

EU Data Protection Addendum (with standard contractual clauses)

The customer agreeing to these terms ("Customer") has entered into an agreement with Gumroad, Inc. (as applicable, "Gumroad") under which Gumroad has agreed to provide services to Customer (as amended from time to time, the "Agreement").

This Data Protection Addendum, including its attachments (the "Addendum") will be effective and replace any previously applicable data processing and security terms as of the Addendum Effective Date (as defined below). This Addendum forms part of the Agreement and consists of (a) the main body of the Addendum; (b) Attachment 1 (Subject Matter and Details of the Data Processing); (c) Attachment 2 (Security Measures); (d) Attachment 3 (Standard Contractual Clauses), including Appendices 1 and 2 thereto.

1. Definitions

For purposes of this Addendum, the terms below shall have the meanings set forth below. Capitalized terms that are used but not otherwise defined in this Addendum shall have the meanings set forth in the Agreement.

- 1.1. "Addendum Effective Date" means the date on which the parties agreed to this Addendum.
- 1.2. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.
- 1.3. "Audit Reports" has the meaning given in Section 5.4.4.
- 1.4. "Customer Personal Data" means any personal data contained within the data provided to or accessed by Gumroad by or on behalf of Customer or Customer end users in connection with the Services.
- 1.5. "EEA" means the European Economic Area.
- 1.6. "EU" means the European Union.
- 1.7. "European Data Protection Legislation" means the GDPR and other data protection laws of the EU, its Member States, and the United Kingdom, applicable to the processing of Customer Personal Data under the Agreement.
- 1.8. "GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- 1.9. "Information Security Incident" means a breach of Gumroad's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data in Gumroad's possession, custody or control. "Information Security Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- 1.10. "Model Contract Clauses" or "MCCs" mean the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.
- 1.11. "Security Documentation" means all documents and information made available by Gumroad under Section 5.4.1 (Reviews of Security Documentation).
- 1.12. "Security Measures" has the meaning given in Section 5.1.1 (Gumroad's Security Measures).
- 1.13. "Services" means the services and/or products to be provided by Gumroad to Customer under the Agreement.
- 1.14. "Subprocessors" means third parties authorized under this Addendum to process Customer Personal Data in relation to the Services.

- 1.15. “Term” means the period from the Addendum Effective Date until the end of Gumroad’s provision of the Services.
- 1.16. “Third Party Subprocessors” has the meaning given in Section 9 (Subprocessors).
- 1.17. “Transfer Solution” means the Model Contract Clauses or another solution that enables the lawful transfer of personal data to a third country in accordance with Article 45 or 46 of the GDPR (for example, the EU-U.S. Privacy Shield).
- 1.18. The terms “personal data”, “data subject”, “processing”, “controller”, “processor” and “supervisory authority” as used in this Addendum have the meanings given in the GDPR, and the terms “data importer” and “data exporter” have the meanings given in the Model Contract Clauses.

2. Duration of Addendum

This Addendum will take effect on the Addendum Effective Date and, notwithstanding the expiration of the Term, will remain in effect until, and automatically expire upon, Gumroad’s deletion of all Customer Personal Data as described in this Addendum.

3. Processing of Data

3.1. Roles and Regulatory Compliance; Authorization.

3.1.1. Processor and Controller Responsibilities. If the European Data Protection Legislation applies to the processing of Customer Personal Data, the parties acknowledge and agree that:

- (a) the subject matter and details of the processing are described in Attachment 1;
- (b) Except as provided in section 3.1.2 below, Gumroad is a processor of that Customer Personal Data under the European Data Protection Legislation;
- (c) Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Legislation; and
- (d) each party will comply with the obligations applicable to it under the European Data Protection Legislation with respect to the processing of that Customer Personal Data.

3.1.2. Gumroad’s Limited Capacity as a Controller. Gumroad is a data controller over any personal data that Gumroad collects in connection with an individual establishing an account with Gumroad’s Services, including account login information, email address, and other data stored in the data subject’s Gumroad account, with the exception of the details of a data subject’s purchase(s) with Customer.

3.1.3. Authorization by Third Party Controller. If the European Data Protection Legislation applies to the processing of Customer Personal Data and Customer is a processor, Customer warrants to Gumroad that Customer’s instructions and actions with respect to that Customer Personal Data, including its appointment of Gumroad as another processor, have been authorized by the relevant controller.

