CompliMind

Terms and Conditions (including SLA, DPA and SRM)

CompliMind: AI-powered compliance and assurance platform for estates and facilities

Version 1.0 | 21 January 2026

Table of Contents

DEFINITIONS

In this Contract the following words have the following meanings:

- "**Affiliate**" means any direct or indirect holding Company or Subsidiary Company of the relevant entity. A Company is a "Subsidiary" of another Company, if the latter company: (a) holds a majority of the voting rights in it; or (b) is a member of it and has the right to appoint or remove a majority of its board of directors; or (c) is a member of it and controls alone, pursuant to an agreement with other shareholders or members, a majority of the voting rights in it.
- **"Agreement"** means Order Form + these Terms + Schedules (SLA/DPA/SRM) + any Statement of Work.
- "**AI Output**" means any content, suggestion, recommendation, summary, or other output generated by or through the Hosted Services using artificial intelligence or machine learning functionality.
- "**Background Intellectual Property**" means all Intellectual Property Rights that:
    - (a) are owned or controlled by the Supplier prior to the Effective Date; or
    - (b) are developed independently of this Contract; or
    - (c) arise from the Supplier's generic know-how, tools, frameworks, or software components used in the provision of the Hosted Services.
- "**Clinical Use**" means any use of the Hosted Services or AI Outputs for clinical decision-making, patient treatment, or any activity that could reasonably be expected to impact patient care, diagnosis, or safety.
- "**Company**" includes any body corporate or any legal entity capable under law of making a contract.
- "**Connectivity Infrastructure**" means the internet, telecommunications links, broadband and/or third-party software and systems which are intended to connect/interface with (or be interoperable with) the Hosted Services and/or Supplier Platform, including any software licences advised by Supplier.
- "**Contract**" means these Terms & Conditions and the Order Form.
- "**Costs**" means costs, liabilities, penalties, and charges.
- "**Customer**" means the 'Customer' specified in the Order Form.
- "**Customer Data**" means any information, materials, or data: (a) uploaded, stored or created in or using the Supplier Platform by: (i) the Customer or its users/ User Accounts; or (ii) by Supplier or a third party on the Customer's or its users' instructions; and/or (b) provided to Supplier by (or on behalf of) the Customer or its users.
- **"Data Processing Agreement"** means the Supplier Data Processing Agreement incorporated into the Agreement via the Order Form (or other agreed written incorporation mechanism in the Agreement).
- "**Effective Date**" means the Contract date specified in the Order Form.

- "**Fees**" means the fees and charges specified in the Order Form.
- "**Hosted Services**" means the Supplier's hosting of the Supplier Platform, as described in the Order Form.
- "**Intellectual Property Rights**" means all copyrights (including copyright in computer software), database rights, rights in inventions, patent applications, patents, trademarks, trade names, know-how, service marks, design rights (whether registered or unregistered), trade secrets, rights in confidential information and all other industrial or intellectual property rights of whatever nature for the full duration of such rights, including any extensions or renewals.
- "**Law**" means any applicable laws, regulations, regulatory constraints, obligations, proclamations, rules (including binding codes of practice and statement of principles incorporated and contained in such rules), or applicable judgment of a relevant court of law which is a binding precedent, in each case in force in any jurisdiction that is or may be applicable to this Contract.
- "**Order Form**" means the order form referenced in the Agreement.
- "**Site-specific Documents**" means documents or content embedded within the Customer's subscription which will be fully integrated into the semantic search functionality of the Supplier's platform. The quantity of Site-Specific Documents may vary as specified in the Order Form.
- "**Supplier**" means the Supplier identified in the Order Form.
- "**Supplier Platform**" means the Supplier's platform described in the Order Form, including all new releases, new versions, updates, and modifications thereto.
- "**User Account**" means an individual account within the Customer's subscription, allowing an authorised individual to access and utilise the Hosted Services provided under this Contract. The number of User Accounts may vary as specified in the Order Form.

TERMS AND CONDITIONS

1. FORMATION AND PRECEDENCE

1.1. This Contract is formed (and becomes legally binding) when the parties complete and sign the Order Form.

1.2. If there is any inconsistency, the order of precedence set out in the Agreement shall apply. Subject to that, as between these Terms & Conditions, the Order Form and any documents incorporated into this Contract, the following order of precedence shall apply: (a) first these Terms & Conditions; (b) second the Order Form; (c) third documents incorporated into this Contract.

1.3. This Contract governs the performance of the Hosted Services to the exclusion of all other terms and conditions, including any terms and conditions put forward by the Customer.

1.4. The following documents are incorporated into, and form part of, this Contract, to the extent set out or expressly referred to in the applicable Order Form:

a) the Supplier Service Level Agreement (“Supplier SLA”) (Schedule 1);

b) the Supplier Specific Shared Responsibility Model (“SRM”) (Schedule 2); and

c) the Supplier Data Processing Agreement (“Supplier DPA”) (Schedule 3);

2. HOSTED SERVICES

2.1. Supplier shall provide Hosted Services with reasonable skill and care in accordance with good industry practice, subject to the terms of this Contract and provided that Supplier does not warrant that the Customer’s use of Hosted Services will be uninterrupted or free from viruses or errors.

2.2. The Supplier warrants that the Hosted Services will comply in all material respects with the description of the Hosted Services in the Order Form.

2.3. Supplier shall not be responsible for any failure to provide Hosted Services as a result of: (a) a failure by the Customer to comply with its responsibilities under this Contract; and/or (b) errors in or corruption of the Connectivity Infrastructure, and/or the Customer Data.

