Effective from 21 June 2024 – 16 June 2026

Vista Cloud Agreement

Data Processing Terms

Client's use of the Services is subject to the Vista Cloud Standard Terms located at https://cloud.vista.co/vista-cloud-agreement, in addition to these following Data Processing Terms ("**Terms**"). By executing the Vista Key Terms or otherwise accessing and using the Services, the Client agrees to be bound by these Terms. Any capitalised terms used by not otherwise defined below have the meaning given to those terms in the Vista Cloud Standard Terms.

1. Definitions

For the purposes of these Terms, the following capitalised words have the following meanings:

Australian Privacy Laws means the Australian Privacy Act 1988 (Cth), including the Australian Privacy Principles, and any other applicable Australian legislation protecting the Personal Data of natural persons, including the Do Not Call Register Act 2006 (Cth) and the Spam Act 2003 (Cth);

Canadian Privacy Laws means the Personal Information Protection and Electronic Documents Act (Canada) and any similar applicable laws of any Canadian province;

CCPA means the California Consumer Privacy Act of 2018, California Civil Code §§1798.100 et seq., including any implementing regulations and as amended or superseded from time to time;

Data Protection Laws means applicable legislation protecting the Personal Data of natural persons, including where applicable the GDPR, CCPA, FADP, LGPD, Canadian Privacy Laws and the Australian Privacy Laws (and any data protection laws substantially amending, replacing or superseding the same) together with binding guidance and codes of practice issued from time to time by relevant Supervisory Authorities and/or any local data protection law applicable in respect of Personal Data collected by the Client and Processed by Vista under the Agreement, including any data protection laws substantially amending, replacing or superseding the same;

EU Personal Data means Personal Data to which Data Protection Laws of the European Union, or of a Member State of the European Union or European Economic Area, was applicable prior to its Processing by Vista.

FADP means the Swiss Federal Act on Data Protection.

GDPR means, in each case to the extent applicable to the Processing activities: (i) Regulation (EU) 2016/679 ("**EU GDPR**"); and (ii) UK GDPR.

LGPD means the Brazilian General Data Protection Law No. 13,709/2018.

Protected Area means:

(a) in the case of EU Personal Data, the members states of the European Union and the European Economic Area and any country, territory, sector or international organisation in respect of which an adequacy decision under Art.45 EU GDPR is in force;
(b) in the case of UK Personal Data, the United Kingdom and any country, territory, sector or international organisation in respect of which an adequacy decision under United Kingdom adequacy regulations is in force; and
(c) in the case of Swiss Personal Data, Switzerland and any country, territory, sector or international organisation which is recognised as adequate under the laws of Switzerland.

Sensitive Data has the meaning given to that term (or any analogous term) in the applicable Data Protection Laws and may include personal, health, financial or legal data that could lead to identity theft, including but not limited to, passwords, credit card data, financial account numbers, personal identification numbers, social security numbers, driver's license number, state-issued identification card numbers or any equivalent data relating to a Data Subject.

Services means the services which are provided by Vista to the Client in accordance with this Agreement.

Standard Contractual Clauses or **SCCs** mean:

(a) in respect of EU Personal Data, the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the EU GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914;
(b) in respect of UK Personal Data, the International Data Transfer Addendum to the EU Standard Contractual Clauses, issued by the Information Commissioner in accordance with s.119A of the Data Protection Act 2018; and/or
(c) in respect of Swiss Personal Data, the EU Standard Contractual Clauses, provided that any references in the clauses to the GDPR shall refer to the FADP, the term 'member state' shall not be interpreted to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the clauses, and the Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner.

Swiss Personal Data means Personal Data to which data protection laws of Switzerland were applicable prior to its Processing by Vista.

UK GDPR means the EU GDPR as applicable as part of UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended).

UK Personal Data means Personal Data to which Data Protection Laws of the United Kingdom were applicable prior to its Processing by Vista.

Vista means the relevant Vista entity as set out in the Key Terms, and may include, where applicable, Movio Limited and/or Movio, Inc.

The terms "**Data Controller**", "**Data Processor**", "**Data Subject**", "**Personal Data**", "**Sensitive Personal Data**", "**Personal Data Breach**", "**Sub-Processor**", "**Supervisory Authority**" and "**Process, Processed or Processing**" have the same meaning given to them (and equivalent expressions) in the Data Protection Laws.

The terms "**Business**", "**Business Purposes**", "**Consumer**", "**Sell**", "**Service Provider**", and "**Third Party**" have the same meaning as described by such term (or the nearest equivalent term) in the Data Protection Laws.

