**TRIAL EVALUATION AGREEMENT**

**TERMS AND CONDITIONS**


**THIS TRIAL EVALUATIONAGREEMENT ("AGREEMENT") IS BETWEEN: (i) LUMINANCE TECHNOLOGIES LTD, A PRIVATE LIMITED COMPANY REGISTERED IN ENGLAND AND WALES WITH COMMERCIAL REGISTRATION NUMBER  09857705 AND ITS REGISTERED ADDRESS AT 5TH FLOOR, 20 STATION ROAD, CAMBRIDGE, ENGLAND, CB1 2JD ("LUMINANCE") AND (ii)  THE ENTITY OR ORGANIZATION  TO WHICH YOU AS A USER OF THE PRODUCT IS AN EMPLOYEE, THIRD PARTY USER AND/OR AUTHORISED AGENT ("CUSTOMER" OR "YOU"). THESE TERMS AND CONDITIONS FORM A LEGALLY BINDING AGREEMENT BETWEEN YOU AND LUMINANCE. BY TICKING THE BOXES BELOW YOU ARE ACCEPTING THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD THIS AGREEMENT, AND YOU AGREE (ON YOUR OWN BEHALF OR, IF YOU REPRESENT AN ENTITY OR OTHER ORGANIZATION, ON BEHALF OF THAT ENTITY OR ORGANIZATION AND ANY OTHER INDIVIDUALS WITHIN THAT ENTITY OR ORGANIZATION USING OR ACCESSING THE OFFERING) TO BE BOUND BY THE TERMS AND CONDITIONS AS OF THE DATE ON WHICH YOU ACCEPT BELOW (SUCH DATE, THE "COMMENCEMENT DATE").**

### Defined Terms

Terms defined shall have the meanings given below.  Defined terms may be used in the singular or plural depending on the context.

"**Additional Generative Models**" means any large language models or additional generative AI models which are technologies or systems that are developed, hosted, or managed by a third-party provider external to Luminance or in partnership with Luminance;

"**Ask Lumi**" means the additional interactive Product interface (which the Customer may opt-in to using by selecting it within the Product) created by Luminance;

"**AWS Region**" means a geographic hosting location as provided by Amazon Web Services and its sub-processors (as detailed at https://aws.amazon.com/compliance/sub-processors and as may be updated from time to time);

"**Commencement Date**" means the date these terms and conditions are accepted by the Customer as per ticking the boxes below and clicking submit;

"**Customer Data**" means any documents, data that Customer uploads to the Product under this Agreement (which, for the avoidance of doubt, may include information about underlying legal documents, metadata related to those documents, and the results of analysis thereof);

"**Data Protection Laws**" means all applicable data protection and privacy legislation in force from time to time, including (without limitation): (a) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR"); (b) EU GDPR, as incorporated by the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018 (DPA) and as amended and updated by applicable UK secondary legislation ("UK GDPR"); (c) the California Consumer Privacy Act 2018 ("CCPA"); (d) the Privacy and Electronic Communications Regulations 2003 (PECR); and (e) laws relating to personal data and privacy or of similar purpose or effect in any relevant jurisdiction; in each case as amended, updated, re-enacted or replaced from time to time.  The terms "Data Controller", "Data Processor", "Data Subject", "Personal Data", "Personal Data Breach" and "processing" shall have the meanings ascribed to them in the GDPR or the UK GDPR, as applicable;

"**Intellectual Property**" means patents, trademarks, service marks, rights (registered or unregistered) in any designs, applications for any of the foregoing, trade or business names,

copyright (including rights in computer software) and topography rights, know-how and other proprietary knowledge and information, internet domain names, rights protecting goodwill and reputation, database rights (including rights of extraction) and all rights and forms of protection of a similar nature to any of the foregoing or having equivalent effect anywhere in the world and all rights under licences and consents in respect of any of the rights and forms of protection mentioned in this definition (and "Intellectual Property Rights" shall be construed accordingly);

"**Documentation**" means user manuals for the Product consisting of the applicable installation guides, service descriptions, technical specifications, and online help files provided by Luminance or available on Luminance's online portal;

"**Learnings**" means the pseudonymised data obtained from the analysis and results Customer interactions, tagging and/or usage within the Product, including but not limited the intricacies of Customer engagement and patterns within the Product. This data does not contain any Personal Data, personally identifiable information and/or Confidential Information derived from Customer Data;

"**Private Learning**" means the clauses or data created as a result of Customer's training of the Product to recognize new clauses and new contract types within the Product;

"**Product**" means, one or all of Luminance's three proprietary software applications (Corporate, Diligence and/or Discovery) hosted on an AWS Region for reviewing and analysing Customer Data as identified and confirmed by Luminance via email, together with any fixes, updates, or enhancements thereto, but not including any additional modules, products or services that Luminance may make commercially available from time to time;

"**OOTB Models**" means Luminance's suite of legal concepts and out-of-the-box standard set of clauses provided with the Product;

"**Open Source Software**" means Third Party Software that Luminance utilises in the Software pursuant to a licence that requires, as a condition of use, modification and/or distribution of such software, that the software or other software combined and/or distributed with it be (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; (iii) redistributable at no charge; or (iv) redistributable but subject to other limitations;

"**Outputs**" means any reports, outputs and/or documentation (in each case, in human-readable form) generated by the Product based on the Customer Data uploaded to the Product by Customer;

"**PoV**" means this proof of value trial;

"**Retention Period**" means the thirty (30) day period from termination or expiration of this Agreement;

"**SCCs**" means the standard contractual clauses for the Personal Data transfers from an EU or UK controller to a processor established in third countries which do not ensure an adequate level of data protection as set out in (i) where the EU GDPR applies, the Annex to Commission Implementing Decision 2021/914 on Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679, pursuant to the European Commission Decision of 4 June 2021, as may be updated by the European Commission from time to time; or where the UK GDPR applies, the Standard Data Protection Clauses as issued by the Information Commissioner under s119A(1) DPA, in the form of an (i) International Data Transfer Agreement; or (ii) International Data Transfer Addendum to the EU Commission Standard Contractual Clauses;

