DataCamp, Inc. Data Processing Addendum

This Data Processing Addendum (**"DPA"**) forms part of the Agreement between DataCamp, Inc. and its affiliates (collectively, **"DataCamp"**) and the entity entering the Agreement as a customer of DataCamp's Services (**"Customer"**). DataCamp and Customer may be collectively referred to herein as the "**Parties**" or individually as a "**Party**."

This DPA is supplemental to the Agreement and sets out the terms that apply when Personal Data is Processed by DataCamp under the Agreement. The Parties agree to comply with the following provisions with respect to DataCamp's Processing of Customer Data. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.

Definitions

"Admin" means the person listed as administrator as part of the business subscription plan for the Services.
"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "**Control**" for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
"**Agreement**" means DataCamp's Standard Terms of Use, or any order form, master service agreement, or any other written agreement which is executed and signed by an authorized representative of DataCamp, which governs the provision of the Services to Customer.
"**Anonymous Data**" means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person, directly or indirectly, by DataCamp or any other party reasonably likely to receive, or access that anonymized Personal Data.
"**CCPA**" means the California Consumer Privacy Act of 2018 and any binding regulations promulgated thereunder, in each case, as may be amended from time to time.
"**Customer Data**" means any Personal Data that DataCamp processes on behalf of Customer in the course of providing Services as either (i) a Data Processor for purposes of EU Data Protection Law, or (ii) a Service Provider for purposes of CCPA.
"**Data Protection Law**" means all data protection laws and regulations applicable to a Party's processing of Customer Data under the Agreement, including, where applicable, EU Data Protection Law and CCPA.
"**Data Controller**" means an entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
"**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.
"**Data Subject**" means the individual to whom Personal Data relates.
"**EU Data Protection Law**" means data protection laws applicable in Europe, including: (i) Regulation 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) ("**GDPR**"); (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector; (iii) applicable national implementations of (i) and (ii) or, in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union; and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance; in each case, as may be amended, superseded or replaced.
"**Europe**" means the European Economic Area ("**EEA**") (which comprises the member

states of the European Union, Norway, Iceland and Liechtenstein), the United Kingdom and Switzerland.
"**Personal Data**" means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is afforded protections as personal data, personal information or personally identifiable information under applicable Data Protection Law.
"**Processing**" has the meaning given to it under Data Protection Law or if not defined thereunder, the GDPR and "**process**", "**processes**" and "**processed**" will be interpreted accordingly.
"**Security Incident**" means any unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer Data. Security Incident will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
"**Services**" means any product or service provided by DataCamp to Customer pursuant to the Agreement.
"Standard Contractual Clauses" or "**SCCs**" means the European Commission's Standard Contractual Clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC (as may be amended, superseded or replaced), as set out in the Annex to Commission Decision 2010/87/EU, a completed copy of which comprises **Annex D** and which forms a part of this DPA.
"**Sub-processor**" means any Data Processor engaged by DataCamp or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or DataCamp's Affiliates but will exclude DataCamp employees.

1. Roles and Scope of Processing

a. Applicability. This DPA only applies to Customer Data that is subject to Data Protection Law and only to the extent that DataCamp processes Customer Data on behalf of Customer in the course of providing Services. This DPA does not apply to Personal Data that DataCamp processes as a Controller or to Anonymous Data.

b. Roles of the Parties. Customer determines the purpose and means of the processing of Personal Data and is therefore the Data Controller. DataCamp will process Customer Data only as a Data Processor acting on behalf of Customer and DataCamp or its Affiliates will engage Sub-processors pursuant to the requirements set forth in Section 2 "**Sub-processing**" below.

c. Customer Compliance. Customer agrees that (i) it will comply with all Data Protection Law in respect of its use of the Services, its processing of Personal Data and any processing instructions it issues to DataCamp; (ii) it will ensure it has the right to transfer, or provide access to, Personal Data to DataCamp for processing pursuant to the Agreement and this DPA; and (iii) it will have sole responsibility for the accuracy, quality and legality of Customer Data and the means by which Customer acquired such Customer Data.