3.2. Scope of Processing.

3.2.1. Customer’s Instructions. By entering into this Addendum, Customer instructs Gumroad to process Customer Personal Data only in accordance with applicable law: (a) to provide the Services; (b) as authorized by the Agreement, including this Addendum; and (c) as further documented in any other written instructions given by Customer and acknowledged in writing by Gumroad as constituting instructions for purposes of this Addendum.

3.2.2. Gumroad’s Compliance with Instructions. Gumroad will only process Customer Personal Data in accordance with Customer’s instructions described in Section 3.2.1 (including with regard to data transfers) unless European Data Protection Legislation to which Gumroad is subject requires other processing of Customer Personal Data by Gumroad, in which case Gumroad will notify Customer (unless that law prohibits Gumroad from doing so on important grounds of public interest).

4. Data Deletion

- 4.1. Deletion on Termination. On expiry of the Term, Customer instructs Gumroad to delete all Customer Personal Data (including existing copies) from Gumroad's systems in accordance with applicable law as soon as reasonably practicable, unless applicable law requires otherwise.

5. Data Security

5.1. Gumroad's Security Measures, Controls and Assistance.

- 5.1.1. Gumroad's Security Measures. Gumroad will implement and maintain technical and organizational measures to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data as described in Attachment 2 (the "Security Measures"). Gumroad may update or modify the Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

- 5.1.2. Security Compliance by Gumroad Staff. Gumroad will grant access to Customer Personal Data only to employees, contractors and Subprocessors who need such access for the scope of their performance, and are subject to appropriate confidentiality arrangements.

- 5.1.3. Gumroad's Security Assistance. Gumroad will (taking into account the nature of the processing of Customer Personal Data and the information available to Gumroad) provide Customer with reasonable assistance necessary for Customer to comply with its obligations in respect of Customer Personal Data under European Data Protection Legislation, including Articles 32 to 34 (inclusive) of the GDPR, by:

- (a) implementing and maintaining the Security Measures in accordance with Section 5.1.1 (Gumroad's Security Measures);
- (b) complying with the terms of Section 5.2 (Information Security Incidents); and
- (c) providing Customer with the Security Documentation in accordance with Section 5.4.1 (Reviews of Security Documentation) and the Agreement, including this Addendum.

5.2. Information Security Incidents

- 5.2.1. Information Security Incident Notification. If Gumroad becomes aware of an Information Security Incident, Gumroad will: (a) notify Customer of the Information Security Incident without undue delay after becoming aware of the Information Security Incident; and (b) take reasonable steps to identify the cause of such Information Security Incident, minimize harm and prevent a recurrence.

- 5.2.2. Details of Information Security Incident. Notifications made pursuant to this Section 5.2 (Information Security Incidents) will describe, to the extent possible, details of the Information Security Incident, including steps taken to mitigate the potential risks and steps Gumroad recommends Customer take to address the Information Security Incident.

- 5.2.3. Notification. Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Information Security Incident(s).

- 5.2.4. No Acknowledgement of Fault by Gumroad. Gumroad's notification of or response to an Information Security Incident under this Section 5.2 (Information Security Incidents) will not be construed as an acknowledgement by Gumroad of any fault or liability with respect to the Information Security Incident.

5.3. Customer's Security Responsibilities and Assessment

- 5.3.1. Customer's Security Responsibilities. Customer agrees that, without prejudice to Gumroad's obligations under Section 5.1 (Gumroad's Security Measures, Controls and Assistance) and Section 5.2 (Information Security Incidents):

- (a) Customer is solely responsible for its use of the Services, including:

- (i) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Data;
 - (ii) securing the account authentication credentials, systems and devices Customer uses to access the Services;
 - (iii) securing Customer's systems and devices Gumroad uses to provide the Services; and
 - (iv) backing up its Customer Personal Data; and
- (b) Gumroad has no obligation to protect Customer Personal Data that Customer elects to store or transfer outside of Gumroad's and its Subprocessors' systems (for example, offline or on-premises storage).