"**Software**" means the Luminance or its licensor's proprietary software utilised by Customer through its usage of the Product, together with all enhancements, error corrections, and/or updates which are generally made available by Luminance as part of the Product. Open Source Software does not form part of the Software and is utilised by Customer directly on the terms of the applicable licences, provided that the Open Source Software will nevertheless be deemed to form part of the Software for the purposes of the support, such that Luminance supports it as if it were part of the Software;

"**Trial Period**" means: (i) two (2) weeks from the Commencement Date; or (ii) as otherwise specific by Luminance in writing via email at its sole discretion, with the latter taking precedence for the purposes of this Agreement;

"**Third Party Licensors**" means the suppliers of the Third Party Software to Luminance; and

"**Third Party Software**" means: (i) any software or other technology that is licensed to Luminance from Third Party Licensors which is not proprietary to Luminance, but which Luminance has the necessary rights to license to Customer; and (ii) Open Source Software;

"**Third Party User**" means a third party (including but not limited to Customer's Affiliate, service provider, consultant, or contractor) utlising the Product(s) with the Customer's permission and/or on behalf of the Customer.

**RECITALS**

A.   Luminance is the supplier of the commercially available Product.
B.   The Customer is interested in using the Product for its internal use and business purposes. Luminance has agreed to license the use of the Product on the terms of this Agreement.
C.   Luminance has agreed, by means of a PoV to demonstrate how the Product will fulfil the Customer's requirements to further achieve its business purpose.
D.   This Agreement was last updated on 01 April 2025.

**IT IS THEREFORE AGREED AS FOLLOWS:**

**1   TERM AND TERMINATION**
1.1   Customer may use the Product free of charge, from the Commencement Date and for the duration of the Trial Period, for evaluation purposes only. Save as stated in Clause 9.1 below, this Agreement and the rights to use the Product will terminate immediately upon the: (i) expiry of the Trial Period, or (ii) the signing of a product order form for the Product.
1.2   Either party may terminate this Agreement for convenience on seven (7) days' written notice via email to Finance@luminance.com; copying Legal@luminance.com at any time during the Trial Period.

**2   BETA TESTING**
2.1   If Luminance provides Customer with a non-commercially available Product for technical preview or beta testing (a "**Preview Product**"), Customer may use the Preview Product for evaluation purposes, in a non-production test environment only, for the period specified by Luminance (the "**Test Period**"). Customer shall test the Preview Product in accordance with any conditions specified in the readme file and/or any accompanying documentation, and shall gather and report test data, feedback, comments and suggestions to Luminance. Customer's right to use the Preview Product shall terminate upon expiry of the Test Period. Luminance makes no warranty it will release a commercial version of the Preview Product, or that a commercial version will contain the same or similar features as the Preview Product.
2.2   A staging environment may be made available to Customer from time-to-time for previewing a Preview Product. Such staging environment will, at Luminance's discretion, be either a shared environment or a private, separate instance of the Product. Staging environments are typically

made available at least two weeks prior to any major Product release and may be subject to charges.

**3    LICENCE GRANT AND RESTRICTIONS**

3.1    The Product and the Software shall throughout the term of this Agreement be the property of Luminance.

3.2    Subject to the terms and conditions of this Agreement, Luminance grants to Customer a non-exclusive, non-transferable, non-sub licensable, licence for the duration of the Trial Period: (i) access and use the Product(s) specified above, for Customer's internal business purpose (other than as a stand-alone commercial offering), relating to the processing and review of relevant Customer Data; (ii) use the Documentation; and (iii) make a commercially reasonable number of copies of the Documentation, provided that Customer reproduces all of Luminance's and its suppliers' copyright notices and proprietary legends on the original versions of the Documentation provided to Customer.

3.3    Save as expressly provided in Clause 3.2, the Customer will have no right to, will not, and will procure that none of its Third Party Users will, load, execute, copy, distribute, modify, create derivative works from, sublicense or otherwise enjoy, derive benefit from or exploit the Product or Third Party Software, or permit any other person to do so, and all of Luminance' rights in the Product and/ Third Party Software are fully reserved.

3.4    Third Party Software/Open Source Software. Customer acknowledges that the Product may contain or be accompanied by certain Third Party Software including Open Source Software. Open Source Software is copyrighted and licensed under the GPL/LGPL and other Open Source Software licences. Luminance shall be solely responsible for obtaining and maintaining (at its sole expense) all necessary licences and other rights to enable Customer to use the Product and to otherwise exploit the rights granted hereunder.

3.5    The Product will be hosted in an AWS Region of Luminance's discretion, unless otherwise agreed between Luminance and Customer in writing.

3.6    The Customer represents and warrants that they possess a valid Microsoft Office licence for any use of Cloudword.

**4    Customer Data**

4.1    For any Customer Data uploaded to the Product, Customer grants to Luminance a limited, non-exclusive, non-transferable, worldwide licence to access and use Customer Data to the extent necessary to provide Product improvements, Private Learning, Learnings, and Outputs. Customer shall ensure that (subject to Luminance's compliance with the confidentiality, data protection and other requirements in this Agreement), it is permitted to do so in accordance with applicable laws and regulations including, without limitation, applicable Data Protection Laws.

4.2    Customer Private Learning. The Product will learn from the Customer's usage of the platform and the interaction of Customer Data with OOTB Models to provide Outputs and Private Learning. Private Learning and Outputs shall vest with Customer, as set out in clause 8.3 of this Agreement, and be considered Customer Confidential Information. Customer shall not retain any Intellectual Property Rights in OOTB Models.

4.3    Luminance Learnings. Luminance may retain and utilise on a perpetual basis any Learnings of the Product to develop or improve the Product, provided that Luminance ensures no Customer Confidential Information or Personal Data is contained therein and Customer is not identified or identifiable as the source.

**5    THIRD PARTY USERS**

5.1    If Customer permits a Third Party User to access and/or use the Product (as a result of the rights granted under clause 3 of this Agreement to the Customer) whether as the Customer's agent, on the Customer's behalf, or for any other purposes, Customer may only do so subject to the

conditions set out in this clause 5.

