the Data is contested;
        - The processing is unlawful but the data subject opposes erasure;
        - The User no longer requires the Data but it is needed for legal claims; or

        - The data subject has objected to processing and verification is pending.
    - During the restriction period, HAQQ will limit processing to secure storage only, except where otherwise legally required.
5. Right to Data Portability
    - Data subjects have the right to receive a copy of their Data in a structured, commonly used, and machine-readable format and to transmit such Data to another controller.
    - HAQQ shall provide the technical means for export or transfer of Data, provided such request is lawful, feasible, and does not infringe upon the rights of other data subjects.
6. Right to Object to Processing
    - Data subjects may object, on grounds relating to their particular situation, to the processing of their Data where processing is based on legitimate interests.
    - HAQQ shall cease such processing unless compelling legitimate grounds override the interests, rights, and freedoms of the data subject, or unless processing is necessary for legal claims.
7. Right to Withdraw Consent
    - Where processing is based on consent, data subjects may withdraw such consent at any time without affecting the lawfulness of prior processing.
    - Withdrawal may limit access to optional features but shall not affect core contractual services.
8. Right to Lodge a Complaint
    - Data subjects have the right to lodge a complaint with a competent supervisory authority in their jurisdiction if they believe that their Data has been processed in violation of Applicable Data Protection Laws.

Requests Procedure

- All data subject rights requests must be submitted in writing to **info@haqq.ai** (or such successor address as HAQQ may designate).
- HAQQ will acknowledge receipt of the request and coordinate with the User, as Controller, to facilitate compliance.
- HAQQ shall respond to requests without undue delay and in any event within thirty (30) calendar days of receipt. Where the request is complex or numerous, this period may be extended by a further sixty (60) days, provided notice of such extension is given within the initial thirty (30) days.
- HAQQ may require reasonable proof of identity prior to fulfilling any request.
- HAQQ reserves the right to charge a reasonable administrative fee for repetitive, manifestly unfounded, or excessive requests.

F. Sub-Processors

1. Authorization to Engage Sub-Processors
    a. The User acknowledges and expressly authorizes HAQQ to engage third-party Sub-Processors in connection with the provision of the Ecosystem and its Products. Sub-Processors may include, without limitation, providers of cloud hosting infrastructure, data storage, payment processing, analytics, customer support systems, communications tools, and other ancillary services reasonably necessary for the operation of the Ecosystem.
2. Selection and Due Diligence
    a. HAQQ shall exercise due diligence in the selection of all Sub-Processors, ensuring that they are reputable entities offering sufficient guarantees to implement appropriate technical and organizational measures so that the processing of Data will meet the requirements of Applicable Data Protection Laws, including GDPR and Lebanese Data Protection Law.
3. Contractual Safeguards
    a. Each subprocessor engaged by HAQQ shall be bound by a written agreement imposing obligations that are no less protective than those imposed on HAQQ under these Terms. Such agreements shall, at a minimum, require Sub-Processors to:
        i. Process Data only on documented instructions from HAQQ and for no other purpose;
        ii. Maintain confidentiality obligations equivalent to those set forth herein;
        iii. Implement industry-standard security measures aligned with SOC2 and ISO 27001;
        iv. Assist HAQQ in meeting its obligations under Applicable Data Protection Laws, including incident response and data subject rights facilitation;
        v. Delete or return Data upon termination of services, unless retention is required by law.
4. Transparency and Subprocessor List
    a. HAQQ shall maintain and make available to Users, upon written request to **info@haqq.ai**, an up-to-date list of current Sub-Processors, including their name, location, and the nature of services provided.
    b. HAQQ shall provide Users with notice of the engagement of any new subprocessor. Such notice may be provided through email, the Platform, or other reasonable means.
5. User's Right to Object
    a. Users may object in good faith to the appointment of a new subprocessor by notifying HAQQ in writing within fifteen (15) days of receiving notice.

b. In the event of an objection, HAQQ will work with the User in good faith to address the concern, which may include replacing the subprocessor or providing alternative technical solutions.
c. If no resolution is achieved within thirty (30) days, the User may terminate the affected Product or Service without penalty.

6. Liability for Sub-Processors
   a. HAQQ shall remain fully liable to the User for the acts and omissions of its Sub-Processors to the same extent HAQQ would be liable if performing the services itself under these Terms.

G. Data Security Measures

1. Commitment to Security Standards
   a. HAQQ shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk presented by the processing of Data. These measures are designed to protect Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Data, in accordance with SOC2 Trust Services Criteria, ISO/IEC 27001, and Applicable Data Protection Laws, including GDPR Article 32.
2. Core Security Controls

   Without limitation, HAQQ's security measures shall include:

   a. **Encryption in Transit and at Rest**: All Data transmitted over public networks is encrypted using Transport Layer Security (TLS 1.2 or higher). Stored Data is encrypted using industry-standard AES-256 or equivalent. Encryption keys are managed in accordance with best practices and subject to access controls.
   b. **Network Segmentation and Firewalls**: The production environment is logically segregated from corporate networks, with firewalls and intrusion detection/prevention systems (IDS/IPS) in place to limit unauthorized access.
   c. **Regular Vulnerability Testing and Audits**: HAQQ conducts periodic internal and external vulnerability scans, penetration testing, and annual SOC2/ISO audits. Identified vulnerabilities are tracked, prioritized, and remediated in accordance with HAQQ's risk management policies.
   d. **Role-Based Access Control (RBAC)**: Access to Data is strictly limited to personnel with a demonstrable business need. Privileges are granted on a least-privilege basis, reviewed regularly, and revoked immediately upon role change or termination of employment.

e. **Incident Detection and Response Protocols**: HAQQ maintains 24/7 monitoring of critical systems. Security incidents are managed under a documented incident response plan that includes triage, containment, investigation, remediation, and user notification (where required by law).

3. Personnel and Confidentiality
    a. All HAQQ employees, contractors, and authorized personnel with access to Data are bound by confidentiality obligations under contract.
    b. Personnel receive regular training on data protection, cybersecurity, and incident response.
4. Business Continuity and Disaster Recovery
    a. HAQQ maintains documented and tested business continuity and disaster recovery (BC/DR) plans.
    b. Data backups are encrypted and stored in geographically redundant locations. Recovery testing is conducted at least annually.
5. Physical and Environmental Security
    a. Data centers hosting the Ecosystem are managed by leading cloud providers certified under ISO/IEC 27001, SOC1/SOC2, and equivalent frameworks.
    b. Physical access to facilities is restricted through multi-factor authentication, biometric screening, and 24/7 monitoring.
6. Audit and Verification
    a. HAQQ regularly reviews and updates its security practices to address emerging threats.
    b. Upon written request and subject to confidentiality obligations, HAQQ shall provide Users with summaries of relevant SOC2, ISO/IEC 27001, or other certification reports as evidence of compliance.
7. User Responsibilities
    a. The User acknowledges that the security of Data also depends on the User's configuration of the Ecosystem and safeguarding of authentication credentials.
    b. The User agrees to implement appropriate measures within its own organization, including secure passwords, access governance, and endpoint protection.

H. Breach Notification

1. Definition and Threshold
    a. A "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Data transmitted, stored, or otherwise processed in the Ecosystem.

b. HAQQ shall assess without undue delay whether a detected security incident constitutes a Personal Data Breach under Applicable Data Protection Laws and whether it is likely to result in a risk or a high risk to the rights and freedoms of natural persons.

2. Processor-to-Controller Notice (Primary Obligation)
   a. Upon becoming aware of a Personal Data Breach affecting Data for which the User is Controller, HAQQ will **notify the User without undue delay and, where feasible, within seventy-two (72) hours**. "Becoming aware" means the point at which HAQQ has a reasonable degree of certainty that a breach has occurred and that it has impacted Data processed for the User.
   b. If notification is not made within seventy-two (72) hours, it shall be accompanied by reasons for the delay.
3. Content of Notification

   HAQQ's notification will include, to the extent known at the time and as information becomes available on a rolling basis:

   a. **Nature of the breach**: categories and approximate volume of data subjects and records concerned;
   b. Likely consequences of the breach;
   c. **Measures taken or proposed** by HAQQ to address and mitigate the breach (including containment, remediation, and recovery steps);
   d. Contact point for further information: HAQQ's privacy office at info@haqq.ai;
   e. **Recommendations** for the User to mitigate possible adverse effects.
4. User's Responsibility to Notify Supervisory Authorities and Data Subjects
   a. As Controller, the User bears primary responsibility for assessing whether notification to supervisory authorities and/or communication to data subjects is required under GDPR Articles 33–34 or other Applicable Data Protection Laws.
5. HAQQ shall **assist** the User in meeting these obligations by providing relevant breach facts, logs, and remedial details reasonably available to HAQQ.
6. Direct Regulator and Data Subject Notice by HAQQ
   a. Where Applicable Data Protection Laws impose a **direct** notification obligation on a Processor, or where HAQQ acts as an **Independent Controller** for specific processing (e.g., billing, fraud prevention), HAQQ will notify the competent supervisory authority and, where required, affected data subjects **without undue delay and, where feasible, within seventy-two (72) hours** after becoming aware of the breach.

b. Communications to data subjects will be made in clear and plain language and will describe the nature of the breach, likely consequences, and measures taken or proposed to address it.