5.3.2. Customer's Security Assessment.

- (a) Customer is solely responsible for reviewing the Security Documentation and evaluating for itself whether the Services, the Security Measures and Gumroad's commitments under this Section 5 (Data Security) will meet Customer's needs, including with respect to any security obligations of Customer under the European Data Protection Legislation.
- (b) Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals) the Security Measures implemented and maintained by Gumroad as set out in Section 5.1.1 (Gumroad's Security Measures) provide a level of security appropriate to the risk in respect of the Customer Personal Data.

5.4. Reviews and Audits of Compliance

- 5.4.1. Customer may audit Gumroad's compliance with its obligations under this Addendum up to once per year. In addition, to the extent required by European Data Protection Legislation, including where mandated by Customer's supervisory authority, Customer or Customer's supervisory authority may perform more frequent audits (including inspections). Gumroad will contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of processing activities applicable to the Services.
- 5.4.2. If a third party is to conduct the audit, Gumroad may object to the auditor if the auditor is, in Gumroad's reasonable opinion, not suitably qualified or independent, a competitor of Gumroad, or otherwise manifestly unsuitable. Such objection by Gumroad will require Customer to appoint another auditor or conduct the audit itself.
- 5.4.3. To request an audit, Customer must submit a detailed proposed audit plan to its Chief Technology Officer at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Gumroad will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Gumroad security, privacy, employment or other relevant policies). Gumroad will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 5.4 shall require Gumroad to breach any duties of confidentiality.
- 5.4.4. If the requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor ("Audit Reports") within twelve (12) months of Customer's audit request and Gumroad confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.
- 5.4.5. The audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and Gumroad's health and safety or other relevant policies, and may not unreasonably interfere with Gumroad business activities.

5.4.6. Customer will promptly notify Gumroad of any non-compliance discovered during the course of an audit and provide Gumroad any audit reports generated in connection with any audit under this Section 5.4, unless prohibited by European Data Protection Legislation or otherwise instructed by a supervisory authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this Addendum. The audit reports are Confidential Information of the parties under the terms of the Agreement.

5.4.7. Any audits are at Customer's expense. Customer shall reimburse Gumroad for any time expended by Gumroad or its Third Party Subprocessors in connection with any audits or inspections under this Section 5.4 at Gumroad's then-current professional services rates, which shall be made available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

5.4.8. The parties agree that this Section 5.4 shall satisfy Gumroad's obligations under the audit requirements of the Model Contractual Clauses applied to Data Importer under Clause 5(f) and to any Sub-processors under Clause 11 and Clause 12(2).

6. Impact Assessments and Consultations

Gumroad will (taking into account the nature of the processing and the information available to Gumroad) reasonably assist Customer in complying with its obligations under European Data Protection Legislation in respect of data protection impact assessments and prior consultation, including, if applicable, Customer's obligations pursuant to Articles 35 and 36 of the GDPR, by:

6.1. Making available for review copies of the Audit Reports or other documentation describing relevant aspects of Gumroad's information security program and the security measures applied in connection therewith; and

6.2. providing the information contained in the Agreement including this Addendum.

7. Data Subject Rights

7.1. Responsibility for Requests. During the Term, if Gumroad receives any request from a data subject in relation to Customer Personal Data for which Gumroad is not a controller, Gumroad will advise the data subject to submit their request to Customer and Customer will be responsible for responding to any such request. Customer acknowledges and agrees that if Gumroad receives a request from a data subject in relation to personal data for which Gumroad is a Controller, Gumroad will respond to the request in its sole discretion.

7.2. Gumroad's Data Subject Request Assistance. Gumroad will (taking into account the nature of the processing of Customer Personal Data) provide Customer with self-service functionality through the Services or other reasonable assistance as necessary for Customer to fulfil its obligation under European Data Protection Legislation to respond to requests by data subjects, including if applicable, Customer's obligation to respond to requests for exercising the data subject's rights set out in Chapter III of the GDPR. Customer shall reimburse Gumroad for any such assistance beyond providing self-service features included as part of the Services at Gumroad's then-current professional services rates, which shall be made available to Customer upon request.

8. Data Transfers

8.1. Data Storage and Processing Facilities. Gumroad may, subject to Section 8.2 (Transfers of Data Out of the EEA), store and process Customer Personal Data anywhere Gumroad or its Subprocessors maintains facilities.