5.2 The Third Party User shall only use the Product subject to terms and conditions that are consistent with the rights and limitations set out in this Agreement. The Third Party User will be deemed to have accepted all of the terms and conditions of this Agreement as if Customer had directly used the Product. Customer shall remain liable for any and all acts and omissions of the Third Party User under this Agreement.

**6    LEGAL ADVICE DISCLAIMER.**

**THE SERVICES ARE NOT INTENDED TO BE, AND MUST NOT BE USED BY CUSTOMER OR ANY THIRD PARTY USERS AS LEGAL ADVICE OR A SUBSTITUTE FOR OBTAINING INDEPENDENT (OR INTERNAL TO CUSTOMER'S ORGANISATION) LEGAL ADVICE WHICH IS RELEVANT AND APPROPRIATE TO CUSTOMER'S OR THIRD PARTY USER'S SPECIFIC REQUIREMENTS. NO LEGAL, ADVISORY OR REGULATORY RELIANCE BY THE CUSTOMER SHOULD BE PLACED UPON THE OUTPUTS OR ANY FUNCTIONALITY OF THE PRODUCT OR SERVICES, NOR ON LUMINANCE. NO LAWYER-CLIENT RELATIONSHIP OR ADVISORY RELATIONSHIP WILL BE CREATED BETWEEN THE PARTIES AS A RESULT OF THE USE OF THE PRODUCT OR SERVICES OR ANY REPORTS AND OUTPUTS. CUSTOMER AND THIRD PARTY USER ACKNOWLEDGE AND AGREE THAT IN NO CIRCUMSTANCES WILL LUMINANCE (OR ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS) BE PROVIDING LEGAL OR OTHER QUALIFIED PROFESSIONAL ADVICE. CUSTOMER AND THIRD PARTY USER SHOULD CONSULT ITS OWN LAWYERS OR OTHER PROFESSIONALS FOR LEGAL OR OTHER ADVICE, WHERE APPROPRIATE. UNLESS EXPRESSLY AGREED, SUPPORT DOES NOT INCLUDE MONITORING, INTERPRETATION AND/OR CORRECTIVE ACTION WITH RESPECT TO ANY RESULTS OR OUTPUTS GENERATED BY THE PRODUCT.  IN THE EVENT THAT CUSTOMER GRANTS A THIRD PARTY USER ACCESS TO, OR USAGE OF, THE PRODUCT, CUSTOMER SHALL BE SOLELY RESPONSIBLE FOR INFORMING THE THIRD PARTY USER OF THE TERMS ALL APPLICABLE TERMS UNDER THIS AGREEMENT. CUSTOMER AND THIRD PARTY USER ASSUME SOLE RESPONSIBILITY FOR RESULTS OBTAINED FROM THE USE OF THE PRODUCT OR SUPPORT, AND FOR CONCLUSIONS DRAWN FROM SUCH USE, AND LUMINANCE DISCLAIMS ALL LIABILITY FOR ANY LOSS OR DAMAGE CAUSED BY ERRORS OR OMISSIONS IN ANY OUTPUTS.**

**7    CONFIDENTIALITY**

7.1 In this Clause 7, "**Confidential Information**" means any information disclosed by Luminance or the Customer (as the case may be, the "**Disclosing Party**") to the other (the "**Receiving Party**") that is marked confidential, that the Receiving Party knows or reasonably ought to know is confidential, or which is of its nature or the circumstances ought to be understood to be confidential, including (a) any Customer programs or data which come into the possession or control of Luminance, or which are accessible to Luminance, in connection with this Agreement; and (b) Intellectual Property or know-how of a Party, and any other information clearly designated by a Party as being confidential to it.

7.2 Each party will treat the other party's Confidential Information as confidential (and for the avoidance of doubt all Customer Data shall be deemed Confidential Information).  Confidential Information of one party may only be used by the other party for the purpose of fulfilling obligations or exercising rights under this Agreement, and shared with employees, agents or contractors with a need to know such information to support that purpose ("Representatives"), provided that such Representatives are (a) informed of the confidential nature of the Confidential information and (b) bound by written confidentiality obligations with the Recipient which are no less onerous than those in this Clause 7, in advance of any such disclosure.  Notwithstanding the foregoing, the Receiving Party shall remain liable for the acts or omissions of its Representatives.

7.3 Confidential information will be protected by the Receiving Party using all reasonable skill and care to prevent unauthorised use or disclosure for five (5) years from the date of receipt or (if longer) for such period as the information remains confidential. These obligations do not cover information that: (i) was known or becomes known to the Receiving Party on a non-confidential basis from a third party, provided that: (A) the Receiving Party has no knowledge that the third party is subject to a confidentiality agreement with the Disclosing Party in respect of the information and (B) such information is not of a type or character that a reasonable person would have regarded it as confidential; (ii) is independently developed by the Receiving Party without violating the disclosing Party's rights; (iii) is or becomes publicly known (other than through disclosure by or through the Receiving Party or one if its Representatives in breach of this Agreement); (iv) was lawfully in the possession of the Receiving Party before the information was disclosed by the Disclosing Party.

7.4 A party may disclose Confidential Information where disclosure is required by law or a governmental agency provided that, to the extent lawful so to do, the Receiving Party shall notify the Disclosing Party of the request giving it reasonable opportunity to respond, and cooperate with the Disclosing Party's reasonable, lawful efforts to resist, limit or delay disclosure at the Disclosing Party's expense, and provided that except for making such required disclosure, such information shall otherwise continue to be Confidential Information. On termination of the Agreement, each Party will promptly return or destroy all Confidential Information of the other Party.

7.5 Notwithstanding the foregoing, either Luminance or Customer may disclose such information of the other party in response to a subpoena, judicial, administrative or arbitral order, provided that the party responding to such an order has given prompt notice to and has cooperated with the other in seeking protection against such disclosure at the other party's expense.