2. Description of Personal Data Processing

2.1.

To the extent that Vista Processes Personal Data on behalf of the Client pursuant to the GDPR or the FADP (as applicable), the Client hereby appoints Vista as Data Processor in relation to the Processing of Personal Data. The parties agree to act in accordance with their respective obligations under this Schedule.

2.2.

Notwithstanding anything to the contrary herein:

(a) Pursuant to the CCPA, Vista may operate as a Business, Service Provider, or a Third Party with respect to Personal Data, when providing Services to Client.
(b) Client acknowledges and agrees that in order to provide the Services described in the Agreement, Vista must Process and use Client Personal Data and other Personal Data.

2.3.

Exhibit A sets out the subject matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of data subject as required by Article 28(3) of the GDPR or equivalent provisions of any Data Protection Laws.

3. Data Processing Terms

3.1.

In the respect of their obligations under the Agreement, both parties will observe their respective obligations under the Data Protection Laws which arise in connection with the provision and use of the Services.

3.2.

Where Vista Processes Client Personal Data under GDPR, Australian Privacy Laws, Canadian Privacy Laws, LGPD or FADP (as applicable), Vista will:

(a) Process the Personal Data solely on the Client's documented instructions (whether in the Agreement or otherwise) for the purposes of providing the Service or as otherwise required by applicable law or the Agreement. If Vista is required by applicable law to Process the Personal Data for any other purpose, Vista will inform Client of this requirement first, unless such law(s) prohibit this;
(b) notify the Client immediately if, in Vista's opinion, an instruction for the Processing of Personal Data given by the Client infringes applicable Data Protection Laws, it being acknowledged that Vista shall not be obliged to undertake additional work to determine if Client's instructions are compliant;
(c) take reasonable steps to ensure the reliability of any staff who may have access to such Personal Data, and their treatment of the Personal Data as confidential and otherwise in accordance with the Agreement;
(d) promptly refer to the Client any requests, notices or other communication applicable to the Client from Data Subjects or any Supervisory Authority or privacy commissioner, for the Client to resolve and, subject to clause 7.8 of the Standard Terms, provide reasonable assistance to the Client to assist the Client to respond to such communication;
(e) provide such information to the Client as the Client may reasonably require, and within the timescales reasonably specified by the Client, to allow the Client to comply with the rights of Data Subjects, including subject-access rights, or with notices served by the Supervisory Authority or privacy commissioner;

(f) within ninety (90) days of termination of the Agreement, (at the Client's option) return to the Client or delete all Personal Data Processed under the Agreement unless Vista is required to continue Processing the data according to applicable law;

(g) implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with Vista's Processing of the Personal Data, including the minimum security measures set out in Exhibit B to these Terms;

(h) promptly notify the Client upon becoming aware of any Personal Data Breach;

(i) on request and subject to clause 7.8 of the Standard Terms, provide the Client with reasonable assistance in carrying out its obligations under Articles 32 to 36 of the GDPR, and any equivalent provisions under other Data Protection Laws, where applicable;

(j) Process only the types of Personal Data, relating to the categories of Data Subjects, and in the manner required to deliver the Service, as further described in Exhibit A to these Terms;

(k) (1) only transfer EU, Swiss or UK Personal Data outside of the Protected Area in accordance with clauses 4.1 and 4.2**Error! Reference source not found.** or with the prior written consent of the Client; and (2) not transfer Personal Data subject to LGPD outside of Brazil other than to countries which have an adequate level of protection for Personal Data, or that the transfer is subject to the standard contractual clauses designed to facilitate transfers of Personal Data from Brazil to other countries in accordance with the LGPD, without the prior written consent of the Client. The Parties acknowledge that Vista may Process Personal Data subject to FADP, GDPR or LGPD from New Zealand and the United Kingdom, and that New Zealand and the United Kingdom are countries which are within the Protected Area;

(l) where the Australian Privacy Principles apply, before disclosing Personal Data to recipients outside Australia, take reasonable steps to ensure that such recipients do not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information; and

(m) on reasonable prior notice, provide the Client with information to demonstrate compliance with Vista's obligations under the Agreement and, at the Client's expense, and subject to at least ten (10) days' prior written notice, submit to audits conducted by the Client under the GDPR (where applicable) provided always that:

i) any such audit is carried out within Vista's normal business hours;

ii) no more than one such audit will be conducted per calendar year;

iii) Vista will not be required to provide or permit access to:

A. information relating to other Clients of Vista;

B. information relating to internal Vista pricing;

C. internal reports prepared by Vista internal audit function and non-public external reports; and

iv) any third party auditor engaged by the Client to carry out such audit enters into such confidentiality obligations with Vista (or its Sub-Processor as the case may be) as may be necessary to respect the confidentiality of Vista (or its Sub-Processor's) business interests and any third party data or information that the auditor becomes aware of during an audit.