7. High-Risk Communications to Data Subjects
    a. Where the Personal Data Breach is likely to result in a **high risk** to the rights and freedoms of natural persons, HAQQ will support the User in drafting and, if agreed or required by law, issuing communications to affected data subjects **without undue delay**.
8. The obligation to communicate to data subjects shall **not** apply if any of the following conditions are met:
    a. HAQQ has implemented appropriate technical and organizational protection measures (such as effective encryption) that render the Data unintelligible to any person not authorized to access it;
    b. HAQQ has taken subsequent measures that ensure the high risk is no longer likely to materialize; or
    c. Such communication would involve disproportionate effort, in which case a public communication or similar equally effective measure shall be made.
9. Incident Management, Forensics, and Preservation
    a. HAQQ maintains a documented incident response plan covering triage, containment, eradication, recovery, and post-incident review.
    b. HAQQ will preserve relevant system logs and evidence for forensic analysis and legal compliance, subject to applicable retention rules and chain-of-custody controls.
    c. HAQQ will provide reasonable cooperation to the User's auditors, regulators, or appointed forensic experts under appropriate confidentiality undertakings and subject to security and operational constraints.
10. Ongoing Updates and Final Report
    a. Where not all information can be provided at the same time, HAQQ will provide information in phases as it becomes available.
    b. Upon closure of the incident, HAQQ will provide the User with a **final incident report** summarizing root cause (where ascertainable), scope of impact, remedial measures taken, and recommended improvements.
11. User's Duty to Notify HAQQ of Suspected Incidents
    a. The User shall promptly notify HAQQ at **info@haqq.ai** upon discovering or reasonably suspecting any incident, vulnerability, credential compromise, or anomaly that may affect the Ecosystem or Data processed by HAQQ.

b. The User shall cooperate in good faith with HAQQ's investigation, including by supplying relevant details, indicators of compromise, and contact points.

12. No Admission of Fault; Mitigation
    a. Any notification by HAQQ shall not be construed as an admission of fault or liability.
    b. Parties shall use commercially reasonable efforts to **mitigate** adverse effects and prevent further or future incidents, including implementing agreed corrective actions without undue delay.
13. Records of Breaches
    a. HAQQ will maintain an internal **breach register** documenting the facts relating to the breach, its effects, and remedial action taken, in accordance with GDPR Article 33(5) and SOC2 requirements.
    b. Summaries or attestations may be made available to the User upon written request, subject to confidentiality and security restrictions.
14. Costs
    a. Each Party shall bear its own costs associated with breach management and notification, except where the breach is primarily caused by the other Party's breach of this Agreement or Applicable Data Protection Laws, in which case the responsible Party shall bear reasonable and demonstrable costs arising therefrom, without prejudice to other remedies available under this Agreement or at law.

I. Data Retention & Deletion

1. Retention Principle
    a. HAQQ shall retain Data only for as long as necessary to fulfill the contractual purposes for which it was collected, to comply with legal and regulatory obligations, to resolve disputes, and to enforce these Terms.
    b. Data shall not be kept in a form which permits identification of data subjects for longer than is necessary in relation to the purposes for which it is processed.
2. Standard Retention Period
    a. Unless otherwise required by Applicable Data Protection Laws, all User Data shall be permanently deleted or anonymized within **ninety (90) days** following the effective termination or expiration of the User's subscription.
    b. During this ninety-day period, the User may request retrieval or export of their Data. HAQQ shall provide reasonable technical means for such export, subject to applicable fees and security requirements.
3. Legal and Regulatory Retention

a. Where Applicable Data Protection Laws or other statutory obligations impose mandatory retention periods (including, but not limited to, financial, tax, audit, anti-money laundering, or litigation hold requirements), HAQQ shall retain relevant Data strictly for the duration required by law and shall ensure such Data remains subject to appropriate technical and organizational protections.
b. Upon expiry of such statutory retention period, the Data shall be securely deleted or anonymized without further notice.

4. Backups and Disaster Recovery Copies
   a. Data may persist in encrypted backup or disaster recovery archives for a period not exceeding **one (1) year** from termination.
   b. Access to such backup Data shall be strictly restricted to authorized personnel with a demonstrable need, and restoration shall occur only for the purposes of disaster recovery or continuity of operations.
   c. Backup copies containing User Data shall be overwritten or securely destroyed in accordance with HAQQ's data sanitization policies and SOC2-compliant lifecycle management standards.
5. Derived and Anonymized Data
   a. HAQQ reserves the right to retain anonymized or aggregated datasets, usage statistics, and performance metrics derived from User Data beyond the retention periods specified herein, provided such datasets are irreversibly anonymized and no longer constitute personal data within the meaning of Applicable Data Protection Laws.
6. Early Deletion at User's Request
   a. The User may request earlier deletion of Data during the subscription term or prior to the expiration of the ninety-day period.
   b. HAQQ shall comply with such requests provided that:
   (i) the request does not conflict with legal or regulatory retention obligations; and
   (ii) the User acknowledges that early deletion may impact service continuity and availability.
7. Certification of Deletion
   a. Upon written request, HAQQ shall provide the User with a confirmation or certificate of deletion, evidencing that Data has been securely and irreversibly deleted in accordance with industry standards.
8. Allocation of Responsibility
   a. The User acknowledges responsibility for exporting and maintaining independent copies of Data it requires beyond the retention period.

b. HAQQ shall not be liable for any loss of Data resulting from the expiration of the retention period or deletion conducted in accordance with this Section.

J. International Transfers

1. Principle of Restricted Transfers
    a. HAQQ acknowledges that transfers of Data originating from the European Economic Area ("EEA"), the United Kingdom ("UK"), or any jurisdiction with equivalent cross-border data transfer restrictions may only occur where adequate safeguards are in place to protect the fundamental rights and freedoms of data subjects in accordance with Applicable Data Protection Laws.
2. Adequacy Decisions
    a. Where the European Commission, the UK Secretary of State, or another competent authority has recognized a third country, territory, or sector as providing an adequate level of protection for personal data, HAQQ may rely on such adequacy decision as the lawful basis for transfer.
3. Standard Contractual Clauses (SCCs) and UK Addenda
    a. In the absence of an adequacy decision, HAQQ shall ensure that transfers are governed by the **Standard Contractual Clauses (SCCs)** approved by the European Commission or, where applicable, the International Data Transfer Addendum issued by the UK Information Commissioner's Office.
    b. The SCCs shall be executed between HAQQ (as Processor or Controller, as applicable) and its Sub-Processors or affiliates located outside the EEA/UK.
4. Supplementary Measures
    a. Where required by law or supervisory guidance (including the European Data Protection Board's recommendations), HAQQ shall implement additional technical, contractual, and organizational measures to ensure transferred Data is afforded a level of protection essentially equivalent to that guaranteed within the EEA/UK. Such measures may include:
        i. End-to-end encryption with keys retained solely under HAQQ's control;
        ii. Data pseudonymization prior to transfer;
        iii. Enhanced contractual obligations on foreign recipients regarding government access requests; and
        iv. Regular assessments of the legal environment of the recipient jurisdiction.
5. Other Transfer Mechanisms

a. In limited circumstances, HAQQ may rely on other derogations permitted under GDPR Article 49 or equivalent provisions of Applicable Data Protection Laws, such as explicit consent, necessity for contract performance, or establishment, exercise, or defense of legal claims. Such reliance will occur only where strictly necessary and shall be documented.