d. Purpose Limitation. DataCamp shall process Customer Data only (i) in accordance with Customer's documented lawful instructions as set forth in the Agreement and this DPA including **Annex A** attached hereto; (ii) as required by Data Protection Law; and (iii) as further documented in any other written instructions given by Customer and acknowledged by DataCamp as constituting instructions for purposes of this DPA. The Parties agree that this DPA and the Agreement set out Customer's complete and final instructions to DataCamp in relation to the processing of Customer Data, and processing outside the scope of these instructions (if any) shall require prior written agreement between the Parties. When DataCamp considers an instruction in conflict with Data Protection Law, it will immediately notify Customer thereof. In addition, when DataCamp is under a legal obligation to process Customer Data outside of Customer instructions, it will immediately notify Customer thereof unless DataCamp is legally prohibited from doing so.

e. Prohibited Data. Customer will not provide (or cause to be provided) any Personal Data that falls within the definition of "special categories of data" or "sensitive personal information" under Data Protection Law, and DataCamp will have no liability whatsoever for such special categories of data or sensitive personal information, whether in connection with a Security Incident or otherwise. For the avoidance of doubt, this DPA will not apply to such special categories of data or sensitive personal information.

2. **Sub-processing**

a. Sub-processors. Customer agrees that (a) DataCamp may engage its Affiliates and third-party sub-processors for specific processing activities ("**Sub-processors**") and (b) such Sub-processors may engage third party processors to process Customer Data on DataCamp's behalf. The Sub-processors currently engaged by DataCamp and authorized by Customer are listed in **Annex B**.

i. DataCamp will: (i) enter into a written agreement with the Sub-processor imposing data protection obligations that protect Customer Data to the standard required by Data Protection Law; and (ii) remain liable to Customer for any breach of the DPA caused by the Sub-processor, but only to the same extent that DataCamp would be liable if it had provided the services of the Sub-processor directly under the terms of this DPA.

ii. DataCamp will: (i) provide an up-to-date list of the Sub-processors it has appointed on request; and (ii) notify Customer (for which email or a notice in the Services will suffice) if it appoints or replaces a Sub-processor at least ten (10) days prior to any such changes.

b. Objection to Sub-processors. Customer may object in writing to DataCamp's appointment or replacement of a Sub-processor within five (5) calendar days of such notice, provided that such objection is based on reasonable grounds related to data

protection. In such event, the Parties will discuss such concerns in good faith with a view to achieving a resolution. If the Parties do not find a solution within fifteen (15) calendar days after Customer has objected to the appointment or replacement of a Sub-processor, both Parties are entitled to terminate the Agreement and this DPA with immediate effect (without prejudice to any fees incurred by Customer prior to the termination of the Agreement and this DPA).

3. **Security**

a. Confidentiality Obligations. DataCamp will ensure that any personnel authorized by DataCamp to process Customer Data will be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

b. Security Measures. DataCamp will maintain appropriate technical and organizational measures to secure Customer Data as outlined in **Annex C** attached hereto, including measures to protect against Security Incidents. These measures refer to a suitable level of security, taking into account the state of the art and the costs of implementation, as well as the risks inherent in data processing proposed by DataCamp and the nature of Customer Data. DataCamp may update or modify such measures from time to time, provided that such updates and modifications do not materially decrease the overall security of the Services.

c. Security Incidents. Upon becoming aware of a Security Incident, DataCamp will notify Customer without undue delay and will provide such information as Customer may reasonably require, including to enable Customer to fulfill its data breach reporting obligations under Data Protection Law. DataCamp's notification of or response to a Security Incident will not be construed as an acknowledgement by DataCamp of any fault or liability with respect to the Security Incident. If DataCamp is not liable for the Security Incident, DataCamp reserves the right to charge a reasonable administrative fee which will be proportional to the effort required to provide assistance.

d. Customer's Appropriate Use of Services. Customer agrees that, without prejudice to DataCamp's obligations under this DPA, (i) Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of Customer Data; and (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; and (ii) DataCamp has no obligation to protect Customer Data that Customer elects to store or transfer outside of DataCamp's and/or its Sub-processors' systems.

4. **International Transfers**

a. Location of Processing. Customer acknowledges that DataCamp may transfer, store and process Customer Data anywhere in the world where DataCamp, its Affiliates or

its Sub-processors maintain data processing operations. DataCamp will at all times ensure that such transfers are made in compliance with the requirements of Data Protection Law.

b. European Transfer Mechanism. The Standard Contractual Clauses, attached hereto as **Annex D**, will apply to Customer Data that is transferred outside the EEA, the United Kingdom or Switzerland, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data. The SCCs will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA, the United Kingdom or Switzerland. Notwithstanding the foregoing, the SCCs (or obligations the same as those under the SCCs) will not apply if DataCamp has adopted, at its sole discretion, an alternative, recognized compliance standard for the lawful transfer of Personal Data outside the EEA, the United Kingdom or Switzerland. If the SCCs in the form attached hereto as **Annex D** are updated, superseded or replaced and such change may have a material effect on the rights or obligations of the Parties under this DPA, then DataCamp may require, and Customer may request, that the Parties enter into a replacement set of SCCs in accordance with EU Data Protection Law.