8.2. Transfers of Data Out of the EEA.

8.2.1. Gumroad's Transfer Obligations. If the storage and/or processing of Customer Personal Data (as set out in Section 8.1 (Data Storage and Processing Facilities)) involves transfers of Customer Personal Data out of the EEA or Switzerland, and the European Data Protection Legislation applies to the transfers of such data ("Transferred Personal

Data”), Gumroad will make such transfers in accordance with a Transfer Solution, and make information available to Customer about such Transfer Solution upon request.

8.2.2. Customer's Transfer Obligations. In respect of Transferred Personal Data, Customer agrees that if under European Data Protection Legislation Gumroad reasonably requires Customer to enter into Model Contract Clauses or use another Transfer Solution offered by Gumroad, and reasonably requests that Customer take any action (which may include execution of documents) required to give full effect to such solution, Customer will do so.

8.3. Disclosure of Confidential Information Containing Personal Data. If Customer has entered into Model Contract Clauses as described in Section 8.2 (Transfers of Data Out of the EEA), Gumroad will, notwithstanding any term to the contrary in the Agreement, make any disclosure of Customer's Confidential Information containing personal data, and any notifications relating to any such disclosures, in accordance with such Model Contract Clauses. For the purposes of the Model Contract Clauses, Customer and Gumroad agree that (i) Customer will act as the data exporter on Customer's own behalf and on behalf of any of Customer's entities and (ii) Gumroad or its relevant Affiliate will act on its own behalf and/or on behalf of Gumroad's Affiliates as the data importers.

9. Subprocessors

9.1. Consent to Subprocessor Engagement. Customer specifically authorizes the engagement of Gumroad's Affiliates as Subprocessors. In addition, Customer generally authorizes the engagement of any other third parties as Subprocessors (“Third Party Subprocessors”). If Customer has entered into Model Contract Clauses as described in Section 9.2 (Transfers of Data Out of the EEA), the above authorizations will constitute Customer's prior written consent to the subcontracting by Gumroad of the processing of Customer Personal Data if such consent is required under the Model Contract Clauses.

9.2. Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at <http://help.gumroad.com/326595-can-i-have-your-list-of-subprocessors>.

9.3. Requirements for Subprocessor Engagement. When engaging any Subprocessor, Gumroad will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in the Agreement (including this Addendum) with respect to the protection of Customer Personal Data to the extent applicable to the nature of the Services provided by such Subprocessor. Gumroad shall be liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

9.4. Opportunity to Object to Subprocessor Changes.

When any new Third Party Subprocessor is engaged during the Term, Gumroad will, at least 30 days before the new Third Party Subprocessor processes any Customer Personal Data, notify Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform).

Customer may object to any new Third Party Subprocessor by providing written notice to Gumroad within ten (10) business days of being informed of the engagement of the Third Party Subprocessor as described above. In the event Customer objects to a new Third Party Subprocessor, Customer and Gumroad will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement by providing written notice to Gumroad.

10. Processing Records

10.1. Gumroad's Processing Records. Customer acknowledges that Gumroad is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Gumroad is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly, if the GDPR applies to the processing of Customer Personal Data, Customer will, where

requested, provide such information to Gumroad, and will ensure that all information provided is kept accurate and up-to-date.

11. Liability

11.1. Liability Cap. The total combined liability of either party and its Affiliates towards the other party and its Affiliates, whether in contract, tort or any other theory of liability, under or in connection with the Agreement, this Addendum, and the Model Contract Clauses if entered into as described in Section 8.2 (Transfers of Data Out of the EEA) combined will be limited to limitations on liability or other liability caps agreed to by the parties in the Agreement, subject to Section 11.2 (Liability Cap Exclusions).

11.2. Liability Cap Exclusions. Nothing in Section 11.1 (Liability Cap) will affect any party's liability to data subjects under the third party beneficiary provisions of the Model Contract Clauses to the extent limitation of such rights is prohibited by the European Data Protection Legislation.

12. Third Party Beneficiary

Notwithstanding anything to the contrary in the Agreement, where Gumroad is not a party to the Agreement, Gumroad will be a third party beneficiary of Section 5.4 (Reviews and Audits of Compliance), Section 9.1 (Consent to Subprocessor Engagement) and Section 11 (Liability) of this Addendum.