2.4. Subject to the Agreement and to the fullest extent permitted by law, the Supplier hereby excludes all implied warranties (whether set out in statute or under common law), including (but not limited to) fitness for purpose and satisfactory quality.

2.5. Subject to payment of the Fees and compliance with this Contract, the Supplier grants the Customer a non-exclusive, non-transferable right during the term stated in the Order Form to access and use the Hosted Services for the Customer’s internal business purposes by its authorised users.

3. NO IMPLIED RIGHTS

3.1. Nothing in this Contract shall confer upon the Customer any ownership or licence rights in the Supplier Platform, its source code, data models, algorithms, or training datasets. All rights not expressly granted are reserved to the Supplier.

4. DATA USE FOR SERVICE IMPROVEMENT

4.1. The Supplier may use usage data to improve and audit the Hosted Services, provided such use does not identify the Customer or any individual and does not involve processing of Customer Data other than as permitted under the Data Processing Agreement.

5. CONFIDENTIALITY

5.1. Each party that receives ("Receiving Party") non-public business or financial information ("Confidential Information") from the other (or the other's Affiliates) ("Disclosing Party"), whether before or after the date of this Contract shall:

5.1.1. keep the Confidential Information confidential;

5.1.2. not disclose the Confidential Information to any other person other than with the prior written consent of the Disclosing Party or in accordance with this confidentiality Clause; and

5.1.3. not use the Confidential Information for any purpose other than the performance of its obligations or its enjoyment of rights under this Contract ("Permitted Purpose").

5.2. The Receiving Party may disclose Confidential Information to its own, or any of its Affiliates, officers, directors, employees, agents and advisers who reasonably need to know for the Permitted Purpose (each a "Permitted Third Party"), provided that the Receiving Party shall remain liable to the Disclosing Party for the acts, omissions, and compliance with the terms of this Clause of such Permitted Third Party as if such Permitted Third Party was the Receiving Party (and a party to this Contract). The Receiving Party shall ensure that each Permitted Third Party is made aware of and complies with all the Receiving Party's obligations of confidentiality under this confidentiality Clause.

5.3. If required by Law, the Receiving Party may disclose Confidential Information to a court or regulatory authority or agency, provided that the Receiving Party shall (if legally permissible) provide reasonable advance notice to the Disclosing Party and co-operate with any attempt by the Disclosing Party to obtain an order for providing for the confidentiality of such information.

5.4. The parties agree that any breach of the restrictions contained in this Clause may cause irreparable harm to the innocent party, whereupon the innocent party shall be entitled to injunctive relief without the necessity of proving damages or the inadequacy of money damages, posting any bond or other security in addition to all other legal or equitable remedies.

6. DATA RETRIEVAL, OFF-BOARDING AND EXIT PLAN

6.1. Upon termination or expiry of this Contract, the Supplier shall make available for download a machine-readable export of the Customer Data held within the Hosted Services for a period of thirty (30) days after termination.

6.2. The Supplier shall have no obligation to assist with migration or data transformation beyond the provision of this standard export, except to the extent required by the Agreement (including the Exit Management provisions).

6.3. Where requested, the Supplier will provide reasonable assistance to support transition or handover to the Customer or an alternative provider, including data migration guidance, knowledge transfer and continuity planning, to the extent applicable. Any such assistance shall be chargeable at the Supplier's standard professional services rate and must be pre-agreed in writing.

6.4. The Supplier shall co-operate with the Customer to ensure minimal disruption during the exit process and shall securely return or destroy Customer Data in accordance with this Clause.

6.5. After the thirty-day period, the Supplier shall securely delete or anonymise remaining Customer Data, except where retention is required by law or for audit purposes.

7. AI OUTPUT AND NON-RELIANCE DISCLAIMER

7.1. The Customer acknowledges that AI Outputs are generated using probabilistic algorithms and may contain inaccuracies, omissions, or outdated information. The Supplier gives no warranty or representation as to the accuracy, completeness, or suitability of any AI Output for any particular purpose. The Hosted Services are designed to provide traceable outputs with source references where available, but outputs may still contain errors or omissions.

7.2. The Customer shall not rely solely on any AI Output for operational, compliance, or decision-making purposes and must independently verify such information using qualified personnel.

7.3. To the extent permitted by applicable law and subject to the liability provisions of the Call-off Contract, the Supplier shall not be liable for any losses, damages, or incidents arising from reliance on any AI Output.

8. CLINICAL AND SAFETY LIMITATION

8.1. The Hosted Services and AI Outputs are not designed or intended for Clinical Use, including diagnosis, treatment, or patient care. The Supplier shall have no liability for any decision, action, or omission taken in reliance upon any AI Output in a clinical or patient-impacting context.

8.2. The Customer is responsible for ensuring that the Hosted Services are not used for Clinical Use and for ensuring that appropriately qualified personnel review and verify any AI Outputs before use in operational decision-making.

9. ASSIGNMENT AND SUBCONTRACTING

9.1. Neither party shall assign or otherwise transfer this Contract or any of its rights and duties under this Contract without the prior written consent of the other, such consent not to be unreasonably withheld or delayed.

9.2. Supplier may sub-contract the performance of any of its duties. The rights and liabilities of the parties hereto are binding on, and shall inure to the benefit of, the parties and their respective successors and permitted assigns. The Supplier remains responsible for the acts and omissions of its subcontractors.

10. CHANGES

10.1. No changes to this Contract shall be valid unless made in writing and signed by the authorised representatives of both parties.

11. GENERAL PROVISIONS

11.1. **Third Party Rights.** The parties hereby exclude to the fullest extent permitted by law any rights of third parties to enforce or rely upon any of the provisions of this Contract and the provisions of the Contracts (Rights of Third Parties) Act 1999 shall not apply.