6. Transparency and User Notification
    a. HAQQ shall maintain an up-to-date record of jurisdictions in which Data may be processed and shall make such information available to Users upon written request to **info@haqq.ai**.
    b. Where HAQQ intends to newly transfer Data to a country without an adequacy decision and relying on SCCs or equivalent safeguards, HAQQ will notify Users in advance, unless Applicable Law prohibits such notice on public interest grounds.
7. Sub-Processor Transfers
    a. Where Sub-Processors are engaged to process Data outside the EEA/UK, HAQQ shall ensure that such Sub-Processors are contractually bound by SCCs or equivalent safeguards prior to the commencement of processing.
    b. HAQQ shall remain fully liable to the User for the compliance of such Sub-Processors with applicable cross-border transfer obligations.
8. Ongoing Assessment
    a. HAQQ shall regularly review the legal frameworks governing jurisdictions in which Data is processed to ensure that transfer mechanisms remain valid and effective.
    b. Where a transfer mechanism is invalidated (e.g., by judicial or regulatory decision), HAQQ will promptly implement alternative lawful safeguards or, if no such safeguard can be applied, suspend the transfer until lawful arrangements are established.

K. Audit Rights

1. Access to Reports
    a. Enterprise Subscribers may, upon providing reasonable written notice to HAQQ, request access to summaries of HAQQ's most recent **SOC2 Type II**, **ISO/IEC 27001**, or equivalent third-party audit reports (collectively, "Audit Reports").
    b. Such Audit Reports shall serve as primary evidence of HAQQ's compliance with its security, confidentiality, and processing obligations under these Terms.
2. Independent Third-Party Certifications

a. HAQQ conducts regular audits by accredited independent third parties. These audits cover the design and operational effectiveness of technical and organizational measures relating to security, availability, processing integrity, confidentiality, and privacy.
b. The results of such audits, together with any certifications achieved, shall be made available to Users as evidence of compliance, subject always to confidentiality and intellectual property restrictions.

3. On-Site and Remote Audits
    a. In exceptional cases where Audit Reports are insufficient to satisfy a User's regulatory obligations, HAQQ may permit the User or its designated independent auditor to conduct a direct audit of HAQQ's relevant data processing facilities, systems, and controls.
    b. Any such audit shall be:
        i. limited in scope to Data processing activities relevant to the User;
        ii. conducted no more than once annually, unless otherwise required by law;
        iii. subject to at least sixty (60) days' prior written notice;
        iv. performed during normal business hours without disrupting HAQQ's operations; and
        v. carried out under strict confidentiality undertakings agreed in advance.
4. Confidentiality and Security Safeguards
    a. All information obtained through an audit, including Audit Reports, system descriptions, and test results, shall be treated as HAQQ's **Confidential Information** and subject to the confidentiality provisions of these Terms.
    b. HAQQ may redact portions of Audit Reports or restrict access to certain facilities or materials where necessary to protect the confidentiality, security, or integrity of HAQQ's systems, or where disclosure would infringe the rights of other Users or third parties.
5. Costs of Audits
    a. Each Party shall bear its own costs relating to any audit.
    b. Where an audit is requested more frequently than once per year without a legal obligation requiring such frequency, or where an audit imposes disproportionate costs on HAQQ, HAQQ reserves the right to charge the User for reasonable, demonstrable expenses incurred in accommodating the audit.
6. Regulatory Access

a. Nothing in this Section shall restrict or prevent HAQQ from cooperating with legally binding inspections or audits conducted by competent supervisory authorities, regulators, or courts.
b. Where permissible, HAQQ shall notify the User of such inspections if and when they relate to the User's Data.

L. Compliance Certifications

1. Maintenance of Certifications
    a. HAQQ shall maintain and periodically renew certifications and attestations from independent third-party auditors demonstrating compliance with recognized industry standards, including but not limited to the **AICPA SOC2 Type II** framework and, where applicable, **ISO/IEC 27001** or equivalent certifications relating to information security management systems.
    b. Such certifications shall be updated in accordance with the audit cycles prescribed by the relevant standard or certifying body.
2. Audit Trails and Records of Processing
    a. HAQQ shall maintain detailed internal audit trails, system logs, and records of processing activities sufficient to demonstrate compliance with its obligations under these Terms and Applicable Data Protection Laws, including GDPR Article 30.
    b. These records shall be preserved in accordance with HAQQ's retention policies and made available to competent supervisory authorities upon lawful request.
3. Evidence of Compliance
    a. Upon written request by a User, and subject to confidentiality and security restrictions, HAQQ shall make available **evidence of compliance**, which may include:
        i. Executive summaries of SOC2 Type II audit reports;
        ii. ISO/IEC 27001 certificates and scope statements;
        iii. Data protection impact assessments (DPIAs) or risk assessments relevant to the Ecosystem; and
        iv. Internal policy summaries and attestations regarding technical and organizational measures.
4. Nondisclosure Agreement Requirement
    a. Access to full or partial audit reports, certifications, or compliance evidence shall be conditioned upon the User's execution of a **mutual nondisclosure agreement (NDA)** with HAQQ.
    b. HAQQ reserves the right to redact or withhold information where disclosure would compromise security, expose proprietary information, or infringe the rights of third parties.

5. Reliance by Users
    a. Users may reasonably rely on the certifications and compliance evidence provided by HAQQ as proof of HAQQ's adherence to industry standards and regulatory requirements.
    b. Such reliance does not relieve the User, in its capacity as Controller, of its independent obligations under Applicable Data Protection Laws to assess and ensure the adequacy of processors engaged to process personal data.
6. Updates and Notifications
    a. HAQQ shall notify Users, through the Platform or by other reasonable means, of material changes in the status of its SOC2, ISO, or equivalent certifications.
    b. Where a certification is revoked, expires without renewal, or is materially limited in scope, HAQQ shall promptly inform affected Users and provide a remediation plan.

BOOK IV. e-Firm

A. Scope and Purpose

1. The e-Firm Product ("e-Firm") provides Users with digital case and matter management functionalities, including the storage, organization, sharing, and tracking of legal documents, case files, client communications, billing records, and associated metadata (collectively, "Matter Data").
2. e-Firm is designed to facilitate professional legal practice workflows. HAQQ does not provide legal advice through e-Firm, nor does e-Firm replace the independent professional judgment of Users.

B. User Responsibility for Content

1. As Controller, the User retains sole responsibility for the accuracy, legality, and completeness of all Matter Data entered into or stored in e-Firm.
2. The User represents and warrants that:
    a. (a) all Matter Data is collected and processed lawfully, with appropriate consents and notices where required;
    b. (b) no unlawful, infringing, or malicious content is uploaded;
    c. (c) storage of Matter Data within e-Firm does not breach attorney–client privilege, confidentiality, or professional conduct rules applicable in the User's jurisdiction.
3. The User indemnifies HAQQ against any liability arising from non-compliance with professional obligations in respect of Matter Data.

C. Confidentiality and Privilege

1. HAQQ acknowledges that Matter Data may include materials protected by attorney–client privilege, professional secrecy, or equivalent doctrines.
2. HAQQ shall not access Matter Data except:
    a. (a) as strictly necessary to provide the Services;
    b. (b) at the documented instruction of the User; or
    c. (c) where legally required to do so, in which case HAQQ shall notify the User unless prohibited by law.
3. HAQQ's handling of Matter Data shall not constitute a waiver of privilege or confidentiality.

D. Access and Permissions

1. e-Firm supports role-based access control (RBAC). The User, as Administrator, configures which persons within its organization may access specific Matter Data.

2. The User acknowledges that HAQQ has no responsibility for the User's internal allocation of access rights.
3. Administrator actions (account creation, revocation, modification) are binding upon the organization.

E. Audit Trails and Logging

1. e-Firm automatically records logs of key activities, including file uploads, downloads, edits, access attempts, permission changes, and deletions.
2. Such logs are available to the User for compliance, supervision, and litigation-hold purposes.
3. HAQQ may retain anonymized or aggregated audit metrics for the purposes of system improvement and compliance reporting.

F. Document Management and Retention

1. The User may define retention schedules for Matter Data within e-Firm, subject to Applicable Law.
2. Upon termination of the subscription, Matter Data shall be deleted or returned in accordance with Section 3.9 (Data Retention & Deletion).
3. Legal holds: Users may suspend deletion of specific Matter Data by activating a "Legal Hold" flag. While active, such Matter Data will not be purged until the hold is released by the User.

G. Integrations and Third-Party Tools

1. e-Firm may interoperate with third-party services (e.g., document editing, e-signature, court-filing systems).
2. Use of such third-party tools is at the User's discretion and subject to separate terms between the User and the third party. HAQQ disclaims liability for third-party integrations not operated by HAQQ.