7.6 It is understood and agreed that money damages would not be a sufficient remedy for any breach of this Clause 7 and that either party shall be entitled to specific performance and injunctive or other equitable relief as remedies for any such breach. Neither Luminance nor Customer will oppose the granting of such relief and each hereby agrees to waive any requirements for the security or posting of any bond in connection with any such remedy. Such remedies shall not be deemed exclusive for breach of this Clause.

Neither Party will make any public statement or issue any public communication regarding any incident described in this Clause 7, without the other Party's prior written consent (not to be unreasonably withheld or delayed), except as strictly required by law or regulation.

## 8   INTELLECTUAL PROPERTY

8.1 Luminance Intellectual Property. Except as expressly set out herein, this Agreement does not grant either Party any rights, implied or otherwise, to the other's Intellectual Property.

8.2 Customer Intellectual Property. Customer retains and/or shall own all right, title and interest in and to Customer Data and the content of any Output.

## 9   LIMITATION OF LIABILITY

9.1 The Customer acknowledges that it is in the nature of a trial that the Product is provided strictly as-is, and Luminance gives no warranty in relation to the Product, the Software, their functionality, or their suitability to the Customer's requirements. All warranties and other terms implied by law are, to the fullest permissible extent, hereby excluded.

9.2 Nothing in this Agreement will limit or exclude either party's liability for (i) breach of Clause 7; (ii) fraud; or (iii) any liability which cannot be limited or excluded by law. Otherwise, Luminance will have no liability for any loss of profits or revenue, any account of profits, any increased costs, any loss of anticipated savings, any loss of opportunity, any loss of goodwill or reputation, any loss or corruption of data, nor for any indirect or consequential loss. Luminance's maximum aggregate liability to the Customer arising out of, or in connection with, this Agreement will be limited to

£10,000.00.

**10   DATA PROTECTION**

The Parties acknowledge that either Party may process Personal Data in accordance with applicable Data Protection Laws and the Parties shall comply with the data processing requirements as set out in Appendix 1. For the purposes of this Agreement, the Customer is the Data Controller and Luminance is a Data Processor for purposes of all applicable Data Protection laws.

**11   GENERAL, GOVERNING LAW AND JURISDICTION**

11.1   Survival. The following provisions shall survive any termination of this Agreement: Clause 3 ("*Licence Grant and Restrictions*"); Clause 7 ("*Confidentiality*"); Clause 9 ("*Limitation of Liability*"); and this Clause 11 ("*General, Governing law and jurisdiction*").

11.2   Entire agreement. This Agreement and the documents referred to in it contain the whole agreement between the parties, and supersede all prior agreements, arrangements and understandings between the parties, relating to its subject matter. Each party acknowledges that, in entering into this Agreement, it does not rely on any statement, representation, assurance or warranty (whether it was made negligently or innocently) of any person (whether a party to this Agreement or not) (each, a "**Representation**") other than as expressly set out in the Agreement. Each party agrees that the only rights and remedies available to it arising out of or in connection with a Representation will be for breach of the Agreement.

11.3   Deletion of Customer Data. Other than as set out in this Agreement and absent written notice from Customer to Finance@luminance.com; copying Legal@luminance.com requesting expedited deletion of Customer Data, Luminance shall maintain Customer Data and full Customer access to the Product for the Retention Period, during which Customer may download and delete any Customer Data or Outputs from the Product. Following expiry of the Retention Period, Luminance shall delete or destroy all copies of Customer Data (including Outputs) without liability or additional notice. Customer Data (including Outputs) cannot be recovered once deleted or destroyed.

11.4   Governing Law. This Agreement and all non-contractual obligations arising out of or in connection with it will be governed by the laws of England and Wales and the courts of England and Wales shall have exclusive jurisdiction to determine any disputes, which may arise out of, under, or in connection with this Agreement. Customer and Luminance agree that the United Nations Convention on Contracts for the International Sale of Goods will not apply to this Agreement.

11.5   Description of entity. Should the entity described or stated as entering into this Agreement not be correctly stated or incorrectly identified, this Agreement shall be binding on the legal entity or legal entities of which each user is an employee.

**For avoidance of doubt, the Commencement Date will be upon the first acceptance by the user of the above Terms and Conditions, and ticking below, thereafter the trial evaluation will start immediately.**

[TICKBOX]

Yes, I agree to the above terms and conditions and confirm that by accepting them, I warrant that I have the legal power and authority, whether in my capacity as authorized signatory or as authorised by such signatory, to bind my organization or entity to such terms and conditions for purposes of this Trial only.

[TICKBOX]

I consent to Luminance processing my personal data, including name, title and email address, for the sole purpose of providing this Trial Evaluation Agreement

APPENDIX 1: DATA PROCESSING ADDENDUM

**Definitions.**

1. For the purposes of this Data Processing Addendum ("DPA"), the terms used herein shall have the meanings set forth in the Agreement. Any terms not specifically defined by this DPA or the Agreement shall have the meanings given by applicable Data Protection Laws.

**Nature, Purpose and Scope of Processing**

2. This DPA applies to the processing of Customer Personal Data under the Agreement.

3. The Parties agree that Customer is the Data Controller and Luminance is the Data Processor. The Parties each agree that they shall comply with the Data Protection Laws (as such laws apply to a Data Controller and Data Processor, respectively) in exercising their rights and performing their obligations under this Agreement.

4. The Data Controller instructs the Data Processor to take such steps in the processing of Personal Data as are reasonably necessary for the performance of the Data Processor's obligations under the Agreement and agrees that such instructions provided herein constitute its full and complete instructions as to the means by which Personal Data shall be processed.

5. The duration of the processing under this DPA shall equal the Term and Retention Period of the Agreement.

**Types and Categories of Personal Data**

6. The categories of Customer Personal Data may include but are not limited to the Data Controller's clients, employees, contractors, suppliers and professional advisors and any other categories of Personal Data that may be contained in the Customer Data uploaded to the Product.

7. The types of Customer Personal Data may include, but are not limited to names, phone numbers, addresses, and any other types of Personal Data that may be contained in the Customer Data uploaded to the Product.