11.2. **Relationship.** Nothing in this Contract shall render the Customer a partner or an agent of the Supplier and the Customer shall not purport to undertake any obligation on the Supplier's behalf nor expose the Supplier to any liability nor pledge or purport to pledge the Supplier's credit.

11.3. **Entire Contract.** This Contract supersedes any prior contracts, arrangements and undertakings between the parties in relation to its subject matter and constitutes the entire Contract between the parties relating to the subject matter.

11.4. **Severance.** If any part of this Contract is held unlawful or unenforceable that part shall be struck out and the remainder of this Contract shall remain in effect.

11.5. **No Waiver.** No delay, neglect or forbearance by either party in enforcing its rights under this Contract shall be a waiver of or prejudice those rights.

11.6. **No Bribery.** Each party warrants to the other that it: (a) has not and will not commit an offence under the Bribery Act 2010 in relation to this Contract or any other contract between the parties; and (b) has adequate procedures (as defined in section 7(2) of that Act) in place to prevent its associated persons from committing an offence under that Act.

11.7. **Force Majeure.** Neither party shall be liable for any failure or delay in the performance of its obligations under this Contract (other than payment obligations) to the extent that such failure or delay is caused by an event or circumstance beyond its reasonable control, including but not limited to acts of God, flood, fire, epidemic or pandemic, war, terrorism, civil unrest, strikes or industrial disputes (other than involving its own workforce), failure of utilities or telecommunications networks, or failure of third-party hosting providers ("Force Majeure Event"). Where a Force Majeure Event occurs, the affected party shall promptly notify the other party and use reasonable

endeavours to mitigate the impact of the Force Majeure Event. The affected party's obligations under this Contract shall be suspended for the duration of the Force Majeure Event, but this Contract shall otherwise remain in full force and effect.

11.8. **Counterparts.** This Contract may be executed in any number of counterparts and by each of the parties on separate counterparts each of which when executed and delivered shall be deemed to be an original, but all the counterparts together shall constitute one and the same Contract.

11.9. **Notices.** All notices (which include invoices and correspondence) under this Contract shall be in writing and shall be sent to the address of the recipient set out in this Contract or to such other address as the recipient may have notified from time to time. Any notice may be delivered personally, by a reputable courier service, by first-class post, or by email and shall be deemed to have been served if by hand when delivered, if by courier service or first-class post 48 hours after delivery to the courier or posting (as the case may be), or if by email immediately.

11.10. **Freedom of Information and Transparency.** The Customer acknowledges that it may be subject to the Freedom of Information Act 2000 ("FOIA") and/or the Environmental Information Regulations 2004 ("EIR"). The Supplier shall provide such reasonable assistance as the Customer may request to enable the Customer to comply with its obligations under FOIA or EIR, including in relation to requests for information relating to this Contract. The Supplier acknowledges that any information disclosed to the Customer may be disclosed in response to a valid request under FOIA or EIR, save where an exemption applies. The Supplier shall not prevent the Customer from complying with its statutory disclosure obligations and shall not assert confidentiality over information solely to prevent disclosure where disclosure is required by law.

11.11. **Law.** This Contract is governed by the laws of England and the exclusive jurisdiction of the English courts.

SCHEDULE 1: SUPPLIER SERVICE LEVEL AGREEMENT (SLA)

1. PURPOSE AND STATUS

1.1. This Supplier Service Level Agreement ("SLA") describes the operational service levels, support arrangements and service management commitments applicable to the CompliMind Hosted Services.

1.2. This SLA forms part of the Agreement. If there is any conflict, the order of precedence set out in the Agreement applies.

1.3. This SLA does not override or amend the Agreement or the Terms & Conditions or any applicable Schedules.

2. SERVICES SCOPE

2.1. The Hosted Services comprise a browser-based Software-as-a-Service platform supporting estates and facilities teams with compliance, regulatory support and administration, including (as applicable to the subscription tier):

- Chat (AI-assisted regulatory and document support);
- Writing (assisted drafting and editing);
- Review (automated document review and compliance checking);
- Wiki (regulatory and organisational document library);
- Assurance and Policy Hubs; and
- Optional associated modules enabled through the Order Form.

2.2. The Hosted Services are hosted on UK cloud infrastructure and accessed via standard web browsers with no local installation required. Supported browsers are the current and previous major versions of Chrome, Edge and Firefox, and Safari where applicable.

3. SERVICE AVAILABILITY

3.1. The CompliMind platform is designed to be available 24 hours per day, 7 days per week.

3.2. The underlying cloud infrastructure is provided by a third-party cloud service provider, which operates under a 99.9% availability SLA across core infrastructure services (compute, storage and networking).

3.3. CompliMind actively monitors service availability and performance but does not provide a separate contractual uptime guarantee beyond the commitments set out in the Agreement.

4. SERVICE ACCURACY DISCLAIMER

4.1. The Supplier endeavours to maintain the accuracy and reliability of the information provided through its Hosted Services. However, the Supplier gives no representation or warranty that any AI Output or information provided is accurate, complete, or up to date.

4.2. The Hosted Services are provided on an "as is" and "as available" basis without warranty of any kind. Customers must not use the Hosted Services

as the sole basis for any significant operational or safety-related decisions and must independently verify all information obtained.

4.3. For the avoidance of doubt, the CompliMind platform is not a medical device under applicable law and is not intended for clinical decision-making or any use affecting patient care.