H. Professional Obligations

1. The User acknowledges that the use of e-Firm does not relieve them of compliance with professional conduct rules, confidentiality duties, bar association regulations, or court-mandated requirements.
2. HAQQ provides e-Firm "as a tool" only; Users remain accountable for ensuring that their legal practice complies with applicable ethical and professional standards.

I. Limitations of Liability Specific to e-Firm

1. HAQQ disclaims liability for:
    a. (a) Matter Data lost or corrupted due to the User's failure to maintain independent backups outside e-Firm;

b. (b) any professional, ethical, or regulatory breach arising from the User's handling of Matter Data;
c. (c) reliance on automated functionalities (e.g., reminders, deadline calculators) without independent verification by the User.

2. These limitations supplement, and do not replace, the general limitations of liability set out in Book XI.

J. Service Levels and Availability

1. Availability Commitment
    a. HAQQ shall use commercially reasonable efforts to ensure that e-Firm is available to Users not less than **99.5% of the time in any given calendar month**, excluding Permitted Downtime.
    b. "Permitted Downtime" includes:
        1. Scheduled maintenance windows notified to Users at least forty-eight (48) hours in advance;
        2. Emergency maintenance reasonably necessary to address security vulnerabilities or service degradation;
        3. Downtime attributable to acts or omissions of the User, third-party integrations, or events of Force Majeure.
2. Incident Response Targets
    a. HAQQ shall monitor e-Firm on a twenty-four (24) hour basis and shall endeavor to meet the following response and resolution objectives:
        i. **Severity 1 (Critical Outage):** Initial response within two (2) hours, resolution or workaround within eight (8) hours.
        ii. **Severity 2 (Material Degradation):** Initial response within four (4) hours, resolution or workaround within twenty-four (24) hours.
        iii. **Severity 3 (Minor Issue):** Initial response within one (1) business day, resolution in a commercially reasonable timeframe.
3. Data Backup and Recovery Objectives
    a. HAQQ shall maintain encrypted backups of Matter Data with the following objectives:
        i. **Recovery Point Objective (RPO):** No more than twenty-four (24) hours of data loss under normal operating conditions.
        ii. **Recovery Time Objective (RTO):** Restoration of service within twelve (12) hours of a declared disaster event affecting primary hosting infrastructure.
    b. These objectives are targets, not guarantees, and shall be subject to Applicable Law and hosting provider capabilities.
4. Remedies

a. In the event that availability falls below the commitment in Section 4.10(1) for two (2) consecutive months, Users may request a **Service Credit** equivalent to a pro-rata portion of subscription fees paid for the affected Product during the period of non-compliance.
b. Service Credits shall be the sole and exclusive remedy for breach of this Service Level Commitment, without prejudice to the disclaimers and limitations of liability set forth in Book XI.

5. Exclusions
    a. No Service Level Commitment applies where downtime or degradation arises from:
        1. misuse or misconfiguration by the User;
        2. third-party services not under HAQQ's control;
        3. regulatory takedowns or lawful access requests; or
        4. Force Majeure events as defined in Section 11.X.

BOOK V. LEGAL AI

A. Definition and Scope

1. "Legal AI" refers to HAQQ's artificial intelligence capabilities made available within the MyHAQQ Platform, including but not limited to the AI Agent and the Firm Digital Twin, collectively designed to assist Users in professional workflows.
2. Legal AI performs assistive tasks, which may include:
    a. Search and retrieval of documents, records, and metadata within the Ecosystem;
    b. Document understanding, parsing, and extraction of structured information;
    c. Summarization of texts, cases, and communications;
    d. Drafting of templates, contracts, or procedural documents;
    e. Workflow automation and task routing;
    f. Predictive analytics and reporting;
    g. In-product guidance, recommendations, and contextual support.
3. Legal AI is designed to adapt and be guided by Customer-authorized data sources to generate outputs reflecting the Customer's knowledge, operating style, and permitted practices.

B. Inclusions

Legal AI includes the following components and capabilities:

1. AI Agent Access: An interactive virtual assistant embedded within the Platform, available across Products for real-time support.
2. Digital Twin: An AI model leveraging the Customer's structured operational data (case records, billing patterns, document libraries, workflows) to replicate and reflect firm-specific practices.
3. Authorized In-Product Actions: Legal AI may execute specific automated functions on behalf of the Customer (e.g., preparing drafts, auto-populating forms, generating summaries, updating records), but only to the extent expressly configured and enabled by the Customer.

C. Exclusions

Legal AI does **not** include, and HAQQ expressly disclaims responsibility for:

1. Provision of **independent legal advice**, advocacy, or representation;
2. Any guarantee of accuracy, completeness, or outcome of legal matters;
3. Substitution for licensed **human professional services**;

4. Use of AI tools outside the Platform environment or for purposes not expressly authorized in writing by HAQQ.

D. Customer Controls and Responsibilities

1. The Customer retains exclusive control over:
    a. Enabling or disabling specific Legal AI functionalities;
    b. Defining permissible data sources and retention schedules;
    c. Supervising, validating, and approving all AI-assisted outputs.
2. The Customer acknowledges that AI outputs are **recommendations, drafts, or analytical aids** and may contain inaccuracies, omissions, or biases.
3. The Customer is solely responsible for:
    a. Reviewing and verifying outputs before relying on them in professional practice;
    b. Ensuring that AI use complies with applicable ethical, regulatory, and professional conduct obligations;
    c. Training its staff on proper and lawful use of Legal AI.

E. Data Processing and Training

1. Legal AI may process Customer Data, subject always to Book III (Data Protection, Hosting & Compliance).
2. Customer Data used for training or fine-tuning Legal AI shall be:
    a. limited to data sources expressly authorized by the Customer;
    b. subject to anonymization, pseudonymization, or equivalent safeguards wherever possible; and
    c. retained only as necessary to provide, improve, and personalize the Legal AI service in accordance with Applicable Data Protection Laws.
    d. used solely within the limits of Customer's account and will in no way be used to train the AI model outside of these limits.
3. Derived AI models and improvements developed by HAQQ remain HAQQ's intellectual property, provided that no model weights or outputs shall directly disclose identifiable Customer Data.

F. Payments and Usage Fees

1. Legal AI may be subject to **usage-based fees**, capacity pricing, or subscription tiers, as set out in Book XI (Commercial Terms).
2. HAQQ may debit usage charges directly from the Customer's registered **eWallet** or other payment method on file.
3. Any changes to fee structures will be communicated with reasonable notice and shall not affect prior committed subscriptions during their active term.

G. Human Oversight

1. Legal AI is an **assistive technology** only. It does not replace lawyers, nor does it constitute licensed legal services, legal advice, or legal representation and requires human oversight.
2. Users remain solely responsible for applying their own **professional judgment**, verifying outputs, and complying with their duties of competence, confidentiality, diligence, and independence under applicable professional rules.
3. Reliance on Legal AI does not relieve Users of obligations owed to clients, courts, regulators, or professional associations.
4. HAQQ disclaims liability for disciplinary, ethical, or professional consequences resulting from misuse or over-reliance on Legal AI.

H. Limitations of Liability Specific to Legal AI

1. To the maximum extent permitted by law, HAQQ shall not be liable, especially when caused by the absence of human oversight, for:
    a. inaccuracies, omissions, or errors in AI-generated outputs;
    b. any legal, regulatory, or professional consequences of blind reliance on such outputs;
    c. damages arising from AI misclassification, hallucination, or unexpected performance.
2. These limitations supplement, and do not replace, the general liability framework in Book XI.

I. Service Levels and Availability

1. Availability Commitment
    a. HAQQ shall use commercially reasonable efforts to ensure that the Legal AI components (including the AI Agent and Digital Twin) are available to Users not less than **99.0% of the time in any given calendar month**, excluding Permitted Downtime.
    b. "Permitted Downtime" includes:
        i. Scheduled maintenance windows notified to Users at least twenty-four (24) hours in advance;
        ii. Emergency maintenance to remediate vulnerabilities or service degradation;
        iii. Downtime attributable to third-party hosting or AI infrastructure providers beyond HAQQ's reasonable control;
        iv. Force Majeure events as described in Book XI.
2. Response Time Objectives

a. HAQQ shall endeavor to achieve the following prompt-processing targets for Legal AI requests under normal operating conditions:
    i. **Standard Text Inference (≤ 5,000 words output):** Median response time under thirty (30) seconds.
    ii. Extended Inference (> 5,000 words output or multi-document context): Median response time under two (2) minutes.
    iii. **Digital Twin Actions:** Completion of routine in-product actions within five (5) minutes of initiation.
b. These objectives are aspirational and may vary based on system load, input complexity, or integration with external systems.