5. **Cooperation and Audits**

a. Data Subject Rights. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, DataCamp will provide Customer with reasonable cooperation and assistance insofar as this is possible, at Customer's expense, to enable Customer to respond to requests from Data Subjects seeking to exercise their rights under Data Protection Law. In the event such request is made directly to DataCamp, DataCamp will promptly inform Customer of the same. Customer authorizes DataCamp to respond to requests from Data Subjects seeking to exercise their rights under the GDPR or the CCPA in order to clarify requests and/or to resolve ordinary customer support requests.

b. Data Protection Impact Assessments. To the extent required under applicable EU Data Protection Law, DataCamp will (taking into account the nature of the processing and the information available to DataCamp) provide all reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by EU Data Protection Law; provided, however, that DataCamp will not be liable for any failure of Customer to comply with Customer's own obligations related thereto.

c. Audits. Upon Customer's reasonable written request, and no more than once per calendar year, DataCamp will make available for Customer's inspection and audit, copies of certifications, records or reports demonstrating DataCamp's compliance with this DPA. While it is the Parties' intention ordinarily to rely on the provision of the documentation to demonstrate DataCamp's compliance with this DPA and the

provisions of Article 28 of the GDPR, in the event that Customer reasonably determines that it must inspect DataCamp's premises or equipment for purposes of this DPA, then no more than once per calendar year, any audits described in this Section 5(c) will be conducted, at Customer's expense, through a qualified, independent third-party auditor ("**Independent Auditor**") designated by Customer. Before the commencement of any such on-site inspection, the Parties will mutually agree on reasonable timing, scope, and security controls applicable to the audit (including without limitation restricting access to DataCamp's confidential information, trade secrets and data belonging to other customers). Any inspection will be of reasonable duration and will not unreasonably interfere with DataCamp's day-to-day operations. All Independent Auditors are required to enter into a non-disclosure agreement containing confidentiality provisions reasonably acceptable to DataCamp and intended to protect DataCamp's and its customers' confidential and proprietary information. To the extent that Customer or any Independent Auditor causes any damage, injury or disruption to DataCamp's premises, equipment, personnel and business in the course of such an audit or inspection, Customer will be solely responsible for any costs associated therewith. Customer will promptly notify DataCamp with information regarding any alleged non-compliance discovered during the course of an audit.

6. **Deletion or Return of Customer Data**

a. Upon request by Customer at the termination or expiration of the Agreement, DataCamp will delete or return Customer Data and copies thereof to Customer that are in DataCamp's possession. Notwithstanding the foregoing, DataCamp may retain copies of Customer Data: (x) to the extent DataCamp has a separate legal right or obligation to retain some or all of the Customer Data; (y) that is incorporated into DataCamp business records such as email and accounting records, and (z) in backup systems until the backups have been overwritten or expunged in accordance with DataCamp's backup policy; provided, however, in each case the confidentiality obligations and use restrictions in the Agreement will continue to apply to such Customer Data for the duration of the retention. The Parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the SCCs will be provided by DataCamp to Customer only upon Customer's request.

7. CCPA

a. Scope. This Section 7 will apply only with respect to Personal Data that is subject to the protection of the CCPA. For purposes of this Section 7, the terms "Business," "sell," "Third Party" and "Service Provider" have the meanings given in the CCPA.

b. Roles of the Parties. With respect to Customer Data as to which CCPA applies, the Parties acknowledge and agree that: (a) DataCamp is a "Service Provider" and not a "Third Party"; (b) Customer is a "Business;" and (c) each Sub-processor is a "Service

Provider". The Parties agree that Customer will disclose to DataCamp the Customer Data as to which CCPA applies for the business purpose of enabling DataCamp to perform the Services in accordance with the Agreement and subject to the requirements of this DPA, including without limitation those set forth in Section 7(c) (No Sale).

c. No Sale. DataCamp will not: (a) "sell" Customer Data; (b) retain, use, or disclose Customer Data for any purpose other than for the specific purpose of performing the Services; (c) retain, use, or disclose Customer Data for a commercial purpose other than providing the Services; or (d) retain, use, or disclose Customer Data outside of the direct business relationship between DataCamp and the Customer. DataCamp certifies that it understands these restrictions and will comply with them.