**Data Processor Obligations**

8. The Data Processor shall not use Personal Data save for the purposes of providing the Product and support as instructed herein unless required to do so by applicable law, including the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA). The Data Processor shall, to the extent legally permissible, inform the Data Controller of that legal requirement before processing.

9. The Data Processor shall immediately inform the Data Controller if, in the Data Processor's opinion, an instruction from the Data Controller infringes the Data Protection Laws.

**Confidentiality and Security**

10. The Data Processor shall take reasonable steps to ensure the reliability of any persons authorised to process any Personal Data, and it shall ensure that all such persons have committed themselves to confidentiality.

11. Taking into account the nature, scope, context and purposes of processing, the Data Processor has implemented and will maintain for the Term the appropriate administrative, physical, technical and organisational measures to protect any Personal Data accessed or processed by it against unauthorised or unlawful processing or accidental loss, destruction, damage or disclosure, in compliance with applicable Data Protection Laws, including the CCPA.

**Subprocessing**

12. Save as expressed herein, the Data Processor shall not without, the prior written consent of the Controller, engage any subprocessors for the processing of Personal Data under this Agreement.

13. The Data Controller hereby gives its prior and general authorisation to the Data Processor to authorise the Data Processor's subprocessors (as set out in Appendix 2) to act for the Data Processor in the provision of the Product, provided that:

    a. The subprocessors are subject to comply with the obligations imposed on the Data Processor and applicable Data Protection Laws;

    b. The Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of the subprocessors; and

    c. The Data Processor shall be fully liable for any breach by the subprocessors of any of the data protection obligations hereunder.

**Cross-Border Transfers**

14. Save as expressed herein, if Personal Data originates in the UK, California, or the European Economic Area ("EEA"), the Data Processor will not transfer such Personal Data outside the EEA, the United States,or the UK without the prior written consent of Controller and without implementing the appropriate data transfer instrument and adequate safeguards of (as defined by the Information Commissioner's Office, the relevant EEA data protection authority, and the California Attorney General, from time to time) in accordance with the Data Protection Laws.

15. The Product will be hosted in an AWS Region of Luminance's discretion, unless otherwise agreed between Luminance and Customer in writing. Notwithstanding the foregoing, Controller acknowledges and consents to the processing of Personal Data outside of the EEA and/or the UK, solely and to the extent necessary for the Data Processors to provide the Product and support (as set out in Appendix 2)for which purposes the applicable data transfer instrument shall apply.

16. Luminance will rely on the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the Swiss-U.S. DPF ("Swiss-U.S. DPF") and the UK Extension to the EU-U.S. Data Privacy Framework as a legal framework for transfers of personal information from the EU to the United States, and from the UK to the United States, respectively.

17. Save as set out in clause 16 of the DPA, any transfer of Personal Data from the UK or the EEA to third countries which do not ensure an adequate level of data protection where processors are established shall be in accordance with the SCCs. The SCCs shall come into effect and be incorporated from the date of the first relevant transfer. Any processing of such Personal Data

shall be (i) under the SCCs; (ii) reflect the subject matter, purpose and scope of Personal Data processed under this DPA; and (iii) subject to the technical and organisational measures provided for by the Data Processor. Either Party may, at any time with not less than 30 days' notice, revise this Clause 17 by replacing it with any applicable form of SCC with the agreement of both Parties by way of amendment to the Product Order Form.

**Data Subject Requests and Assistance**

18. The Data Processor shall notify Customer within three (3) days if it receives: (a) A request from a Data Subject to have access to that person's Personal Data, including requests under the CCPA for the right to know, delete, correct, or limit the use of personal information; or (b) a complaint or request relating to the Customer's obligations under the Data Protection Laws, including the CCPA; or (c) any other communication relating directly or indirectly to the Processing of any Personal Data in connection with this Agreement.

19. Taking into account the nature of processing and the information available to the Data Processor, the Data Processor will provide reasonable support to the Data Controller in (i) complying with any legally mandated request for access to or correction of any Personal Data by a data subject under Chapter III GDPR and the CCPA; (ii) responding to requests or demands made to the Data Controller by any court or governmental authority responsible for enforcing privacy or data protection laws, including the CCPA; and (iii) its preparation of a Data Protection Impact Assessment.

**Personal Data Breach**

20. In the event that the Data Processor suffers or becomes aware of a Personal Data Breach it will inform the Data Controller within twenty-four (24) hours of becoming aware of the same and take reasonable steps to mitigate the effects and to minimise any damages resulting from such breach.

21. To the extent reasonably possible, the notification to the Data Controller shall include: (i) a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained; (iii) a description of the likely consequences of the incident; and (iv) a description of the measures taken or proposed to be taken by the Data Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.

**Audit**

22. On the Data Controller's written request, and subject to appropriate confidentiality obligations, the Data Processor will make available to the Data Controller: (i) a copy of its current ISO 27001 certification; and (ii) Information reasonably requested by the Data Controller with regards to the Data Processor's processing of Personal Data under this DPA. The Data Controller agrees to exercise any right it may have to conduct an audit or inspection under GDPR (or the EU Model Clauses if they apply) in the first instance by requesting the foregoing information.

23. In the event that the foregoing does not confirm the Data Processor's compliance with the obligations laid down herein or an onsite inspection is required by a supervisory authority, then the Data Processor will, subject to appropriate security and confidentiality arrangements, allow

for and contribute to such inspection, and the Data Controller shall bear any costs associated with such audit.

**Data Return and Destruction.**

24. On termination of the Agreement  and in accordance with Clause 11.3, the Data Processor shall delete or return to Controller's (in accordance with Controller's written instructions) all Personal Data in its and/or its subprocessors' possession or control.

**Data Privacy Framework**

25. On 10 July 2023, the European Commission's adequacy decision for the EU-U.S. DPF entered into force, followed by the Swiss-U.S. Data Privacy Framework on 17 July 2023 and the UK extension to the EU-U.S. DPF on 12 October 2023.