3. Incident Response Targets
    a. Legal AI incidents shall be classified and addressed as follows:
        i. **Severity 1 (Critical Outage, Legal AI unavailable across all Users):** Initial response within two (2) hours, mitigation within eight (8) hours.
        ii. **Severity 2 (Material Degradation, major latency or partial unavailability):** Initial response within four (4) hours, mitigation within twelve (12) hours.
        iii. **Severity 3 (Minor Issue, isolated errors, non-critical inaccuracies):** Initial response within one (1) business day, resolution in a commercially reasonable timeframe.
4. Model Recovery Objectives
    a. HAQQ shall maintain redundant hosting for Legal AI inference services with the following recovery objectives:
        i. **Recovery Point Objective (RPO):** Less than twelve (12) hours of model-training data loss.
        ii. **Recovery Time Objective (RTO):** Restoration of functional Legal AI services within twelve (12) hours of a declared service disruption.
5. Remedies
    a. Where availability falls below the commitment in Section 5.9(1) for two (2) consecutive months, Users may request a **Service Credit** equal to a pro-rata portion of fees attributable to Legal AI during the affected period.
    b. Service Credits are the sole and exclusive remedy for failure to meet these service levels and shall not give rise to damages or other monetary compensation.
6. Exclusions
    a. Service levels shall not apply where downtime or degraded performance results from:
        i. Misuse of Legal AI beyond intended purpose;

ii. User-supplied data errors or excessive input complexity beyond system parameters;
iii. Third-party integrations or systems not operated by HAQQ;
iv. Suspension or limitation of access due to User breach of these Terms.

BOOK VI. e-Client

A. Definition and Scope

1. "**e-Client**" refers to HAQQ's client-facing portal application delivered on the MyHAQQ Platform, designed to facilitate digital interaction between a Client and their legal service provider.
2. e-Client enables Clients of subscribing firms to:
    a. Onboard digitally and complete intake or "Know-Your-Client" (KYC) workflows;
    b. Communicate securely with their lawyer or firm;
    c. Upload, receive, and review files or correspondence;
    d. Track assigned tasks, deadlines, and case progress;
    e. Review invoices, settle accounts through integrated payment tools (including eWallet); and
    f. Maintain a personal legal archive of engagements with one or more lawyers or firms.

B. Inclusions

e-Client expressly includes:

1. **Client Identity and Login** – Creation of a unique e-Client login credential linked to the Client's verified identity;
2. **Secure Messaging and File Exchange** – Encrypted, role-restricted communication channels for correspondence and document transfer between Client and firm;
3. **Invoice Review and Payment** – Access to electronic invoices issued by the firm, with integrated payment via eWallet or other supported methods;
4. **Status and Task Tracking** – Client visibility into matter status, key deadlines, and assigned tasks as configured by the firm within e-Firm.

C. Exclusions

e-Client does **not** include:

1. Any adjudicatory or governmental court filing, hearing, or decision-making function;
2. Case outcome guarantees, legal advice, or independent legal services;
3. Custom branding, white-label configurations, or non-standard portal design, except as expressly provided in **Book VIII: Customization Services**.

D. Dependencies and Integration

1. e-Client requires an active subscription to **e-Firm** or equivalent integration to supply case, document, billing, and matter data.
2. In the absence of such integration, e-Client functionality may be limited to identity creation, secure messaging, and invoice payment.
3. HAQQ disclaims liability for degraded performance where dependency on e-Firm or third-party integration is misconfigured by the firm.

E. Client Identity, Onboarding, and KYC

1. Firms utilizing e-Client must configure intake and KYC workflows appropriate to their jurisdictional and regulatory requirements.
2. HAQQ provides the technical capability for KYC collection and secure storage, but the **firm remains responsible** for:
    a. Lawful collection of personal and sensitive data;
    b. Verification of client identity;
    c. Compliance with anti-money laundering (AML), counter-terrorism financing (CTF), and sanctions obligations.
3. e-Client login credentials are personal, non-transferable, and must be protected by the Client using reasonable security practices.

F. Communications and Confidentiality

1. Communications exchanged via e-Client are encrypted in transit and at rest in accordance with Book III (Data Protection, Hosting & Compliance).
2. Firms are responsible for ensuring that communications with Clients through e-Client do not waive professional privilege, confidentiality, or equivalent doctrines under applicable law.
3. HAQQ does not monitor the substance of Client–firm communications except as necessary for technical support, security monitoring, or as legally required.

G. Payments and Invoices

1. e-Client integrates with HAQQ's **eWallet** and other approved payment processors to enable secure settlement of invoices.
2. Clients may view, download, and pay invoices issued by the firm, with transaction records retained in accordance with Book III and applicable financial laws.
3. HAQQ is not a party to the underlying legal engagement or fee agreement between Client and firm. HAQQ provides only the technical infrastructure to transmit payment instructions.

H. Personal Legal Archive

1. e-Client enables Clients to maintain a record of their engagements, including correspondence, files, invoices, and matter summaries.
2. The archive is for informational purposes only and does not constitute an official or legally binding record of judicial or governmental proceedings.
3. Clients may export their personal archive during the subscription period or within the retention period defined in Section 3.9 (Data Retention & Deletion).

I. Service Levels and Availability

1. **Availability Commitment**: HAQQ shall use commercially reasonable efforts to make e-Client available not less than **99.5% of the time in any given calendar month**, excluding Permitted Downtime (maintenance, third-party outages, Force Majeure).
2. Incident Response Targets
    a. **Severity 1 (Critical outage – client portal inaccessible):** Initial response within two (2) hours; mitigation within eight (8) hours.
    b. **Severity 2 (Material degradation – messaging or payment functions impaired):** Initial response within four (4) hours; mitigation within twenty-four (24) hours.
    c. **Severity 3 (Minor issues – isolated errors, cosmetic defects):** Response within one (1) business day; resolution in a commercially reasonable timeframe.
3. **Data Recovery Objectives**, Encrypted backups of e-Client data shall be maintained with an RPO of twenty-four (24) hours and an RTO of twelve (12) hours following a declared disaster event.
4. **Remedies**: Where availability falls below the commitment in Section 6.9(1) for two (2) consecutive months, Users may request a pro-rata Service Credit for the portion of subscription fees attributable to e-Client. Service Credits are the sole and exclusive remedy for failure to meet this commitment.

J. Professional Responsibility

1. e-Client is an assistive tool designed to enhance Client–firm collaboration. It does not provide legal advice, replace in-person consultations, or guarantee legal outcomes.
2. Firms remain solely responsible for supervising Client interactions, reviewing communications, and fulfilling professional and regulatory obligations.
3. HAQQ disclaims liability for disputes between Clients and firms, including but not limited to billing disputes, malpractice claims, or misinterpretation of portal communications.

BOOK VII. Legal Directory (Hire Your Lawyer)

A. Definition and Scope

1. "**Legal Directory**" or "**Hire Your Lawyer**" refers to the MyHAQQ Platform's professional directory and matchmaking features that enable end users ("Clients") to:
    a. Discover, filter, and search for licensed lawyers and law firms by geography, specialization, language, and experience;
    b. Review professional profiles, credentials, and practice descriptions;
    c. Initiate inquiries, intake, or consultations through integrated workflows;
    d. Where available, commence engagement via e-Client and process payments through eWallet.
2. The Legal Directory may interconnect with the broader MyHAQQ marketplace stack, including but not limited to **content exchanges, template libraries, and job listings** accessible to participating legal professionals.

B. Inclusions

The Legal Directory expressly includes:

1. **Search and Discovery**, Searchable and filterable listings of participating lawyers and law firms;
2. **Profile Listings**, Publication of professional profiles including name, jurisdiction of practice, credentials, contact information, and areas of specialization, as provided by the lawyer or firm;
3. **Inquiry Workflows**, Structured intake requests or inquiries enabling potential Clients to request consultations or initiate communication;
4. **Optional Intake and Payments**, Where integrated, Clients may initiate onboarding via e-Client and transmit payments via eWallet, subject to the relevant Books of these Terms.

