Data processing agreement

The terms on which Storiara processes personal data on a customer's behalf.

Processor Storiara Inc. **Applies to** Shared product and dedicated customer environments **Contact** security@storiara.com

This Data Processing Agreement ("Agreement") forms part of the contract for services ("Principal Agreement") between Storiara Inc. ("Storiara" or the "Processor") and the customer that has entered into the Principal Agreement (the "Customer"). Storiara and the Customer are together the "Parties". This Agreement applies from the date the Principal Agreement takes effect and for as long as Storiara Processes Customer Personal Data.

Background

A. The Customer acts as a Data Controller.

B. The Customer uses the Services, which involve the Processing of Personal Data by Storiara as a Data Processor on the Customer's behalf.

C. The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

D. The Parties wish to lay down their rights and obligations.

1. Definitions and interpretation

1.1 Unless otherwise defined in this Agreement, capitalised terms have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules;

1.1.2 "Customer Personal Data" means any Personal Data Processed by Storiara or a Subprocessor on behalf of the Customer pursuant to or in connection with the Principal Agreement;

1.1.3 "Data Protection Laws" means EU Data Protection Laws, UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country, including the California Consumer Privacy Act as amended;

1.1.4 "EEA" means the European Economic Area;

1.1.5 "EU Data Protection Laws" means the GDPR and laws implementing or supplementing the GDPR, as amended, replaced or superseded from time to time;

1.1.6 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.7 "UK Data Protection Laws" means the UK GDPR and the Data Protection Act 2018;

1.1.8 "Restricted Transfer" means a transfer of Customer Personal Data from the EEA, the United Kingdom or Switzerland to a country that has not been found to provide an adequate level of protection under the applicable Data Protection Laws;

1.1.9 "Standard Contractual Clauses" means the clauses annexed to Commission Implementing Decision (EU) 2021/914 and, for transfers from the United Kingdom, the International Data Transfer Addendum issued by the UK Information Commissioner;

1.1.10 "Services" means the film and television production planning services Storiara provides to the Customer under the Principal Agreement, in the shared Storiara product or in a dedicated customer environment;

1.1.11 "Subprocessor" means any person appointed by or on behalf of Storiara to Process Customer Personal Data in connection with the Principal Agreement.

1.2 The terms "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing", "Processor" and "Supervisory Authority" have the same meaning as in the GDPR, and their cognate terms are construed accordingly.

2. Processing of Customer Personal Data

2.1 Storiara shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Customer Personal Data; and

2.1.2 not Process Customer Personal Data other than on the Customer's documented instructions, unless Processing is required by a law to which Storiara is subject, in which case Storiara shall inform the Customer of that legal requirement before Processing, unless that law prohibits it.

2.2 The Customer instructs Storiara to Process Customer Personal Data as needed to provide the Services. The Principal Agreement, this Agreement and the Customer's use and configuration of the Services are the Customer's documented instructions. Schedule 1 describes the Processing.

2.3 Storiara shall not sell Customer Personal Data, share it for advertising, or use it for any purpose other than providing the Services. Storiara does not use Customer Personal Data to train artificial intelligence models.

2.4 Storiara shall inform the Customer if, in its opinion, an instruction infringes Data Protection Laws.

3. Storiara personnel

Storiara shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to Customer Personal Data. Access is limited to those individuals who need it for the purposes of the Principal Agreement, and every such individual is subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Storiara shall implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR. The measures in place are set out in Schedule 2.

4.2 In assessing the appropriate level of security, Storiara shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

4.3 Storiara may update the measures in Schedule 2 over time, provided the overall level of protection is not reduced.

5. Subprocessing

5.1 The Customer authorises Storiara to appoint the Subprocessors listed in Schedule 3. Storiara shall not appoint or disclose Customer Personal Data to any other Subprocessor except as set out in this section 5.

5.2 Storiara shall give the Customer at least 30 days' written notice before appointing a new Subprocessor. If the Customer objects on reasonable data protection grounds within that period, the Parties shall work in good faith to resolve the objection. If they cannot, the Customer may end the affected Services.

5.3 Storiara shall bind each Subprocessor by a written agreement with data protection obligations no less protective than those in this Agreement, and remains responsible to the Customer for each Subprocessor's performance.