26. Luminance complies with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF as set forth by the U.S. Department of Commerce.  Luminance has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles with regard to the processing of personal data received from the EU and the UK in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

27. Luminance certified to the United States Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF.

28. Further details on the Data Privacy Framework Program may be seen here https://www.dataprivacyframework.gov/. Luminance's certification may be located here.

**Order of Precedence.**

29. In a conflict between this Appendix (Data Protection) and Clause 7 of the Agreement (Confidentiality), the provisions that offers greater protection for Personal Data, including those under the CCPA will apply.

APPENDIX 2: SUBPROCESSORS

Luminance, in its role as a Processor, currently uses the following subprocessors in the processing of personal data for the purposes of providing the Product:

**Product support**

| Subprocessor | Service Provided | Location | Data Processed | Further Details |
|---|---|---|---|---|
| Luminance, Inc | 24/7 support services | United States | Limited data as needed to provide customer support to Controller. | n/a |
| Luminance Technologies Pte. Ltd | 24/7 support services | Singapore | Limited data as needed to provide customer support to Controller. | n/a |

**Hosting of Customer Data**

| Subprocessor | Service Provided | Location | Data Processed | Further Details |
|---|---|---|---|---|
| AWS | Cloud-hosting | The location is dependent on the geographic hosting location, the list of AWS entities can be found here: https://aws.amazon.com/compliance/sub-processors/ | Data which is uploaded to the Product by Controller. | n/a |

**Functionalities using Additional Generative Models**

| Subprocessor | Service Provided | Location | Data Processed | Further Details |
|---|---|---|---|---|
| AWS (AWS BedRock) | Provision of Additional Generative Models within secured AWS servers.<br><br>Luminance runs dedicated, segregated AWS servers for secure hosting of Additional Generative Models for the provision of additional functionalities (including but not limited to Ask Lumi). | The location is dependent on the geographic hosting location, the list of AWS entities can be found here:<br><br>https://aws.amazon.com/compliance/sub-processors/ | Limited data as needed to provide generative natural language prompts and replies (including, but not limited to Ask Lumi question and answers) to the Controller of the data.<br><br>No data passed to OpenAI or directly to any other provider of Additional Generative Models. | Additional Generative Model approval ("Generative Model Approval") is only required to utilise functionality hosted segregated secure AWS servers for external LLMs or third party integrations for specific functionalities within the Product (including, but not limited to Ask Lumi).<br><br>Controller may 'opt out' of the additional functionalities which utilise Additional Generative Models by raising a support ticket to disable.<br><br>The Additional Generative Models hosted on AWS may be distinct and separate to the Additional Generative Models hosted on Microsoft Azure. |

| Subprocessor | Service Provided | Location | Data Processed | Further Details |
|---|---|---|---|---|
| Microsoft Azure | Provision of Additional Generative Models within secured Microsoft Azure servers.<br><br>Luminance runs dedicated, segregated Microsoft Azure servers for secure hosting of Additional Generative Models for the provision of additional functionalities (including but | 1. If Controller's AWS hosting location is based in the EU or UK:<br><br>Default will be selected to reflect the relevant AWS hosting location and may be switched between UK and EU at Processor's discretion, for optimal service delivery.<br><br>2. If AWS hosting location is based outside of the EU or UK, and on either (i) express written request from the Controller; or (ii) otherwise at the discretion of Processor, for | Limited data as needed to provide generative natural language prompts and replies (including, but not limited to Ask Lumi question and answers) to the Controller of the data.<br><br>No data passed to OpenAI or directly to any other provider of Additional Generative Models. | Additional Generative Model approval ("Generative Model Approval") is only required to utilise functionality hosted segregated secure Azure servers for external LLMs or third party integrations for specific functionalities within the Product (including, but not limited to Ask Lumi).<br><br>Controller may 'opt out' of the additional functionalities which utilise Additional Generative Models by raising a support ticket to disable.<br><br>The Additional Generative Models hosted on Microsoft Azure may be distinct and separate to the Additional Generative Models hosted on AWS. |

| | | | | |
|---|---|---|---|---|
| | not limited to Ask Lumi). | optimal service delivery:<br><br>United States or another international location (unless otherwise expressly excluded in writing by the Controller) may be used as choice of server location. | | |

| Subprocessor | Service Provided | Location | Data Processed | Further Details |
|---|---|---|---|---|
| OpenAI, L.L.C ("OpenAI") | Provision of Additional Generative Models by OpenAI.<br><br>Luminance may utilise OpenAI directly for the use of Additional Generative Models for the provision of additional functionalities (included by not limited to Ask Lumi). | United States. | Limited data as needed to provide generative natural language prompts and replies (including, but not limited to Ask Lumi question and answers) to the Controller of the data.<br><br>Data is deconstructed and redacted by Luminance prior to any transfer of transformed data or metadata. | Generative Model Approval is only required to utilise functionality hosted segregated secure Azure servers for external LLMs or third party integrations for specific functionalities within the Product (including, but not limited to Ask Lumi).<br><br>Controller may 'opt out' of the additional functionalities which utilise Additional Generative Models by raising a support ticket to disable.<br><br>The Controller recognises and agrees that by opting in to using functionalities (including, but not limited to Ask Lumi) which utilise Additional Generative Models, in certain circumstances redaction may not be possible (for example with respect to the actual words/data entered as a query or requested redraft), and that the Processor shall not be responsible or liable for any confidentiality or intellectual property issues which may arise as a direct result (superseding any terms set out in the Agreement). |

<u>APPENDIX 3: TERMS SPECIFICALLY APPLICABLE TO AI SYSTEMS</u>

**<u>Explanatory Summary:</u>**

1. This appendix contains tailored standard contractual clauses which have been drafted (as amended) for organisations procuring technology which includes an AI System developed by Luminance. These standard clauses are based on standard EU model contractual AI clauses which have been drafted by legal experts and have been peer-reviewed. More information available here https://living-in.eu/group/16/commitments/standard-eu-model-contractual-ai-clauses.