3.3.

To the extent Vista Processes Personal Data for the Client as a Service Provider under CCPA, Vista shall not: (a) Sell such Personal Data; (b) retain, use, or disclose such Personal Data for any purpose other than performing the Services specified in this Agreement (or as otherwise permitted by the CCPA); or (c) retain, use, or disclose such Personal Data outside of the direct business relationship between the Client and Vista. Vista certifies that it and each of its employees, agents, and representatives who will receive such personal information understand, and shall comply with, the restrictions set forth in this clause **Error! Reference source not found.**. Client is responsible for determining whether its sharing of Personal Data under the Agreement is a Sale or otherwise impacts Client's legal obligations. If Client deems the disclosure and usage of Personal Data as permitted under the Agreement constitutes a Sale or otherwise modifies Client's notice and choice obligations to individuals under Data Protection Law, then Client agrees to provide such notice and choice as required under Data Protection Law.

3.4.

To the extent that the disclosure of Personal Data as contemplated by the Agreement is deemed to be a Sale, the disclosing Party shall inform the other Party of any "Do Not Sell" or opt-out request received from a Consumer requiring that the Party in receipt of the request refrain from selling that Consumer's Personal Data. Upon notice of such a request, each Party shall promptly cease any sale of that Consumer's Personal Data.

3.5.

Vista will be responsible for costs and expenses incurred by Vista in complying with its obligations as a Data Processor or Service Provider under these Terms unless otherwise agreed by the Parties. The Client will be responsible for costs and expenses incurred by the Client in complying with its obligations as a Data Controller or Business under these Terms unless otherwise agreed by the Parties. Unless stated otherwise in these Terms, Vista reserves its right to charge the Client additional reasonable fees for any assistance provided by Vista to the Client to assist the Client to comply with its obligations as a Data Controller under these Terms which go beyond any reasonable level of support/assistance, such fees to be pre-agreed by the Parties in writing.

3.6.

The Client will not provide Sensitive Data to Vista via the Services or otherwise. Where Vista becomes aware that it has received Sensitive Data, Vista will promptly notify the Client in writing and delete from its systems all Sensitive Data (unless Vista is required to continue Processing the Sensitive Data according to applicable law). Vista will have no liability to the Client or any third party in respect of any Sensitive Data provided to Vista.

4. **Transfers of EU, Swiss and UK Personal Data outside of the Protected Area**

4.1.

Vista shall not, and shall ensure that none of its Affiliates or Sub-Processors, transfer, access or use EU, or UK Personal Data outside of the Protected Area without Client's prior authorisation. Client agrees to authorise the transfers to Sub-Processors as set out on the Vista Cloud Sub-Processors page available at https://www.vista.co/list-of-sub-processors (as such list may evolve pursuant to the terms of the Agreement) and Vista confirms that it has in place a mechanism for lawful transfer and where necessary agrees to procure that its Affiliates or Sub-Processor's (as applicable) comply with the obligations set out in the Standard Contractual Clauses, with Vista as the 'data exporter' and the relevant Vista Affiliate or Sub-Processor (as applicable) as the 'data importer'. Where Client provides Personal Data described in Exhibit A to one of the Vista Affiliate Sub-Processors authorised under these Data Processing Terms for the purposes of enabling Vista to fulfil its obligations under the Agreement, then Client and Vista agree that such transfer shall be deemed to be a transfer from Client via Vista to such Vista Affiliate and that Vista shall be the 'data exporter' and the Vista Affiliate shall be the 'data importer' in relation to such transfers.

4.2.

For the purpose of clause **Error! Reference source not found.**(k) above, in the event that a relevant European Commission decision or other valid adequacy method under applicable Data Protection Laws on which the parties have relied as the basis for any data transfer is held to be invalid, or that any Supervisory Authority requires transfers of Personal Data made pursuant to such decision to be suspended, then the parties agree to discuss in good faith and facilitate use of an alternative transfer mechanism.