C. Exclusions

The Legal Directory does **not** include, and HAQQ expressly disclaims responsibility for:

1. Certification, accreditation, or endorsement of any lawyer, firm, or listed professional credentials;
2. Validation of licensing status, bar membership, or disciplinary history except where expressly required by law in the operating jurisdiction;
3. Fee sharing, splitting, or referral compensation with firms or lawyers where prohibited under applicable laws or professional conduct rules;

4. Regulation, oversight, or enforcement of lawyer conduct, which remain the responsibility of the competent professional bodies.

D. Profile Data and User Responsibility

1. Lawyers and firms are solely responsible for the accuracy, currency, and lawfulness of the information they submit to the Legal Directory.
2. By submitting a profile, the professional represents and warrants that:
    a. they are duly licensed, registered, or authorized to practice law in the jurisdiction(s) indicated;
    b. information provided is truthful, not misleading, and compliant with applicable advertising and solicitation rules;
    c. use of the Legal Directory will not cause HAQQ to contravene any local or cross-border legal practice restrictions.
3. HAQQ may, but is not obliged to, conduct background checks or verification of professional credentials.

E. Independence of Engagements

1. All contracts for legal services initiated through the Legal Directory are **independent bilateral agreements** directly between the Client and the selected lawyer or firm.
2. HAQQ is **not a party** to any such engagement and shall not be deemed to provide legal services, legal advice, or representation.
3. The Client and lawyer/firm remain independently responsible for negotiating engagement terms, verifying credentials, and complying with professional and regulatory obligations.

F. Payments and eWallet Integration

1. Where eWallet functionality is enabled, HAQQ provides the technical infrastructure for the transfer of funds between Clients and firms.
2. HAQQ does not determine fees, billing terms, or payment schedules, which remain exclusively governed by the agreement between Client and lawyer/firm.
3. Transaction records are maintained for audit and compliance purposes in accordance with Book III (Data Protection, Hosting & Compliance).

G. Professional Conduct and Regulation

1. Lawyers and firms listed in the Directory remain subject to the rules of professional conduct, ethics codes, and regulatory oversight of their respective jurisdictions.
2. Use of the Legal Directory does not relieve professionals of their independent obligations, including restrictions on advertising, solicitation, conflicts of interest, confidentiality, or unauthorized practice of law.

3. HAQQ disclaims liability for disciplinary or regulatory actions arising from professional conduct of listed lawyers or firms.

H. Limitations of Liability

1. HAQQ shall not be liable for:
    a. (a) Misrepresentation, inaccuracies, or omissions in lawyer or firm profiles;
    b. (b) Disputes between Clients and lawyers or firms, including fee disputes, malpractice claims, or dissatisfaction with legal outcomes;
    c. (c) Any direct or indirect reliance placed by a Client on Directory content without independent verification.
2. These limitations supplement, and do not replace, the general limitations of liability set forth in Book XI.

I. Service Levels and Availability

1. HAQQ shall use commercially reasonable efforts to maintain the Legal Directory's search and listing functions with **99.5% monthly availability**, excluding Permitted Downtime as defined in Book IV and Book V.
2. Response targets for Directory-related incidents shall be:
    a. **Severity 1 (Complete unavailability):** Response within two (2) hours, mitigation within eight (8) hours;
    b. **Severity 2 (Major degradation – search or profile publishing impaired):** Response within four (4) hours, mitigation within twenty-four (24) hours;
    c. **Severity 3 (Minor issues – isolated profile errors or cosmetic defects):** Response within one (1) business day, resolution in a commercially reasonable timeframe.
3. Remedies for downtime are limited to Service Credits as described in Book XI.

BOOK VIII. CUSTOMIZATION SERVICES

A. Definition and Scope

1. "**Customization Services**" means professional services performed by HAQQ, whether remotely or on-site, to configure, localize, and extend a Customer's use of the MyHAQQ Platform and subscribed Books.
2. Such services are **governed exclusively** by a **Statement of Work ("SOW")** executed between HAQQ and the Customer, which shall define scope, deliverables, assumptions, acceptance criteria, timelines, responsibilities, and fees.
3. In the event of conflict between these Terms and an executed SOW, the SOW shall prevail solely with respect to the specific Customization Services covered therein.

B. Inclusions

Customization Services expressly include, without limitation:

1. **Configuration and Enablement**, Adjusting settings, permissions, and workflows within supported product boundaries to align with Customer requirements.
2. **Workflow and Process Design**, Designing automated workflows, matter intake processes, approval hierarchies, and task routing consistent with the Customer's operating model.
3. **Taxonomy and Ontology Mapping**, Aligning Customer data models, classifications, and controlled vocabularies with the Platform's ontology for consistency and interoperability.
4. **Template and Document Assembly Setup**, Creating, importing, and testing firm-specific templates and document automation rules within the supported Platform framework.
5. **Report and Dashboard Building**, Configuring dashboards, analytics, and reporting functions, including role-based and cross-functional visualizations.
6. **Light UI Adjustments**, Applying supported theming, branding, and layout adjustments within Platform limits.
7. **Connector and Integration Development**, Developing approved connectors or mappings between MyHAQQ and third-party systems, where technically feasible and within supported APIs.
8. **Knowledge Transfer Sessions**, Conducting workshops or training to ensure Customer teams understand deployed configurations and can maintain them going forward.

C. Exclusions

Unless expressly provided in the SOW, Customization Services shall not include:

1. **Core Product Feature Changes**, Modification of underlying source code, proprietary algorithms, or Platform architecture.
2. **Unsupported Code Modifications**, Reverse engineering, unauthorized scripting, or use of unsupported SDKs or APIs.
3. **Third-Party Digitization Programs**, Governmental, court, or regulatory digitization projects, or integrations requiring direct governmental contracting, which must be separately scoped and contracted.
4. **Custom Development Beyond Approved Boundaries,** Features requiring bespoke engineering outside of the standard customization toolset unless separately contracted as Product Development.

D. Service Delivery and Acceptance

1. **Delivery Framework**, HAQQ will deliver Customization Services in accordance with industry-standard project management practices and any milestones set forth in the SOW.
2. **Acceptance Criteria**, Each deliverable shall be deemed accepted upon:
    a. written confirmation by the Customer that the deliverable conforms to the specifications in the SOW; or
    b. absent written objection within ten (10) business days of delivery, provided such objection is not unreasonably withheld.
3. **Dependencies**, Timely completion of services is contingent upon Customer providing necessary access, data, personnel, and approvals. Delays attributable to Customer may extend delivery timelines.

E. Intellectual Property (IP)

1. **HAQQ Ownership**: Unless expressly stated otherwise in the SOW:
    a. HAQQ retains ownership of all Platform configurations, accelerators, connectors, scripts, mappings, and tools developed or deployed in connection with Customization Services;
    b. Such materials are deemed part of the HAQQ Ecosystem and may be reused by HAQQ in engagements with other customers.
2. **Customer Ownership**, Customer retains ownership of:
    a. its Data, files, and records;
    b. firm-specific templates, workflows, or branding elements developed exclusively from Customer materials; and
    c. any deliverables expressly designated as “Customer Property” in the SOW.
3. **Licenses**, To the extent HAQQ deliverables incorporate HAQQ IP, HAQQ grants Customer a non-exclusive, non-transferable, worldwide license to use such deliverables solely in connection with the Ecosystem and subject to the subscription term.

F. Fees and Payment

1. Fees for Customization Services shall be set forth in the applicable SOW and invoiced on a fixed-fee, milestone-based, or time-and-materials basis as specified therein.
2. Payments are due within thirty (30) days of invoice unless otherwise stated in the SOW.
3. Travel and accommodation costs for on-site services are billable at cost and must be pre-approved by Customer.

G. Service Levels and Warranty

1. **Performance Warranty**, HAQQ warrants that Customization Services will be performed:
    a. in a professional and workmanlike manner consistent with industry standards; and
    b. substantially in accordance with the specifications set forth in the SOW.
2. **Remedy for Non-Conformance**, Customer's exclusive remedy for breach of warranty shall be, at HAQQ's option:
    a. re-performance of the deficient services at no additional cost; or
    b. refund of the fees actually paid for the deficient services.
3. **Exclusions**, HAQQ makes no warranty with respect to:
    a. outcomes dependent on Customer's own data or configurations;
    b. unsupported modifications by Customer or third parties;
    c. delays or failures arising from Customer's failure to provide necessary inputs, data, or approvals.