13. Analytics

Customer acknowledges and agrees that Gumroad may create and derive from processing related to the Services anonymized and/or aggregated data that does not identify Customer or any natural person, and use, publicize or share with third parties such data to improve Gumroad's products and services and for its other legitimate business purposes.

14. Notices

Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Gumroad to Customer may be given (a) in accordance with the notice clause of the Agreement; (b) to Gumroad's primary points of contact with Customer; and/or (c) to any email provided by Customer for the purpose of providing it with Service-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

15. Effect of These Terms

Notwithstanding anything to the contrary in the Agreement, to the extent of any conflict or inconsistency between this Addendum and the remaining terms of the Agreement, this Addendum will govern.

Attachment 1

Subject Matter and Details of the Data Processing

Subject Matter	Gumroad's provision of cloud computing services to Customer.
Duration of the Processing	The Term plus the period from the expiry of the Term until deletion of all Customer Personal Data by Gumroad in accordance with the Addendum.
Nature and Purpose of the Processing	Gumroad will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with the Addendum.
Categories of Data	Data relating to individuals provided to Gumroad in connection with the Services, by (or at the direction of) Customer.
Data Subjects	Data subjects include the individuals about whom Gumroad Processes data in connection with the Services.

Attachment 2

Security Measures

As from the Addendum Effective Date, Gumroad will implement and maintain the Security Measures set out in this Attachment 2. Gumroad may update or modify such Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.

- 1) Organizational management and staff responsible for the development, implementation and maintenance of Gumroad's information security program.
- 2) Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Gumroad's organization, monitoring and maintaining compliance with Gumroad's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.
- 3) Data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available and industry standard encryption technologies for Personal Data that is:
 - a) transmitted over public networks (i.e. the Internet) or when transmitted wirelessly; or
 - b) at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).
- 4) Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).
- 5) Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Gumroad's passwords that are assigned to its employees: (i) require two factor authentication, (ii) not be stored in readable format on Gumroad's computer systems;
- 6) System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review going back 1 month.
- 7) Physical and environmental security of data center, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of Gumroad facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
- 8) Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Gumroad's possession.
- 9) Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to Gumroad's technology and information assets.
- 10) Incident / problem management procedures design to allow Gumroad to investigate, respond to, mitigate and notify of events related to Gumroad's technology and information assets.
- 11) Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

- 12) Vulnerability assessment, patch management and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
- 13) Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

Attachment 3

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Customer, as identified in the Agreement

(the data **exporter**)

and

Name of the data importing organisation: Gumroad, Inc.

Address: 225 Valencia St Suite A, San Francisco, CA 94103

e-mail: support@gumroad.com

Other information needed to identify the organization: N/A

(the data **importer**)

each a **party**; together **the parties**,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) *‘the data exporter’* means the controller who transfers the personal data;
- (c) *‘the data importer’* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *‘the subprocessor’* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *‘the applicable data protection law’* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *‘technical and organisational security’ measures* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

that it will ensure compliance with the security measures;

that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause (3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

that it will promptly notify the data exporter about:

- (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
- (ii) any accidental or unauthorised access, and
- (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

that the processing services by the subprocessor will be carried out in accordance with Clause 11;

to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

2. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

1. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

3. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

to refer the dispute to the courts in the Member State in which the data exporter is established.

The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

4. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, as set out in Appendix 3 below.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

5. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, as set out in Appendix 3 below.

The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

6. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
7. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is: The party that has executed the Standard Contractual Clauses as a Data Exporter

Data importer

The data importer is (please specify briefly activities relevant to the transfer): Gumroad, a provider of cloud computing services that processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement

Data subjects

The personal data transferred concern the following categories of data subjects (please specify): the individuals about whom Gumroad Processes data in connection with the Services

Categories of data

Data relating to individuals provided to Gumroad in connection with the Services, by (or at the direction of) Customer

Special categories of data (if appropriate)

N/A

Processing operations

Gumroad will process Customer Personal Data for the purposes of providing the Services to Customer in accordance with the Addendum.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See the security measures identified in Attachment 2 to the Addendum