5. Sub-Processing

The Client authorises Vista to appoint third party Sub-Processors to assist in the management and provision of the Service provided Vista has entered into an agreement with the Sub-Processor which imposes obligations on the Sub- Processor no less onerous than as are imposed on Vista under these Terms. Vista's use of Sub-Processors will not relieve it of any liability, and Vista will remain liable to the Client for the performance of the Sub-Processors' obligations. The list of current Sub-Processors used by Vista is set out on the Vista Cloud Sub-Processors page available at https://www.vista.co/list-of-sub-processors and Vista will notify the Client of any additional Sub-Processor 10 days in advance. If the Client reasonably objects to a new Sub-Processor, the Client may inform Vista in writing of the reasons for the Client's objections. If the Client objects to such additional Sub- Processor(s) within such notice period, the Client should stop using the Service and providing data to Vista and Vista may terminate the Agreement by providing written notice to Client with immediate effect and the Parties obligations on termination will apply in accordance with clause 9.5 of the Standard Terms. The Client hereby specifically consents to Vista's appointment of its Affiliates as Sub-Processors for the purposes of assisting Vista to provide the Service under the Agreement.

6. General

6.1. The provisions of these Terms are supplemental to the provisions of the Agreement and shall not reduce either Party's obligations under the Agreement in relation to the protection of Personal Data. In the event of inconsistencies between the provisions of these Terms and the provisions of the Agreement the provisions of these Terms shall prevail.

6.2. The Parties shall cooperate in good faith to enter into additional or modified contract terms to address any modifications, amendments, or updates to Data Protection Laws, including applicable regulatory or self-regulatory guidance.

Exhibit A – Personal Data and Sub-Processors

1. Overview

This Exhibit A includes certain details of the Processing of the Personal Data as may be required by applicable Data Protection Laws.

2. Subject matter and duration of the Processing of the Personal Data

The subject matter and duration of the Processing of the Personal Data is the provision of the Services pursuant to the Agreement.

3. The nature and purpose of the Processing of the Personal Data

Vista may access, collect and Process the Client's Personal Data where Vista provides the Services to the Client pursuant to the Agreement, including where the Client provides Vista with access to the Client's systems for the purposes of providing the Support

Services. Where possible, the Parties will work together to ensure that Personal Data is anonymised by the Client prior to any transfer to Vista for Processing. Vista may also Process the Personal Data for the applicable purposes set out in clause 7.2 of the Standard Terms and for any additional purposes applicable to the SaaS Service as specified in the Key Terms.

4. The categories of the Personal Data to be Processed

Vista

The types of Personal Data to be Processed commonly includes, but is not limited to, the following information uploaded by the Client into the Services (as applicable):

(a) title; full name; address; email address; phone number(s);

(b) user account information, including: username; user ID; and transaction history;

(c) loyalty scheme member information - this is highly configurable by the Client, but may include member name; member ID; gender; date of birth; email address; phone number; photo; preferences for contact, movie genres, locations;

(d) payment card information, including: credit card details: first six and last four digits of the card name, cardholder's name as recorded on the card and card expiry date; and gift card details; and(e) any additional Personal Data applicable to the Services as specified in the Key Terms or a Statement of Work; and

(f) any other information uploaded by the Client into the SaaS Applications.

5. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

None.

7. The categories of Data Subject to whom the Personal Data relates

Vista: Client employees, end users, patrons, guests and the Client business contacts.

7. The obligations and rights of the Client

The obligations and rights of the Client are set out in the Agreement and these Terms.

8. Frequency of transfer (e.g. whether on a one-off or continuous basis) (EU standard contractual clauses only):

Continuous (ad-hoc).

9. Sub-Processors

The Sub-Processors set out on the Vista Cloud Sub-Processors page available at https://www.vista.co/list-of-sub-processors may act as Sub-Processors in accordance with these Terms (as applicable)

Exhibit B – Security measures

1. Overview

1.1

This Exhibit B sets out the security measures which Vista will take to ensure a level of security for the Personal Data appropriate to the level of the risk.

1.2

Any SaaS Application delivered under the Agreement is installed within Vista's subscription with the Cloud Service Providers.

1.3

Under the Agreement, the Client may request assistance from Vista support personnel in providing the Support Services, which may include the use of Vista Affiliates in accordance with clause 4.2 of the Data Processing Terms above. In order to adequately provide the Support Services, Vista and its Affiliates may need (i) to access the SaaS Application located in Vista's subscription with the Cloud Service Providers for the purpose of diagnosing the reason for the incident or issue; or (ii) a copy of the applicable SaaS Application's database to be transferred to Vista premises to aid in further investigations.

2. Remote Support

2.1

For any SaaS Service, the Client acknowledges and accepts that Vista's support personnel will have access to the subscription and therefore data stored within, including Personal Data, for the purposes of delivering the Support Services.