H. Limitations of Liability

1. HAQQ's liability for Customization Services shall be limited in accordance with Book XI (Commercial Terms, Disclaimers & Miscellaneous).
2. In no event shall HAQQ be liable for indirect, consequential, or punitive damages arising from the use or inability to use Customization Services.

BOOK IX. ELITE SUPPORT

A. Definition and Scope

1. "**Elite Support**" means HAQQ's premium support tier, available to Customers who have subscribed via Order Form or Support Policy, designed to provide enhanced responsiveness, senior resource allocation, and proactive success management for the Customer's use of the Ecosystem.
2. Elite Support supplements (and does not replace) HAQQ's standard support offerings, incorporating the standard channels and business hours published by HAQQ while extending entitlements as described herein.
3. In case of conflict between this Book IX and any published **Support Policy** or **Order Form**, the latter shall prevail for the scope of Elite Support purchased.

B. Inclusions

Elite Support expressly includes, without limitation:

1. **Priority Incident Processing** Placement of all submitted cases in priority support queues, with expedited triage and assignment to available engineers.
2. **Escalation Pathways** Defined escalation to senior support engineers, technical leads, or product managers where appropriate.
3. **Customer Success Management** Assignment of a designated Customer Success Manager ("CSM") who serves as the primary advocate and liaison between HAQQ and the Customer.
4. **Proactive Health Reviews** Periodic review of system health, usage trends, adoption metrics, and configuration alignment, with recommendations for optimization.
5. **Enablement Sessions** Scheduled knowledge transfer or training sessions designed to upskill Customer teams on newly released features, best practices, and compliance alignment.
6. **Release Coordination** Early access briefings and readiness sessions prior to major product releases, to support Customer planning and integration.

C. Exclusions

Unless expressly included in the Order Form or SOW, Elite Support does not cover:

1. **Professional Services Deliverables** – Any custom workflow, development, configuration, or training that falls under Book VIII (Customization Services).
2. **Data Migration Tasks** Large-scale or one-time migration of legacy data, which is separately scoped under Book X (Data Migration).
3. **On-Site Presence** – On-site support or staffing unless explicitly agreed in writing and separately charged.

4. **Third-Party Products** Issues arising from Customer's non-HAQQ systems, third-party hardware, or unsupported integrations.

D. Service Levels

1. Case Severity Levels and Response Times
    a. **Severity 1 Critical Business Impact (system down, no workaround):** Response within one (1) hour, updates every two (2) hours until resolution or workaround is in place.
    b. **Severity 2 High Business Impact (major functionality impaired, limited workaround):** Response within four (4) business hours, updates every business day until resolution.
    c. **Severity 3 Medium Business Impact (non-critical function issue, workaround available):** Response within one (1) business day, resolution in a commercially reasonable timeframe.
    d. Severity 4 Low Business Impact (how-to questions, minor cosmetic issues, enhancement requests): Response within two (2) business days, resolution in future release or update.
2. Availability of Support Channels
    a. **Standard Hours:** HAQQ's published business hours for the Customer's region.
    b. **Elite Entitlement:** Extended availability, including emergency weekend coverage for Severity 1 cases.
3. Proactive Success Reviews
    a. Conducted at least once per quarter, covering usage adoption, compliance posture, upcoming releases, and optimization opportunities.

E. Customer Responsibilities

1. **Contact Points**, Customer must maintain current contact details for authorized support liaisons and ensure such liaisons are trained in case submission guidelines.
2. **Case Submission**, Customer must follow HAQQ's published case submission process, including classification by severity, provision of diagnostic information, and reproduction steps.
3. **Environment Cooperation**, Customer shall provide HAQQ with timely access to relevant system logs, configurations, and test environments necessary to diagnose and resolve incidents.
4. **Reasonable Use**, Elite Support entitlements are subject to fair use. HAQQ reserves the right to discuss adjustment of scope or fees where support usage is excessive or materially exceeds anticipated volumes.

F. Fees and Term

1. Elite Support is billed as a subscription add-on, at rates specified in the applicable Order Form.
2. Fees are payable in advance on an annual or multi-year basis unless otherwise agreed.
3. Elite Support shall renew automatically with the Customer's base subscription unless either Party provides thirty (30) days' prior written notice of termination or non-renewal.

G. Warranty and Disclaimer

1. HAQQ warrants that Elite Support will be provided with commercially reasonable skill and care consistent with industry practices.
2. HAQQ does not warrant that all errors will be corrected or that operation of the Ecosystem will be uninterrupted or error-free.
3. Remedies for breach of this warranty are limited to re-performance of services or, if re-performance is not feasible, a refund of fees paid for the affected support period.

H. Limitation of Liability

1. HAQQ's liability for Elite Support shall be subject to and limited by the provisions of Book XI (Commercial Terms, Disclaimers & Miscellaneous).
2. Service credits, re-performance, or refunds (as applicable) shall constitute the Customer's exclusive remedy for failures in the provision of Elite Support.

BOOK X. SERVICE LEVELS, MAINTENANCE, AND REMEDIES

A. Purpose and Scope

1. This Book establishes HAQQ's baseline commitments with respect to service availability, maintenance practices, support response targets, and remedies for downtime across the Ecosystem.
2. These commitments apply to all Products and Services unless expressly supplemented or modified by a Product-specific SLA contained in another Book.
3. In the event of conflict, the **more stringent commitment** (whether under this Book or a Product-specific SLA) shall prevail.

B. Availability Target

1. HAQQ shall use commercially reasonable efforts to maintain a **monthly uptime availability of 99.5%**, measured across the Ecosystem on a calendar-month basis.
2. For purposes of this SLA, "Uptime" means the percentage of time during which the core functionalities of the Ecosystem are accessible and operational, excluding:
    a. Scheduled Maintenance (per Section 10.3);
    b. Force Majeure events; and
    c. Outages attributable to Customer systems, networks, or third-party providers not under HAQQ's control.

C. Scheduled Maintenance

1. HAQQ will provide at least **forty-eight (48) hours' prior notice** of planned maintenance where reasonably feasible.
2. Maintenance will be scheduled, where practicable, during **low-impact usage windows** to minimize Customer disruption.
3. Emergency maintenance may be conducted without prior notice when necessary to remediate vulnerabilities or service degradation; in such cases HAQQ shall notify affected Customers promptly.

D. Support Hours and Response Targets

Unless otherwise specified in a Product-specific SLA or Support Policy, HAQQ shall apply the following baseline targets:

1. **Severity 1 (Critical Production Outage):** Initial response within 1 hour; continuous efforts until restoration or workaround.
2. **Severity 2 (Major Functionality Impaired):** Initial response within 4 business hours.

3. **Severity 3 (Degraded Performance / Non-Critical Defect):** Initial response within 1 business day.
4. **Severity 4 (General Question / Feature Request):** Response within 3 business days.

E. Service Credits

1. If actual availability in a given calendar month falls below the 99.5% target for reasons attributable to HAQQ, Customer may request a **Service Credit** equal to **5% of the monthly subscription fee for each full 1% below the target**, capped at **25% of the monthly fee** for that month.
2. Service Credits must be requested in writing within thirty (30) days of the relevant month-end.
3. Service Credits constitute the Customer's **exclusive monetary remedy** for availability issues under this Book.

F. Remedies and Limitations

1. Service Credits are not available where downtime results from:
    a. misuse of the Ecosystem by the Customer;
    b. issues with Customer-supplied data, configurations, or networks;
    c. failures of third-party services not under HAQQ's control; or
    d. suspension of access due to Customer breach of these Terms.
2. Nothing in this Book shall affect HAQQ's obligations to re-perform services or provide remedies under Product-specific Books (e.g., Legal AI, e-Firm, Elite Support).

G. Relationship to Product-Specific SLAs

1. Product-specific SLAs (e.g., Books IV, V, IX) may define stricter availability commitments, narrower response windows, or additional remedies.
2. Where such provisions apply, the stricter obligation shall govern for the relevant Product.
3. This Book continues to apply as a baseline framework for all other Products and Services not otherwise covered by a Product-specific SLA.