4.4. The Supplier disclaims all liability for any indirect or consequential loss, including loss of profit, revenue, anticipated savings, or reputation, arising from reliance on any AI Output, subject always to applicable law and the liability cap set out in the Call-off Contract.

5. SUPPORT HOURS AND CONTACT CHANNELS

5.1. Standard support hours are: Monday to Friday, 09:00–17:00 (UK time), excluding public holidays.

5.2. Support is available via: email; telephone; and video call where appropriate.

5.3. Customers may also schedule technical or service review meetings during standard support hours.

6. INCIDENT CLASSIFICATION AND RESPONSE TARGETS

Incidents are prioritised based on severity:

a) Severity 1 – Critical
- Complete loss of service or significant security incident.
- Target initial response: within 4 business hours (Business Hours means 09:00–17:00 UK time Monday to Friday excluding UK public holidays.)
- Personal data breaches are handled in accordance with the Supplier Data Processing Agreement.

b) Severity 2 – High
- Material degradation of Hosted Services affecting multiple users or key functionality.
- Target initial response: **within 1 business day**.

c) Severity 3 – Medium
- Partial loss of functionality or issue with an available workaround.
- Target initial response: **within 2 business days**.

d) Severity 4 – Low
- Minor issues, usage queries or enhancement requests.
- Target initial response: **within 5 business days**.

Response targets relate to acknowledgement and investigation, not guaranteed resolution times.

7. INCIDENT MANAGEMENT

7.1. All incidents are logged and tracked internally by the CompliMind engineering team.

7.2. Incidents are reviewed and prioritised by the CTO or a delegated engineering lead.

7.3. For significant incidents, summary information may be provided to the customer on request.

8. PLANNED MAINTENANCE AND UPDATES

8.1. Planned maintenance is rare and, where service disruption is expected, is normally scheduled outside standard business hours.

8.2. Customers are notified in advance of planned maintenance wherever reasonably practicable.

8.3. The platform receives regular updates to deliver feature improvements, security patches and performance enhancements. Updates are deployed using controlled release processes designed to minimise disruption.

9. OUTAGE AND RESILIENCE MANAGEMENT

9.1. Service resilience is supported through the third-party cloud service provider's redundancy, monitoring and disaster recovery capabilities, including geographically separate UK regions and automated replication.

9.2. In the event of a third-party cloud service provider outage or degradation, CompliMind follows its incident management and communication procedures to keep customers informed until service restoration.

10. DATA BACKUP AND RESTORATION (OPERATIONAL)

10.1. The platform employs automated backups stored within a third-party cloud service provider's UK regions.

10.2. Backups are encrypted and support low-hour Recovery Point Objectives (RPO) and same-business-day Recovery Time Objectives (RTO) for critical data.

10.3. Further detail on backup and restoration processes can be provided on request.

11. BUSINESS CONTINUITY

11.1. CompliMind maintains a documented Business Continuity and Disaster Recovery Plan covering hosting, development and support operations.

11.2. Continuity measures include:

- multi-region cloud hosting;
- automated fail-over and replication;
- off-site backups; and
- a distributed remote workforce model.

11.3. As a browser-based, non-clinical system, CompliMind operates independently of customer internal network resilience.

12. ONBOARDING, TRAINING AND SERVICE MANAGEMENT

12.1. The onboarding approach and any on-site sessions are subject to agreement in the Order Form, and may include:

- a kick-off meeting;

- configuration support;
- Champion training sessions; and
- access to onboarding tutorials and guidance materials.

12.2. Ongoing service management includes:

- performance monitoring;
- access to regular training and masterclasses; and
- ad-hoc support and refresher sessions on request.

13. SERVICE CONSTRAINTS

13.1. The Hosted Services are configurable through the user interface but are not customised at code level.

13.2. The Hosted Services perform best on desktop or laptop devices and are not yet fully optimised for mobile use.

13.3. Access requires standard web browser compatibility and HTTPS connectivity.

14. FINANCIAL RECOMPENSE

14.1. CompliMind does not operate a formal service-credit or financial recompense scheme for service availability or performance.

14.2. Where availability is materially impacted, CompliMind will work with affected customers to assess the impact and discuss appropriate remedial or support measures, subject to the Agreement.

15. PROFESSIONAL JUDGEMENT AND USE OF OUTPUTS

15.1. The Hosted Services support customers by assisting with information retrieval, drafting and review activities.

15.2. Customers remain responsible for exercising professional judgement and verifying outputs before use in operational or compliance contexts.

15.3. The Hosted Services do not replace internal governance processes or professional expertise.

SCHEDULE 2: SUPPLIER SPECIFIC SHARED RESPONSIBILITY MODEL (SRM)

1. PURPOSE AND STATUS

1.1. This Supplier Specific Shared Responsibility Model (the **Model**) describes the division of security and operational responsibilities between the **Supplier** and the **Customer** for the Hosted Services.

1.2. This Model is descriptive and intended to support implementation, governance and assurance. It does not override or amend the Agreement. If there is any conflict, the order of precedence set out in the Agreement applies.

1.3. This Model applies to the Hosted Services delivered as **Software-as-a-Service (SaaS)**, accessed via standard web browsers over HTTPS and hosted on **a third-party cloud service provider in the UK**. Feature availability depends on the licence tier and modules enabled in the Order Form.

2. SERVICE BOUNDARIES AND SHARED RESPONSIBILITY PRINCIPLES

2.1. The Supplier is responsible for securing the Hosted Services and the components it operates and controls, including the platform application, tenant segregation controls, and the Supplier-managed cloud configuration within a third-party cloud service provider.