2. The standard contractual clauses presented are based on the requirements and obligations for high-risk AI Systems included in Title III of the proposal for a Regulation on artificial intelligence* ("AI Act").

3. **Luminance has carried out a FRIA and has determined that the Luminance AI Systems are classified as non-high risk**. For non-high risk AI, the application of these requirements is not mandatory under the AI Act, but is recommended to improve trustworthiness of AI applications procured by organisations. This version of the standard contractual clauses targets, in particular, non-high risk AI systems, such as Luminance's AI Systems.

4. The standard contractual clauses contain provisions specific to AI Systems and on matters covered by the proposed AI Act and are distinct to the standard contract clauses pertaining to data transfers and Data Protection Laws. For obligations relating to Data Protection Laws, please see Appendix 1 and Appendix 2 of the Agreement. Any conditions concerning intellectual property, acceptance, payment, Term, applicable law, confidentiality, or liability are set out in the Agreement.

*\* Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain union legislative acts, COM(2021)206 final.*

Article 1                 Definitions

1.1.    Capitalised terms used in the Clauses shall have the meanings ascribed to them in the Agreement, unless otherwise defined in the Clauses below.

a)    Agreement: the entire agreement of which the Clauses, as a schedule, are an integral part;
b)    AI System: the AI system(s) as referred to in **Annex A**, including any new versions thereof;
c)    Clauses: these standard contractual clauses for the procurement of artificial intelligence by Customer;
d)    Data Sets: all data sets used in the development of the AI System;
e)    Intended Purpose: the use for which an AI System is intended by the Customer, considering the specific context and conditions of use, as well as the technical Documentation;
f)    Reasonably Foreseeable Misuse: the use of the AI System in a way that is not in accordance with its Intended Purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems; and
g)    Substantial Modification: a change to the AI System during the Term which affects the compliance of the AI System with the material requirements set out in these Clauses.

## Section B – Essential requirements in relation to the AI-system

Article 2                 Risk management system

Luminance takes reasonable steps so that a risk management system shall be established and implemented in relation to the AI System.

2.1.    The risk management system will comprise the following steps:
a.    identification, estimation and evaluation of the known and reasonably foreseeable risks to the fundamental rights of the European Union that are likely to arise in the light of the Intended Purpose of the AI System and Reasonably Foreseeable Misuse;
b.    evaluation of other possibly arising risks;
c.    adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to points a and b of this paragraph in accordance with the provisions of the following paragraphs.

2.2.    Luminance will review the relevant residual risks associated with each material hazard (as well as the overall residual risk) of the AI system. Such risks may be judged to be acceptable by Luminance, provided that the AI System is used in accordance with the Intended Purpose or under conditions of Reasonably Foreseeable Misuse.

2.3.    In identifying the most appropriate risk management measures referred to in paragraph 2.2, point (c), Luminance will include:
a.    elimination or reduction of identified risks as far as technically feasible through adequate design and development of the AI System; and
b.    where appropriate, implementation of adequate mitigation and control measures in relation to risks that cannot be eliminated.

2.4.    Luminance takes reasonable steps so that the AI System is tested appropriately in order to verify whether the AI System complies with the Clauses and whether the risk management measures referred to in paragraph 2.2, point (c) are effective in light of the Intended Purpose and Reasonably Foreseeable Misuse.

2.5.    Luminance will document risks identified, measures taken, and tests performed in the context of compliance with this article.

2.6.    The risk management system shall consist of a continuous and iterative process run throughout the entire duration of the Agreement. After the Commencement Date, Luminance will regularly review and update the risk management process, to ensure its continuing effectiveness.

2.7.    If reasonably required for the proper execution of the risk management system by Luminance, the Customer will provide Luminance, on request, information insofar as this is not of a confidential nature.

Article 3          Data Sets

3.1.    Luminance takes reasonable steps so that the Data Sets used in the development of the AI System, including training, validation and testing, are subject to data governance appropriate for the Intended Purpose of the AI System. Those measures will include
   a.    transparency as regards the original purpose of data collection;
   b.    relevant design choices;
   c.    data collection processes;
   d.    data preparation for processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;
   e.    the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;
   f.    examination in view of possible biases that are likely to affect health and safety of natural persons or lead to discrimination prohibited by the laws of the European Union;
   g.    appropriate measures to detect, prevent and mitigate possible biases;
   h.    the identification of relevant data gaps or shortcomings that prevent compliance with these Clauses, and how those gaps and shortcomings can be addressed.

3.2.    Luminance takes reasonable steps so that the Data Sets used in the development of the AI System are relevant, representative, and free of errors (once categorised and reviewed, as far as reasonably possible) and be as complete as possible in view of the Intended Purpose. These characteristics of the Data Sets may be met at the level of individual data sets or a combination thereof.

3.3.    The obligations under this article apply not only to the development of the AI System, prior to the Commencement Date, but also to any use of Data Sets by Luminance that may affect the functioning of the AI System at any other time during the term of the Agreement.

Article 4          Technical documentation and instructions for use

4.1.    The instructions for use shall include clear and user-friendly information.
4.2.    The technical Documentation and instructions for use will be drawn up in English.
4.3.    Subject to the terms of the Agreement, the Customer may make copies of the technical Documentation and instructions for use to the extent necessary for internal use within the organisation of the Customer.

Article 5          Record-keeping

5.1.    Luminance takes reasonable steps so that the AI System is designed and developed with proportionate and technically appropriate capabilities enabling the automatic recording of events ('logs') while the AI System is operating. Those logging capabilities will reasonably conform to industry standard.
5.2.    The logging capabilities shall ensure a level of traceability of the AI System's functioning throughout its lifecycle that is appropriate to the Intended Purpose of the system and Reasonably Foreseeable Misuse. In particular, they shall enable the recording of events relevant for the identification of situations that may:
   a.    result in the AI System presenting a risk to the health or safety or to the protection of fundamental rights of persons; or
   b.    lead to a Substantial Modification.
5.3.    Luminance shall keep the logs automatically generated by the AI System, to the extent such logs are under its control, for the duration of the Agreement.

