

LUMINANCE DATA PROCESSING ADDENDUM

Version 3.0 | Last updated 01 October 2026

This Data Processing Addendum (this “DPA”) supplements, and is incorporated by reference into, the agreement between Luminance Technologies Ltd (“Luminance”) and the Customer into which it is incorporated, being either the Master Agreement or the Proof of Value Terms (in each case, the “applicable Agreement”). This DPA applies where Luminance processes Customer Personal Data in connection with the Product. Luminance and Customer may be referred to as the “Parties” and each a “Party”.

1. DEFINITIONS

- 1.1 For the purposes of this DPA, capitalised terms have the meanings given in the applicable Agreement and the Luminance Glossary. Any terms not specifically defined in this DPA, the applicable Agreement or the Glossary shall have the meanings given by applicable Data Protection Laws. The terms “Data Controller”, “Data Processor”, “Data Subject”, “Personal Data”, “Personal Data Breach” and “processing” have the meanings given in the UK GDPR or the EU GDPR, as applicable.

2. NATURE, PURPOSE AND SCOPE OF PROCESSING

- 2.1 This DPA applies to the processing of Customer Personal Data under the applicable Agreement.
- 2.2 The Parties agree that Customer is the Data Controller and Luminance is the Data Processor. Each Party shall comply with the Data Protection Laws (as such laws apply to a Data Controller and Data Processor, respectively) in exercising its rights and performing its obligations under the applicable Agreement.
- 2.3 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 applicable 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.
- 2.4 The duration of the processing under this DPA shall equal the Term (or, under the Proof of Value Terms, the PoV Period) and the Retention Period of the applicable Agreement.

3. TYPES AND CATEGORIES OF PERSONAL DATA

- 3.1 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.
- 3.2 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.

4. DATA PROCESSOR OBLIGATIONS

- 4.1 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.
- 4.2 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.

5. CONFIDENTIALITY AND SECURITY

- 5.1 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.
- 5.2 Taking into account the nature, scope, context and purposes of processing, the Data Processor has implemented and will maintain, for the term of the applicable Agreement, 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. The technical and organisational measures applied by the Data Processor are set out in the Technical and Organisational Measures document available at the Legal Hub.

6. SUBPROCESSING

- 6.1 The Data Controller hereby provides its prior and general authorisation for the Data Processor to engage subprocessors for the processing of Personal Data under the applicable Agreement, subject to this Clause 6. The subprocessors currently engaged by the Data Processor are listed on the Subprocessor Page (available at the Legal Hub), which is incorporated into this DPA by reference.
- 6.2 The Data Processor may engage subprocessors in connection with the provision of the Product, provided that:
- (a) the subprocessors are subject to obligations (i) substantially similar to those imposed on the Data Processor under the applicable Agreement, and (ii) applicable Data Protection Laws;
 - (b) the Data Processor shall provide the Data Controller with at least thirty (30) days' prior written notice of any intended addition or replacement of a subprocessor; and
 - (c) during the fifteen (15) days following receipt of such notice, the Data Controller may object on reasonable grounds relating to data protection and/or technical and organisational measures.
- 6.3 The Data Processor shall remain responsible for the performance of its subprocessors' data protection obligations in accordance with Article 28(4) GDPR, subject to the liability limitations set out in the applicable Agreement.

7. CROSS-BORDER TRANSFERS

- 7.1 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 the Data Controller and without implementing the appropriate data transfer instrument and adequate safeguards (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.
- 7.2 Customer Data will be hosted in the AWS hosting location specified in the Product Order Form. Notwithstanding the foregoing, the Data 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 Processor to provide the Product and Support (as set out on the Subprocessor Page), for which purposes the applicable data transfer instrument shall apply.
- 7.3 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.
- 7.4 Save as set out in Clause 7.3, 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 thirty (30) days' notice, revise this Clause 7 by replacing it with any applicable form of SCC with the agreement of both Parties by way of amendment to the applicable Agreement.

8. DATA SUBJECT REQUESTS AND ASSISTANCE

- 8.1 The Data Processor shall notify the Data Controller 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; (b) a complaint or request relating to the Data Controller'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 the applicable Agreement.

- 8.2 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.

9. PERSONAL DATA BREACH

- 9.1 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.
- 9.2 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.

10. AUDIT

- 10.1 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 regard 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 SCCs if they apply) in the first instance by requesting the foregoing information.
- 10.2 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.

11. DATA RETURN AND DESTRUCTION

- 11.1 On termination of the applicable Agreement, and in accordance with its provisions on the effect of termination, the Data Processor shall delete or return to the Data Controller (in accordance with the Data Controller's written instructions) all Personal Data in its and/or its subprocessors' possession or control.

12. DATA PRIVACY FRAMEWORK

- 12.1 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.
- 12.2 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.
- 12.3 Luminance has 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.
- 12.4 Further details on the Data Privacy Framework Program may be seen at <https://www.dataprivacyframework.gov/>.

13. GOVERNING LAW AND DISPUTES

- 13.1 This DPA is governed by, construed in accordance with, and subject to the dispute-resolution provisions of, the applicable Agreement.

14. ORDER OF PRECEDENCE

- 14.1 In the event of a conflict between this DPA and the applicable Agreement, this DPA shall prevail, but only to the extent that it provides greater protection for Personal Data (including those protections under the CCPA), consistent with the order of precedence set out in the applicable Agreement.

[End of Data Processing Addendum]