2.2. The Customer is responsible for securing its own environment and use of the Hosted Services, including user access, endpoints, networks, internal governance processes, and decisions about what data and documents are uploaded and shared.

2.3. The Hosted Services support estates, facilities, governance and assurance workflows. Outputs are designed to be **traceable to underlying sources where available**. The Customer remains responsible for professional judgement, verification and approval of outputs before use.

2.4. The Hosted Services are not intended for Clinical Use. The Customer is responsible for ensuring the Hosted Services are not used for clinical decision-making or patient care.

2.5. Where optional modules, integrations, or enhanced migration support are procured, responsibilities may be further specified in the Order Form and any agreed implementation plan.

3. RESPONSIBILITY ALLOCATION TABLE

The table below shows the primary allocation of responsibilities. “Shared” means both parties have responsibilities that must be performed for the control to be effective.

3.1. GOVERNANCE AND ASSURANCE

Area	Supplier responsibility	Customer responsibility	Allocation
Overall service governance	Provide service documentation, onboarding guidance, and operational processes for the Hosted Services.	Apply Customer governance processes for using AI and cloud services (IG, security, procurement), and ensure appropriate approvals for use.	Shared
Organisational and personal libraries	Provide storage, indexing and access controls for organisational and personal libraries in the platform.	Maintain and govern Customer-uploaded content, including ownership, versioning decisions, retention expectations and appropriateness of content.	Customer
Outputs and decision making	Provide outputs to assist workflows, with references to underlying sources where available.	Verify outputs and apply professional judgement. Approve documents through Customer governance processes.	Shared
Non-clinical limitation	Provide clear service limitation statements in service materials and contracts.	Ensure the Hosted Services are not used for Clinical Use.	Shared

3.2. IDENTITY, ACCESS AND TENANT CONTROLS

Area	Supplier responsibility	Customer responsibility	Allocation
Tenant segregation	Provide logical segregation of each organisation's data at tenant level.	Configure internal sharing rules and operational processes for cross-team sharing within the organisation.	Shared
Authentication and session security	Operate platform authentication and session controls.	Provision and de-provision users promptly (joiners/movers/leavers). Ensure users protect credentials and follow Customer security policies.	Shared
Role-based access control (RBAC)	Provide RBAC functionality and apply permissions as configured.	Define role groups and least-privilege access appropriate to job roles and modules. Review access periodically.	Shared
Browser and endpoint hygiene	N/A	Maintain supported browsers, endpoint patching, device security controls and secure use on Customer-managed devices.	Customer
Network access	Provide the Hosted Services over HTTPS with standard browser access.	Provide network connectivity and allow access through Customer networks where permitted.	Shared

3.3. DATA HANDLING, CLASSIFICATION AND CONTENT GOVERNANCE

Area	Supplier responsibility	Customer responsibility	Allocation
Data residency and hosting location	Store and process customer data within EEA and UK jurisdictions on a third-party cloud service provider's UK and EEA infrastructure, subject to Subprocessors listed in the DPA for analytics/monitoring where enabled.	Approve (or decline) use of optional analytics/monitoring features where relevant to Customer assurance, and apply internal risk acceptance processes.	Shared
Upload decisions and data minimisation	Provide platform capability to upload and manage content.	Decide what content to upload, ensuring minimisation, legality, and alignment with Customer policies.	Customer
Special category data	Process only on the Customer's instructions in accordance with the DPA where such data is included in Customer Data.	Avoid uploading special category data unless a lawful basis and safeguards are in place. Apply redaction where appropriate.	Customer
Data accuracy and currency (Customer content)	Preserve integrity of stored content and provide platform features to support search and access.	Ensure uploaded content is accurate, current, and appropriate for use. Maintain document lifecycle and review schedules (unless using configured Policy Hub prompts).	Shared
Data export and exit	Provide standard export mechanisms and cooperate with exit as required by the Agreement.	Plan internal migration and validate exported data meets Customer needs. Handle exported data securely in Customer systems.	Shared

3.4. SECURITY CONTROLS AND OPERATIONAL SECURITY

Area	Supplier responsibility	Customer responsibility	Allocation
Security controls (Supplier scope)	Implement technical and organisational measures consistent with the DPA Security Measures, including encryption in transit and at rest, privileged access controls, and security logging within Supplier systems.	Maintain Customer-side security controls for devices, identity governance, and internal monitoring.	Shared
Vulnerability and patch management	Patch and maintain Supplier-managed components and configurations; deploy updates through controlled release processes.	Patch Customer-managed devices and browsers. Maintain internal controls for software versions and secure configurations.	Shared
Monitoring and logging	Log security events and administrative actions within Supplier scope; review high-risk events and investigate.	Report suspected misuse or incidents; use Customer governance and processes for internal investigations.	Shared
Incident response	Contain, investigate and remediate incidents within Supplier scope; communicate with customers for significant incidents.	Contain and remediate incidents within Customer scope; coordinate internal comms and escalation.	Shared
Personal Data Breach	Notify and assist in accordance with the DPA.	Decide on notifications as Controller and comply with Customer obligations.	Shared

3.5. BACK-UP, RESTORATION AND CONTINUITY

Area	Supplier responsibility	Customer responsibility	Allocation
Backups	Operate automated encrypted backups within a third-party cloud service provider's UK regions, supporting low-hour RPO and same-business-day RTO for critical data (operational targets).	Specify any additional retention requirements before ordering. Maintain internal continuity planning for access to critical documents if required by Customer policy.	Shared
Restoration	Restore service data within Supplier scope following incidents, subject to operational processes and dependencies.	Validate restored content and manage local workarounds during service disruption.	Shared
Business continuity	Maintain BC/DR plan for hosting, development and support operations, including multi-region hosting and remote workforce operations.	Maintain Customer continuity processes for governance and assurance activities relying on the Hosted Services.	Shared

3.6. INTEGRATIONS AND OPTIONAL MODULES

3.6.1. Where the Customer procures integrations (for example with CAFM, DMS or SharePoint workflows) or optional modules, responsibilities are shared as follows:

a) Supplier: provide integration mechanisms within Supplier scope and agree a secure transfer method; implement configuration agreed in writing.

b) Customer: provide required access, permissions, credentials, and internal approvals; ensure data shared via integrations is lawful and appropriate.