Article 6          Transparency of the AI System

6.1.   Luminance takes reasonable steps so that the AI System is designed and developed in such a way that the operation of the AI System is sufficiently transparent to enable the Customer to reasonably understand the system's functioning.

6.2.   To maximise appropriate transparency appropriate technical and organisational measures will be implemented by Luminance. These measures should result in the Customer being able to understand and use the AI System appropriately.

Article 7          Human oversight

7.1.   Luminance takes reasonable steps so that the AI System is designed and developed in such a way, including with appropriate human-machine interface tools.

7.2.   Luminance takes reasonable steps so that appropriate measures shall be embedded in the AI System and taken to facilitate human oversight. Luminance may provide Customer with support (as further set out in the Order Form), which may include (a) information on how to sufficiently understand the relevant capacities and limitations of the AI System; (b) being able to duly monitor its operation information; and (c) managing the characteristics of the system and the tools and methods of usage available.

Article 8          Robustness and cybersecurity

8.1.   Luminance takes reasonable steps so that the AI System is designed and developed following the principle of security by design and by default. In the light of the Intended Purpose, it should achieve an appropriate and reasonable level of robustness, safety and cybersecurity, and perform consistently in those respects throughout the lifecycle of the AI System.

8.2.   In order to facilitate an appropriate and reasonable level of robustness, safety and cybersecurity, Luminance shall at least implement the technical and organisational measures described in **Annex B** before the Commencement Date.

Article 9          Compliance

9.1.   Luminance will take reasonable steps so that from the Commencement Date until the end of the term of the Agreement the AI System complies with these Clauses.

9.2.   If during the term of the agreement Luminance considers or has reason to consider that the AI System is not in conformity with these Clauses, whether in response to a comment by the Customer or not, it will take the corrective actions to bring the system into conformity.

Article 10         Obligation to explain the functioning of the AI System on an individual level

10.1.   In addition to the obligations described in article 6, during the term of the Agreement Luminance may provide reasonable assistance to the Customer, on request, to explain (if reasonably possible and without compromising any trade secrets or proprietary processes) how the AI System arrived at a particular decision or outcome. This assistance may include an indication of the key factors that led the AI System to arrive at a particular result and the changes to the input which may be made in order for it to arrive at a different outcome.

**Annex A – The AI System and the Intended Purpose**

Description of the AI System

Within the scope of these clauses are the following systems or components of systems:

*Luminance's proprietary Large Language Model, which leverages advanced Transformers-based Natural Language Processing (NLP) as well as other Machine Learning (ML) techniques in order to provide end users with assistance and acceleration in their legal processes. Functionality may include supervised and semi-supervised ML techniques, and manual workflows or agentic workflows.*

Intended Purpose

*Luminance delivers a service to the Customer, which includes the AI System. The Intended Purpose aims to facilitate and enhance legal document analysis, improve legal research, contract analytics and legal workflows of numerous varieties as the product capability expand.*

**Annex B – Measures to ensure an appropriate level of robustness, safety and cybersecurity (General Technical and Organizational Security Measures)**

1. The Product is a web application hosted in the cloud using AWS and accessed through the Chrome browser. The cloud application environment is managed by Luminance on behalf of the Customer. Users can upload documents into the application either locally from their computer or through integration with a third-party document source (such as a document management system or virtual data room). Customer carries out their document review and usage within the Product, subject to pursuant to the terms of the Agreement.

2. Customers can choose which AWS data centre (subject to availability) to host Customer Data in. Once selected, data residency will be fixed to this data centre and a backup data centre within the same region according to the S3 durability method.

3. All Customer Data is encrypted at rest and in transit. Full backups are taken every 24 hours, and OS security updates are deployed nightly. Strong access controls are in place at all technical levels, with controls by the customer. The application supports MFA, and single sign-on can be configured upon request. Luminance is ISO 27001 certified (certificate can be provided upon request) and AWS maintain a range of industry certifications including ISO 27001 and SOC 2/3.

4. Measures specific to processing of Personal Data include:

   a) Data encrypted at rest using open encryption standards, with minimum standards enforced through cryptographic policies that are externally reviewed.
   b) Data encrypted in transit using open encryption standards, with minimum standards enforced through cryptographic policies that are externally reviewed.
   c) Data backed up every 24 hours to a secondary AWS datacenter within the same region, ensuring redundancy without requiring data transfer across borders.
   d) Maintenance of a Business Continuity Plan (BCP), including individual Disaster Recovery plans that encompass relevant internal and customer managed environments.
      i. BCP includes a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of 24 hours for a complete failure in the primary data centre
   e) A formal change control policy and change management process for managing changes to production and non-production environments
   f) A formal Access Control policy governing access to all systems on the basis of:
      i. Least-privilege
      ii. Need-to-know
      iii. Need-to-use
   g) A dedicated DPO who oversees security of both our software and client data
   h) Single-tenancy architecture for customer environments, including:
      i. Dedicated virtual servers and storage for customer application services, segregating these from other customers or Luminance development environments;
      ii. Dedicated virtual servers and storage for customer data base services, segregating these from other customers or Luminance development environments.
   i) Data retention
      i. Control by the customer, with the ability to delete the data at any time. After which data will be removed from any data stores within 30 days and back up data stores within a further 30 days, in line with industry standards. Removal can be expedited on request.

   j) Measures for internal IT and IT security governance and management include:
      i. Formal and ongoing governance program encompassing all aspects of security and risk.
      ii. Quarterly Information Security Management Review Meetings attended by senior management in Technology, Legal, Operations and the wider business.
      iii. Dedicated security advisory board composed of global experts in cybersecurity and risk management.

   k) Maintenance of an ISO27001 certification which covers *the Information Security Management System for the development, sales, support, and operation of artificial intelligence software and technology platforms for the*

*legal industry. This includes the Cambridge technical headquarters, remote workers globally, and cloud data hosting and processing.*

l)   Conducting of Data Privacy Impact Assessments, Fundamental Rights Impact Assessments and transfer risk assessments.