BOOK XI. Data Migration

A. Definition and Scope

1. "**Data Migration Services**" means professional services performed by HAQQ, whether remotely or on-site, to transfer User Data onto the MyHAQQ Platform and subscribed Books and may include:
    a. physical records requiring digitization;
    b. digital data stored on Customer premises; and
    c. digital data stored in third-party applications, CRMs, legacy systems or databases.
2. Such services are **governed exclusively** by a **Statement of Work ("SOW")** executed between HAQQ and the Customer, which shall define scope, deliverables, assumptions, acceptance criteria, timelines, responsibilities, and fees. Data Migration is provided as an ancillary service to facilitate onboarding and does not form part of the core subscription unless expressly purchased by Customer under an Order Form or Statement of Work.
3. In the event of conflict between these Terms and an executed SOW, the SOW shall prevail solely with respect to the specific Data Migration Services covered therein.

B. Fees

1. Data Migration services are billed on an **hourly basis at pre-agreed rates**, unless otherwise set forth in the applicable Order Form or SOW.
2. Final fees depend on the **quality, accessibility, and completeness of Customer's data sources**, and may be subject to adjustment if the effort materially exceeds assumptions.
3. Out-of-pocket expenses (e.g., shipping, digitization hardware, secure couriers) are chargeable at cost with prior approval.

C. Confidentiality

1. For purposes of this Book, "**Confidential Information**" includes any Customer data, client files, personal information, legal documents, filings, case strategies, communications, contact lists, databases, and any proprietary or sensitive material accessed by HAQQ or its subcontractors during Data Migration.
2. Confidential Information excludes data that:
    a. becomes publicly available without breach;
    b. was lawfully known to HAQQ before disclosure; or
    c. is received lawfully from a third party without restriction.
3. HAQQ shall not disclose or use Confidential Information except:
    a. as strictly necessary to perform Data Migration;

b. as required by law or court order; or
c. as otherwise authorized in writing by Customer.

D. Data Security and Custody

1. HAQQ shall implement **industry-standard technical and organizational safeguards** aligned with SOC2 and GDPR Article 32, including encryption, access control, and secure transfer protocols.
2. Physical and digital custody of Customer Data during migration shall be restricted exclusively to **HAQQ Inc., its employees, officers, directors, contractors, agents, affiliates, and approved Sub-Processors**, each of whom shall be subject to confidentiality obligations no less protective than those set forth herein. HAQQ shall ensure that all such personnel and entities:
    a. access Customer Data solely on a strict need-to-know basis;
    b. are bound by the duties of confidentiality, security, and restricted use herein; and
    c. undergo regular training in information security and data protection appropriate to their role.
3. Upon completion or termination of Data Migration, HAQQ shall return or securely delete all copies of Customer Data in its possession, subject to legal or regulatory retention requirements.

E. Non-Solicitation and Misappropriation

1. For a period of two (2) years following completion of Data Migration, HAQQ shall not, without Customer's written consent:
    a. solicit or engage directly with Customer's clients, affiliates, or referred parties for services unrelated to the Ecosystem; or
    b. solicit for hire any employees or contractors of Customer involved in the migration project.
2. Nothing in this Section restricts HAQQ's right to provide services to other customers generally, provided such services do not involve the use of Customer's Confidential Information.

F. Term and Survival

1. Data Migration services continue until completion or termination under the applicable Order Form or SOW.
2. Obligations relating to confidentiality, security, and non-solicitation shall **survive for five (5) years from execution** or **two (2) years following service completion**, whichever is longer.
3. Nothing herein limits HAQQ's broader confidentiality obligations under Book III (Data Protection, Hosting & Compliance).

BOOK XII. COMMERCIAL TERMS, DISCLAIMERS, AND OTHER TERMS

A. Subscriptions, Billing, and Taxes

1. Subscriptions are sold on a monthly, annual, or multi-annual basis, as specified in the applicable Order Form.
2. Fees are invoiced in advance of each billing cycle and are **non-refundable**, except where expressly provided under this Agreement (e.g., pro-rata refunds under termination for HAQQ breach).
3. All published prices exclude value-added taxes (VAT), sales taxes, withholdings, duties, or other governmental charges. The Client is solely responsible for remitting such taxes. If HAQQ is required to collect or withhold, such amounts will be added to the invoice.

B. Overages and Changes

1. Adding new users, modules, or storage during a subscription term will result in a **pro-rata fee adjustment** for the remainder of that billing period.
2. HAQQ may revise subscription fees or pricing for renewals, provided that written notice is given at least thirty (30) days prior to renewal.

C. Suspension for Non-Payment or Misuse

1. HAQQ may suspend access to the Services if:
    a. undisputed invoices remain unpaid thirty (30) days after due date; or
    b. the Client materially breaches the Acceptable Use Policy (Book III) and fails to remedy within fifteen (15) days of notice.
2. Suspension does not relieve the Client of payment obligations.

D. Intellectual Property

1. HAQQ retains and exclusively owns all intellectual property rights in the Ecosystem, the Products, documentation, designs, methodologies, and underlying software.
2. Client retains ownership of its **Client Materials** (documents, templates, files, case content) and **Client Personal Data**.

3. Client grants HAQQ a limited, worldwide, royalty-free license to host, copy, process, transmit, and display Client Materials and Client Personal Data solely as required to provide the Services.

E. Confidentiality

1. Each Party shall protect the other Party's **Confidential Information** with at least the same degree of care it uses to protect its own confidential information, and in any event not less than reasonable care.
2. Confidential Information shall be used solely for performance under this Agreement.
3. Disclosure is permitted only:
    a. with prior written consent;
    b. to affiliates, employees, agents, and Sub-Processors bound by equivalent duties; or
    c. as required by law or court order, with prior notice where legally permitted.

F. Warranties and Disclaimers

1. HAQQ warrants that it will deliver the Services in a **professional, workmanlike manner**, consistent with industry standards.
2. Except for the limited warranty above, the Services are provided **"as is" and "as available."**
3. To the fullest extent permitted by law, HAQQ disclaims all implied warranties, including merchantability, fitness for a particular purpose, accuracy of results, and non-infringement.
4. HAQQ is **not a law firm** and does not provide independent legal advice. Legal AI and other AI outputs are **assistive tools only**; Clients remain responsible for exercising independent professional judgment.

G. Indemnities

1. **HAQQ Indemnity.** HAQQ will defend and indemnify the Client against third-party claims that the Services, as provided by HAQQ (excluding Client Materials or third-party integrations), infringe or misappropriate such third party's intellectual property rights.
2. **Client Indemnity.** The Client will defend and indemnify HAQQ against third-party claims arising out of:

a. Client Materials or Client Personal Data;

b. use of the Services in violation of law or this Agreement; or

c. modifications, configurations, or combinations not provided by HAQQ.

3. Each Party's indemnity is conditioned on prompt written notice, sole control of defense, and reasonable cooperation.

H. Limitation of Liability

1. Neither Party shall be liable for indirect, incidental, special, consequential, exemplary, or punitive damages, or for lost profits, lost revenue, loss of goodwill, or business interruption.

2. Each Party's total aggregate liability for all claims in any twelve (12) month period shall not exceed the total fees paid or payable by Client to HAQQ for the Services giving rise to the claim during that period.

3. These limitations shall not apply to indemnity obligations, gross negligence, fraud, or willful misconduct.

I. Force Majeure

1. Neither Party shall be liable for any delay or failure in performance caused by events beyond its reasonable control, including acts of God, natural disasters, war, terrorism, civil unrest, labor disputes, pandemics, governmental actions, or failures of third-party networks or utilities. Performance shall be excused for the duration of the force majeure event.

J. Term and Termination

1. The Term commences on the Effective Date and continues through the subscription term specified in the Order Form.

2. Either Party may terminate this Agreement for **material breach** if not cured within thirty (30) days of written notice.

3. Upon expiration or termination:

a. HAQQ will provide Client a ninety (90) day export window to retrieve Client Materials and Client Personal Data;

b. thereafter, HAQQ will delete or irreversibly anonymize all Client Data, subject to retention required by law or Book XII (Data Retention and Deletion).

K. No Money Back Guarantee

1. No money-back guarantee applies under this Agreement. Any promotional programs or prior guarantees referenced in legacy agreements are expressly retired.

L. Changes to Terms

1. HAQQ may update these Terms from time to time.
2. Material changes will be notified in writing at least thirty (30) days in advance and will take effect at the next renewal unless earlier required by law, security, or compliance obligations.

M. Export Control and Sanctions Compliance

1. The Client represents and warrants that neither it, nor its affiliates, nor any Authorized Users are located in or acting on behalf of an entity in a country subject to comprehensive sanctions, nor are they named on any government sanctions or restricted parties list.
2. The Client shall comply with all applicable export control laws, trade restrictions, and sanctions regulations in its use of the Services.