3.6.2. Any module-specific responsibilities (for example Appointment Matrix governance in Training Hub, or workflow ownership in Policy Hub) will be determined by the Customer and set out in the Order Form and/or implementation plan where needed.

4. CUSTOMER RESPONSIBILITIES SUMMARY

The Customer is responsible for:

- governance approvals for using the Hosted Services and AI tools
- user lifecycle management and permission design
- endpoint, browser and network security
- deciding what content is uploaded, including minimisation and classification

- avoiding special category data unless properly governed
- verifying outputs and ensuring the Hosted Services are not used for Clinical Use
- handling exported data securely and managing migration planning

5. SUPPLIER RESPONSIBILITIES SUMMARY

The Supplier is responsible for:

- operating the SaaS platform and securing Supplier-controlled components
- tenant segregation and RBAC capabilities within the platform
- encryption, logging, and security controls within Supplier scope
- backups and continuity measures within Supplier scope
- incident management and breach notification assistance per the DPA
- maintaining the Supplier-managed regulatory library included with the Hosted Services.

6. REVIEW AND UPDATES

6.1. The Supplier may update this Model for future Agreements.

6.2. For this Agreement, the applicable version is the version referenced or incorporated in the Order Form and it may only be varied in accordance with clause 10.1 of the Supplier Terms and Conditions.

SCHEDULE 3: SUPPLIER DATA PROCESSING AGREEMENT (DPA)

1. PURPOSE AND STATUS

1.1. This Supplier Data Processing Agreement ("DPA") sets out the terms on which the Supplier processes Personal Data on behalf of the Customer under the Agreement.

1.2. This DPA forms part of the Agreement where incorporated via the Order Form (or other agreed written incorporation mechanism in the Agreement).

1.3. This DPA applies only to the extent the Supplier processes Personal Data as a Processor on behalf of the Customer (as Controller) in connection with the Hosted Services.

1.4. If there is any inconsistency between this DPA and the Agreement (including the General Terms), the order of precedence set out in the Agreement shall apply.

1.5. This DPA does not limit either party's obligations under Data Protection Legislation. Where this DPA includes optional or additional provisions, they apply only to the extent they are consistent with the Agreement.

2. DEFINITIONS AND INTERPRETATION

2.1. Capitalised terms used but not defined in this DPA have the meaning given in the Agreement (including the Supplier Terms & Conditions where incorporated).

2.2. For the purposes of this DPA: "Data Protection Legislation" has the meaning set out in Clause 4.22.

2.3. "Personal Data", "Data Controller", "Data Processor", "Data Subject" and "Process" have the meanings given in Data Protection Legislation.

2.4. **"Subprocessor"** means any Data Processor engaged by the Supplier to process Personal Data on behalf of the Customer in connection with the Hosted Services.

2.5. **Part A** (Details of Processing), **Part B** (Security Measures), **Part C** (Approved Subprocessors) and **Part D** (Controller Instructions) form part of this DPA.

3. PROCESSING DETAILS

3.1. The subject matter, duration, nature and purpose of the processing, type of Personal Data and categories of Data Subjects are described in **Part A**.

3.2. The Customer instructs the Supplier to process Personal Data only as necessary to provide the Hosted Services and related support, in accordance with **Part D** and the Agreement.

4. DATA PROTECTION

4.1. Supplier shall not own (or claim ownership rights in respect of) Customer Data. The Customer is responsible for the accuracy, reliability, lawfulness,

and integrity of all Customer Data. The Customer warrants that Customer Data shall not be defamatory or offensive and that it, and its users, have all consents, licences and permissions (including the consent of any Data Subjects) in respect of Customer Data as are required for Customer (and its users) to lawfully upload, store, distribute, publish, share and/or Process the Customer Data (as applicable): (a) in/through Supplier Platform; and/or (b) to/with other users or any third parties who are authorised by the Customer or by Law to view/access the Customer Data. The Customer shall indemnify and hold harmless Supplier for Costs arising from a breach of this Clause, including all Costs associated with handling a complaint or allegation which, if substantiated, would constitute a breach by the Customer of this Clause.

4.2. The Customer acknowledges and agrees that the Supplier does not assume any responsibility for the voluntary ingestion of special category data (and/or criminal offence data) into the system by the Customer. The Customer is solely responsible for ensuring that any special category data inputted into the system is in compliance with applicable data protection laws and regulations, and for implementing appropriate measures to protect such data.

4.3. In relation to the Processing of any Personal Data in the Customer Data, the parties agree that the Customer and/or its user(s) is/are the Data Controller and Supplier is the Data Processor.

4.4. The Supplier shall notify the Customer immediately if it considers that any of the Customer's instructions infringe Data Protection Legislation.

