

LUMINANCE TECHNICAL AND ORGANISATIONAL MEASURES

Version 3.0 | Last updated 01 October 2026

These Technical and Organisational Measures (the “TOMs”) describe the administrative, physical, technical and organisational measures Luminance applies to protect the Product and the data processed within it. They are referenced by, and incorporated into, the Master Agreement (Clause 16), the Data Processing Addendum and the AI Systems Terms, and are maintained and updated by Luminance from time to time in accordance with the Master Agreement. Capitalised terms have the meanings given in the Luminance Glossary.

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 or through integration with a third-party document source (such as a document management system or virtual data room). The Customer carries out its document review and usage within the Product, subject to the terms of the applicable Agreement.

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

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. The application supports MFA, and single sign-on can be configured on request. Luminance is ISO/IEC 27001 certified (certificate available on request); AWS maintains a range of industry certifications including ISO/IEC 27001 and SOC 2/3.

Measures specific to the processing of Personal Data include:

- (a) data encrypted at rest and in transit using open encryption standards, with minimum standards enforced through externally reviewed cryptographic policies;
- (b) data backed up every 24 hours to a secondary AWS data centre within the same region, ensuring redundancy without requiring data transfer across borders;
- (c) maintenance of a Business Continuity Plan (BCP), including Disaster Recovery plans, with a Recovery Time Objective and Recovery Point Objective of 24 hours for a complete failure in the primary data centre;
- (d) a formal change control policy and change management process for production and non-production environments;
- (e) a formal Access Control policy governing access on the basis of least-privilege, need-to-know and need-to-use;
- (f) a dedicated DPO who oversees the security of Luminance’s software and client data; and
- (g) an isolated environment for each customer within the Luminance cloud infrastructure, with tenant-specific application workloads and data, segregated and restricted from that of other tenants through layered logical, technical, and access controls (a Customer Instance).

Data retention is controlled by the Customer, with the ability to delete data at any time, after which data will be removed from data stores within 30 days and from backup data stores within a further 30 days, in line with industry standards. Removal can be expedited on request.

Measures for internal IT and IT-security governance include a formal and ongoing governance programme; quarterly Information Security Management Review Meetings attended by senior management in Technology, Legal, Operations and the wider business; a dedicated security advisory board; maintenance of an ISO/IEC 27001 certification covering the Information Security Management System for the development, sales, support and operation of the Product (including the Cambridge technical headquarters, remote workers globally, and cloud data hosting and processing); and the conducting of Data Protection Impact Assessments, Fundamental Rights Impact Assessments and transfer risk assessments.