5.4 Third-party services that the Customer chooses to connect to the Services are not Subprocessors.

6. Data Subject rights

6.1 Taking into account the nature of the Processing, Storiara shall assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws. The Services let the Customer view, correct, export and delete the Personal Data it holds in them.

6.2 Storiara shall:

6.2.1 promptly notify the Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data; and

6.2.2 not respond to that request except on the documented instructions of the Customer or as required by a law to which Storiara is subject, in which case Storiara shall, to the extent that law permits, inform the Customer of the legal requirement before responding.

7. Personal Data Breach

7.1 Storiara shall notify the Customer without undue delay, and in any event within 72 hours, upon becoming aware of a Personal Data Breach affecting Customer Personal Data. The notice shall give the Customer sufficient information to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws, and Storiara shall add to it as further information becomes available.

7.2 Storiara shall co-operate with the Customer and take the reasonable commercial steps the Customer directs to assist in the investigation, mitigation and remediation of each Personal Data Breach.

8. Data protection impact assessment and prior consultation

Storiara shall provide reasonable assistance to the Customer with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which the Customer reasonably considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any

other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by Storiara and its Subprocessors, and taking into account the nature of the Processing and the information available to them.

9. Deletion or return of Customer Personal Data

9.1 The Customer can export its data from the Services at any time during the term of the Principal Agreement.

9.2 Storiara shall delete Customer Personal Data, and procure its deletion by Subprocessors, promptly and in any event within 30 days of the date the Services involving the Processing of Customer Personal Data end (the "Cessation Date"). Where the Customer uses a dedicated customer environment, Storiara deletes that environment in full, including its database, files and encryption keys.

9.3 Copies held in backups are overwritten on a rolling schedule and expire within 7 days of deletion from the live systems. Storiara does not restore them for any purpose other than recovery of the Services during that period.

9.4 Storiara may retain Customer Personal Data only to the extent and for as long as a law to which Storiara is subject requires, and shall keep it confidential and Process it only for that purpose.

9.5 On request, Storiara shall confirm in writing that deletion has been completed.

10. Audit rights

10.1 Storiara shall make available to the Customer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of Customer Personal Data.

10.2 The Customer shall give at least 30 days' written notice of an audit, carry out no more than one audit in any 12-month period unless a Personal Data Breach has occurred or a Supervisory Authority requires it, conduct the audit during business hours without unreasonable disruption, and keep the results confidential. Each Party bears its own costs.

10.3 Where the Customer uses a dedicated customer environment, the audit log of that environment can be delivered to the Customer's own security monitoring system.

11. Data transfer

11.1 Storiara Processes Customer Personal Data in the United States, and the Customer authorises that Processing. Storiara shall not transfer Customer Personal Data to any other country, other than through the Subprocessors in Schedule 3, without the Customer's prior written consent.

11.2 Where the Processing involves a Restricted Transfer, the Parties rely on the Standard Contractual Clauses, which are incorporated into this Agreement by reference. Module Two (controller to processor) applies, with the Customer as data exporter and Storiara as data importer. Schedules 1, 2 and 3 provide the information required by the annexes to the Standard Contractual Clauses. If the Standard Contractual Clauses conflict with this Agreement, the Standard Contractual Clauses prevail.

12. General terms

12.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that (a) disclosure is required by law, or (b) the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing. Notices to Storiara are sent by email to security@storiara.com. Notices to the Customer are sent to the contact address the Customer has given under the Principal Agreement.

12.3 Order of precedence. If this Agreement conflicts with the Principal Agreement on the Processing of Customer Personal Data, this Agreement prevails. Liability under this Agreement is subject to the limits in the Principal Agreement.

12.4 Term. This Agreement ends when Storiara no longer Processes Customer Personal Data.

13. Governing law and jurisdiction

13.1 This Agreement is governed by the laws of the State of Delaware, United States, except where the Standard Contractual Clauses require the law of another jurisdiction.

13.2 Any dispute arising in connection with this Agreement that the Parties cannot resolve amicably will be submitted to the exclusive jurisdiction of the state and federal courts located in the State of Delaware.

14. Acceptance

The Parties accept this Agreement by entering into the Principal Agreement. No separate signature is required.