4.5. The Supplier shall, at the Customer's request and expense, provide the Customer with reasonable assistance as is contemplated by Article 28(3)(f) of the UK GDPR including, but not limited to, the preparation of any Data Protection Impact Assessment prior to commencing any Processing of the Customer Data. Such reasonable assistance may, at the discretion of the Customer, include:

4.5.1. systematic description of the envisaged Processing operations and the purpose of the Processing;

4.5.2. an assessment of the necessity and proportionality of the Processing operations in relation to the Customer Data;

4.5.3. an assessment of the risks to the rights and freedoms of natural persons; and

4.5.4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

4.6. The Supplier shall, in relation to the Customer Data:

4.6.1. process that Customer Data only in accordance with the Customer's instructions, including as set out in this Clause and **Part D** to this DPA, unless the Supplier is required to do otherwise by law,

4.6.2. ensure that:

a) Supplier personnel do not Process the Customer Data except in accordance with this Clause;
b) it takes all reasonable steps to ensure the reliability and integrity of any Supplier personnel who have access to the Customer Data and ensure that they:
   (i) are aware of and comply with Supplier's duties under this Clause;
   (ii) are subject to appropriate confidentiality undertakings that are in writing and are legally enforceable;
   (iii) are informed of the confidential nature of the Customer Data and do not publish, disclose or divulge any of the Customer Data to any third party unless directed in advance and in writing to do so by the Customer or as otherwise permitted by this Clause; and
   (iv) have undergone adequate training in the use, care, protection and handling of Personal Data that enables them and Supplier to comply with their responsibilities under Data Protection Legislation and this Clause;

4.6.3. not transfer Personal Data outside the UK (but within the EEA), unless the prior written consent of the Customer has been obtained. Such consent to transfer may be conditional on Supplier entering into the Standard Contractual Clauses, or other appropriate data transfer mechanism (For the avoidance of doubt, consent may be provided in advance in accordance with **Part C**); and

4.6.4. at the written direction of the Customer, securely delete or return the Customer Data (and any copies of it) to the Customer promptly following the earlier of:

a) the termination or expiry of this Agreement; or
b) a request from the Customer;

in each case after completion of any agreed export and exit period under the Agreement.

4.7. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Supplier shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, but not limited to, as appropriate:

4.7.1. the encryption of Customer Data;

4.7.2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

4.7.3. the ability to restore the availability and access to Customer Data Processed further to this Clause, including transfers to third parties who are authorised by the Customer or by Law to view/access the

Customer Data in a timely manner in the event of a physical or technical incident; and

4.7.4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of Processing.

4.8. The Supplier shall not engage a Subprocessor to undertake the Processing of any Personal Data (within Customer Data), unless, prior to any Processing taking place by the Subprocessor, the Supplier:

4.8.1. notifies the Customer in writing of the intended Subprocessor and Processing;

4.8.2. enters into a written agreement with the Subprocessor which gives effect to the terms set out in this Clause such that they apply to the Subprocessor, including providing terms that provide at least the same level of protection for the Customer Data as this Clause and which meet the requirements of Data Protection Legislation;

4.8.3. informs the Customer of any addition or replacement of a Subprocessor; and

4.8.4. provides the Customer with such information regarding the Subprocessor as the Customer may reasonably require.

4.9. The Supplier may update the list of Subprocessors by notice in accordance with Clause 4.8, and Part C will be deemed updated accordingly.

4.10. The Customer's approval of Subprocessors and any associated processing locations in **Part C** constitutes the Customer's prior written consent to any corresponding transfers of Personal Data outside the UK (but within the EEA), for the purposes of Clause 4.6.3, subject always to implementation of an appropriate transfer mechanism where required by Data Protection Legislation.

4.11. The Supplier shall ensure that any Subprocessor's access to the Personal Data (within Customer Data) terminates automatically on termination of the Agreement for any reason, save that any Subprocessor may access the Customer Data in order to securely destroy it.

4.12. The Supplier shall remain fully liable for all acts or omissions of any Subprocessor.

4.13. The Supplier shall notify the Customer without undue delay if it:

4.13.1. receives a request from Data Subjects in connection with Customer Data;

4.13.2. receives any other request for information, complaint or communication relating to either Party's obligations under Data Protection Legislation connected with Customer Data;

4.13.3. receives any communication from the Information Commissioner's Office or any other regulatory or supervisory body connected with Customer Data; or

4.13.4. receives a request from any third party for disclosure of Customer Data.

4.14. The Supplier shall provide reasonable assistance to enable the Customer to respond to requests from Data Subjects to exercise their rights under Data Protection Legislation, to the extent the Supplier is permitted to do so and the Customer cannot reasonably obtain the information by other means.

4.15. The Supplier shall not respond substantively to the communications listed above save that it may respond to a regulatory or supervisory body following prior consultation with the Customer.

4.16. The Supplier's obligation to notify under this Clause includes the prompt provision of further information to the Customer in phases, as details become available.

4.17. The Supplier shall, without undue delay, notify the Customer in writing of any event that results in unauthorised Processing of Customer Data including, without limitation, destruction of Personal Data and including any Personal Data Breach (as defined by the UK GDPR). The Supplier shall provide such assistance as is reasonably requested by the Customer following a Personal Data Breach.

4.18. In the event of a Personal Data Breach the Supplier shall:

4.18.1. investigate the reasons for and circumstances of the Personal Data Breach;

4.18.2. take all necessary actions to prevent, contain, mitigate and remediate the Personal Data Breach;

4.18.3. if requested, assist the Customer with the provision of information or updates to Data Subjects whose Personal Data was affected by the Personal Data Breach;

4.18.4. provide the Customer with all information requested by the Customer to enable the Customer to verify Supplier's compliance with this Clause and Data Protection Legislation.