3. Anonymised Database to Vista Offices

3.1

Where Vista is required to retrieve a copy of the Client's database back to Vista's premises (the Database) to perform the requested Support Services and any Personal Data in that Database is not required to perform such Support Services, the Parties will work together in good faith to anonymise the Database prior to transfer as set out in this clause 3.

3.2

Prior to transferring the Database to Vista by uploading such Database on Vista's servers, the Client will, or Vista will on the Client's behalf:

(a) run a tool provided by Vista that identifies the type of Database and anonymises any Personal Data in the Database; and
(b) encrypt the Database. Only Vista can decrypt the Database to a useable state.

3.3

Where the Database is no longer required by Vista to carry out the requested Support Services, Vista will promptly and securely destroy the Database.

4. Non-anonymised database to Vista offices

4.1

In the rare event that Vista is required to retrieve a copy of a Database back to Vista's premises and any Personal Data in that Database is required to perform the Support Services, Vista will only work on a non-anonymised Database with the written approval of the Client's nominated Representative(s) (email to suffice).

4.2

Vista will securely hold and destroy the non-anonymised Database in accordance with the prescribed methods outlined in paragraph 5 below.

5. Confidentiality and security

5.1

In addition to the security methods detailed above, Vista will implement the following common measures and Processes set out below. Vista will:

(a) ensure the use of role-based access and login to sections with Personal Data (including the option of follow-up on/adjustment of role-based access) and that only authorised devices and authorised relevant personnel with a work-related need for Processing have access to the Personal Data. For example, only Vista's support personnel will connect to Vista's subscription with the Cloud Service Providers;

(b) ensure that any employee who changes roles within Vista does not retain access to Personal Data unless such Personal Data is required for their new role. When an employee leaves Vista, Vista will ensure that they do not have access to, or take with them, any Personal Data or business critical information. Vista will ensure that no previous employees or external consultants have access rights to the Vista systems holding Personal Data;

(c) ensure use of pseudonymisation and encryption of Personal Data where reasonable feasible;

(d) use secure/encrypted transfer of Personal Data on the open internet;

(e) ensure appropriate physical security of Personal Data, including:

- fit appropriate locks or other physical controls to the doors and windows of rooms where computers are kept;
- destroy or remove all Personal Data from media such as CDs before disposing of them; and
- ensure that all Personal Data is removed from the hard drives of any used computers before disposing of them.

(f) implement best practice access controls, including:

- best practice password procedures must be in place, including using strong passwords; and
- industry standard hard drive encryption for internal or external hard drives; and

(g) ensure suitable firewall and infrastructure logging to ensure the ongoing logging of failed login attempts or attacks on Vista systems, including log of time, user, etc. and block access after a certain number of failed login attempts for each user.

6. Integrity and availability

6.1

Vista will protect Personal Data, Vista's networks, systems and logs against tampering.

Vista will ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, including by backing-up data.

7. Resilience

7.1

Vista will have a vulnerability management program, including regular monitoring of potential vulnerabilities and performance of penetration tests of networks and Vista systems.

7.2

The vulnerability management program will include, but is not limited to:

(a) performing vulnerability scans on internal and external perimeters at least quarterly;

(b) performing penetration tests on external network perimeters at least annually or more frequently where incidents disclose the need for such tests; and

(c) following up on and remedy of any weaknesses identified in connection with such scans and tests.

On an ongoing basis, Vista will keep networks and systems up to date with regard to new versions, updates, and patches.

7.3

Vista will keep Vista networks and systems up to date with regard to new versions, updates, and patches on an ongoing basis.

8. Awareness, training and security checks in relation to Vista representatives

8.1

Vista will perform appropriate reference checks on all new employees.

8.2

Vista will provide training to new employees regarding information security and ensure that they read and understand Vista's internal policies related to information security and data protection. Vista will ensure that employees know where to find details of information security standards and procedures relevant to their role and responsibilities.

9. Incident response management and business continuity

9.1

Vista will ensure that employees understand what a Personal Data Breach and a security incident mean, and train employees to recognise the signs thereof and to respond appropriately.

9.2

Vista will have a Security Incident Response Plan (Plan) in place in the event of a serious security incident. The Plan will be regularly reviewed and will be reviewed after every Personal Data Breach and security incident in which the Plan is used and updated according to the lessons learned.

10. Monitoring

10.1

Vista will monitor and keep up to date all security measures, processes and risk analyses.

10.2

Vista will implement a process for periodical testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the Processing, including, but not limited to, the measures set out in these Terms.

10.3

Vista will implement procedures for effectively following up on non-compliance.