Schedule 1: Details of the Processing

SUBJECT MATTER	Provision of the Services to the Customer: planning, budgeting, scheduling and coordinating film and television productions.
DURATION	The term of the Principal Agreement, and the deletion period in section 9.
NATURE AND PURPOSE	Hosting, storing, organising, displaying and transmitting the information the Customer and its users enter into the Services; analysing scripts and production documents with automated tools to produce breakdowns, schedules and budgets; sending call sheets, invitations and messages by email and text at the Customer's direction; support and security monitoring.
CATEGORIES OF DATA SUBJECTS	The Customer's users (employees and contractors); cast, crew and other people working on the Customer's productions; contacts at the Customer's vendors and locations.
TYPES OF PERSONAL DATA	Name, email address, telephone number, job title, role and department; account identifiers and sign-in records; availability and scheduling details; rates and deal terms entered in a budget; contact details shown on call sheets; headshots or other images the Customer uploads; any Personal Data contained in scripts, receipts and other documents the Customer uploads.
SPECIAL CATEGORIES OF DATA	The Services are not designed for special categories of Personal Data, and the Customer agrees not to submit them.
FREQUENCY OF TRANSFER	Continuous, for the duration of the Services.
STORIARA CONTACT	security@storiara.com

Schedule 2: Technical and organisational measures

AREA	MEASURES
HOSTING	The Services run on Google Cloud in the United States. The database is stored across multiple regions. Storiara operates no servers or data centres of its own.
ENCRYPTION	Data is encrypted in transit with TLS and at rest. In a dedicated customer environment the database and the file storage are encrypted with customer-managed keys held in Google Cloud Key Management Service.
TENANT SEPARATION	In the shared product, every read and write is checked against project membership by database and storage security rules or by the server. A dedicated customer environment runs in its own Google Cloud project with its own database, file storage, sign-in directory, secrets and keys.
SIGN-IN AND ACCESS	Verified email and password, Google or Apple sign-in in the shared product. A dedicated customer environment is invitation only, offers two-step sign-in with an authenticator app that can be required for every user, and supports company single sign-on (SAML or OIDC) and SCIM user provisioning. Within a project, roles limit who can see budgets, scripts and other areas.
ADMINISTRATIVE ACCESS	Production administrator access is held by a single named officer of Storiara. Service accounts hold only the roles they use. Secrets are kept in Google Cloud Secret Manager.
LOGGING AND MONITORING	Google Cloud audit logs record administrative activity and reads and writes of the database, file storage and sign-in service. Alerts notify Storiara of function errors and unusual database activity. A dedicated customer environment can deliver its audit log to the Customer's security monitoring system.
BACKUP AND RECOVERY	The database is backed up daily and protected against deletion. Files are copied daily to separate storage held in two regions, with earlier versions kept. Backups are kept for 7 days. The recovery point objective is 48 hours and the recovery time objective is 24 hours.
SECURE DEVELOPMENT	All code is held in version control. Changes are checked automatically before release by type checking, linting, unit tests, tests of the security rules and a production build. Dependencies are monitored for known vulnerabilities.
ARTIFICIAL INTELLIGENCE	Automated analysis runs on Google Cloud Vertex AI under Storiara's own cloud account. Customer content is not used to train models.
DEVICES	Storiara staff work on Mac computers with full-disk encryption and a screen lock. Customer Personal Data is not stored on removable media.
POLICIES AND PEOPLE	Storiara maintains approved information security policies covering access control, data management, cryptography, secure development, operations security, incident response, business continuity and disaster recovery, risk management, third-party management and human resource security. A code of conduct applies to all staff. Storiara's cloud, source code and identity accounts are monitored continuously by a compliance platform.
INCIDENT RESPONSE	Storiara maintains an incident response plan and notifies the Customer of a Personal Data Breach as set out in section 7.

Schedule 3: Subprocessors

SUBPROCESSOR	PURPOSE	LOCATION
Google LLC (Google Cloud, Firebase, Vertex AI, Google Maps Platform)	Hosting, database, file storage, sign-in, automated analysis, address lookup and weather	United States
Twilio Inc.	Sending email and text messages	United States
Mapbox, Inc.	Maps and address search	United States
TypeSafe	Classifying budget line descriptions for production incentive tagging	United States
Stripe, Inc.	Subscription billing in the shared product	United States