4.19. The Supplier shall, at the Customer's expense, allow the Customer or the Customer's appointed representatives to audit and inspect its activities in relation to the Processing of Customer Data to enable the Customer to verify the Supplier's compliance with this Clause, and the Supplier shall cooperate and provide reasonable assistance to the Customer (and its representative) with each audit and inspection.

4.20. The Supplier shall, in connection with the Customer Data, maintain complete and accurate records and information to demonstrate its compliance with this Clause and Data Protection Legislation.

4.21. Neither Party shall do nor omit to do anything that will put the other Party in breach of Data Protection Legislation.

4.22. For the purposes of this Clause, "Data Protection Legislation" means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic

Communications Regulations 2003 and any related act or regulation in the UK, including statutory modification or re-enactment of it, and “Data Controller”, “Data Subject”, “Personal Data”, “Data Processor”, and “Process” shall have the meaning specified in the UK GDPR (as amended).

SCHEDULE 3: PART A – DETAILS OF PROCESSING (UK GDPR ARTICLE 28)

1. SUBJECT MATTER OF PROCESSING

Provision of the Hosted Services and related support, including hosting, storage, access management, user support, service monitoring, backup and restoration, and (where enabled) AI-assisted features used to process and generate outputs based on Customer-provided inputs.

2. DURATION OF PROCESSING

For the term of the Agreement and any agreed exit period, plus any retention period required by applicable law.

3. NATURE AND PURPOSE OF PROCESSING

Processing necessary to:

- provide and maintain the Hosted Services;
- manage user accounts, authentication and access controls;
- store, retrieve, display, export and otherwise make available Customer Data within the platform;
- provide support, troubleshooting and service communications;
- perform security monitoring, logging, backup, disaster recovery and resilience operations; and
- where applicable, perform AI-assisted processing on Customer inputs and documents to support search, drafting and review workflows.

4. TYPES OF PERSONAL DATA (TO THE EXTENT INCLUDED IN CUSTOMER DATA)

- Customer account data (name, email address, role/job title, organisation, authentication identifiers).
- Content uploaded or created by users (documents, text, meeting minutes, action logs, policies, SOPs, and related metadata).
- Usage and audit logs (timestamps, actions, access events).
- Support correspondence and service tickets.

5. CATEGORIES OF DATA SUBJECTS

Users and other personnel of the Customer (employees, contractors, agency staff) and any other individuals whose Personal Data is contained in documents uploaded by the Customer.

6. SPECIAL CATEGORY DATA

The Hosted Services are not intended for special category data. Where the Customer chooses to upload such data, it forms part of Customer Data and is processed only in accordance with the Customer's instructions and this DPA.

SCHEDULE 3: PART B – SECURITY MEASURES

The Supplier implements technical and organisational measures appropriate to risk, including (as applicable):

1. HOSTING AND RESILIENCE

- Hosting in a third-party cloud service provider's UK regions with redundancy and monitoring.
- Business continuity and disaster recovery controls, including replication and failover capabilities.

2. ENCRYPTION

- TLS 1.2+ encryption in transit.
- AES-256 (or a third-party cloud service provider-managed equivalent) encryption at rest.

3. ACCESS CONTROLS

- Role-based access control with least-privilege principles.
- Segregation of customer data by logical tenancy.

4. SECURITY MONITORING AND LOGGING

- Central logging of security events and administrative actions.
- Incident response procedures and escalation for significant security events.

5. BACKUPS

- Encrypted automated backups stored within a third-party cloud service provider's UK regions.
- Recovery targets aligned to low-hour RPO and same-business-day RTO for critical data (subject to incident type and dependency impacts).

6. PEOPLE AND PROCESS

- Personnel confidentiality undertakings and security training.
- Secure development and change management practices.

SCHEDULE 3: PART C – APPROVED SUBPROCESSORS (AND LOCATIONS)

The following Subprocessors are approved for the purposes of Clause 4.9 and Clause 4.6.3, subject to the Supplier's obligations to notify the Customer of additions or replacements in accordance with the DPA:

1. **Microsoft Azure** (hosting and infrastructure) – United Kingdom.
2. **Google Cloud** (analytics and monitoring support, where enabled) – European Union/EEA.
3. **PostHog** (product analytics, where enabled) – European Union/EEA.
4. **Langfuse** (observability/monitoring, where enabled) – European Union/EEA.
5. **Hubspot** (CRM) – European Union/EEA.
6. **Customer.io** (Email communication) – European Union/EEA.

Notes:

- The Supplier may add or replace Subprocessors only in accordance with **Clause 4.8** (and the notification/consent approach in **Clause 4.9**).
- Where Subprocessors are located outside the UK, the Customer's prior written consent is provided via incorporation of this DPA and **Part C**, and any required transfer mechanism (including SCCs) will be implemented where applicable.

SCHEDULE 3: PART D – CONTROLLER INSTRUCTIONS

The Customer instructs the Supplier to process Personal Data within Customer Data only as necessary to:

1. Provide the Hosted Services described in the Order Form, including hosting, storage, retrieval, display, search, export, collaboration features, and the ongoing improvement of the Hosted Services.
2. Provide support and service management, including:
    - incident management and troubleshooting;
    - responding to support requests;
    - communicating service notices; and
    - maintaining service continuity.
3. Operate security, monitoring, logging, backup and restoration processes consistent with the Supplier's security and operational controls.
4. Process Customer Data using AI-assisted functionality only as initiated by users through the platform's features, and only to provide outputs to the Customer within the Hosted Services (unless otherwise agreed in writing in the Agreement and the Order Form).
5. Delete or return Customer Data in accordance with the Agreement and Clause 4.6.4 (including on termination/expiry or written request), subject to legal retention requirements.