8. **Liability**

a. Indemnification. DataCamp will indemnify Customer from and against all third party claims, liabilities, costs, damages, judgments, expenses and losses (including reasonable attorneys' fees and costs) arising from any breach by DataCamp of this DPA; provided however, under no circumstances will DataCamp be liable for any breaches of this DPA or violations of Data Protection Law that are caused by Customer. Any such indemnification obligation of DataCamp is contingent upon:
    i. Customer promptly notifying DataCamp in writing of any claim which could give rise to an indemnification obligation;
    ii. DataCamp being given the possibility to control the defense of any litigation and to settle or compromise all claims which could give rise to this indemnification obligation (provided that Customer may always appoint advisory counsel at its own expense to assist DataCamp in the defense of such claim);
    iii. Customer cooperating in all reasonable respects and at its own expense with DataCamp in the defense of the claim.

b. This clause is without prejudice to the liability of each Party to Data Subjects that cannot lawfully be limited or disclaimed and the obligations of both Parties to indemnify Data Subjects as set out in Article 82 of the GDPR and in Article 6 of the SCCs.

c. Where DataCamp is obliged to provide assistance to Customer or third parties at the request of Customer (including submission to an audit hereunder and/or the provision of information) in connection with this DPA or the Data Protection Law, such assistance will be provided at the sole cost and expense of Customer, save where such assistance directly arises from DataCamp's breach of its obligations under this DPA, in which event the costs of such assistance will be borne by DataCamp.

d. Limitation of Liability. Each Party's liability to the other taken together in the aggregate, arising out of or related to this DPA (including the SCCs), whether in contract, tort or under any other theory of liability, is subject to the exclusions and limitations of liability set forth in the Agreement and any reference in such sections to the liability of a Party means aggregate liability of that Party and all of its Affiliates under the Agreement (including this DPA). Under no circumstances will DataCamp be liable for any violations of this DPA or violations of Data Protection Law that are caused by Customer.

9. Miscellaneous

a. Effective Date. This DPA will become effective on the latest signed date by both Parties below ("**Effective Date**"). If DataCamp has already processed Personal data within the scope of the Agreement prior to the Effective Date, the DPA will apply retroactively from the start of the processing of Personal Data by DataCamp on behalf of Customer.

b. Agreement. Except as amended by this DPA, the Agreement will remain in full force and effect.

c. Priority. If there is a conflict between this DPA and the Agreement, the DPA will control. In the event of a conflict between the terms of the DPA and the SCCs, the SCCs will prevail.

d. Modifications. Customer agrees that DataCamp may modify this DPA at any time provided DataCamp may only modify the SCCs (i) to incorporate any new version of the SCCs (or similar model clauses) that may be adopted under GDPR or (ii) to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency. If DataCamp makes any material modifications to this DPA, DataCamp shall provide Customer with at least ten (10) days' notice (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect by either: (a) sending an email to the Admin; or (b) alerting Customer via the Services. If Customer reasonably objects to any such change, Customer may terminate the Agreement and this DPA by giving written notice to DataCamp within ten (10) days of notice from DataCamp of the change.

e. Governing Law. This DPA will be governed by and construed in accordance with the governing law stated in the Agreement, unless required otherwise by applicable Data Protection Law.

f. Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

Annex A

Description of processing

Subject Matter	● DataCamp's provision of the Services to Customer
Nature and purposes of the processing	● Providing an online education service on the DataCamp website located at http://www.datacamp.com and a mobile application ● Communicating with users on the DataCamp website or email (incl. helpdesk)
Duration of the Processing	● Until deletion of all Customer Data in accordance with the DPA.
Categories of Personal data	● Personal identifiers: name, email, telephone, avatar ● Electronic identifiers: Device ID, IP address, tracking ID ● Financial data (as applicable): credit card information, billing information and/or transaction information ● Professional data: company name, company domain ● Educational data (if applicable): school name, faculty page, teaching role ● Account information: learning history, exercise submissions
Categories of Data Subjects	● Users ● Account Administrators
Categories of Recipients	● DataCamp employees and individual self-employed contractors ● DataCamp Sub-processors

Annex B - List of DataCamp Sub-processors

DataCamp, Inc. uses its Affiliates (Data Science Central UK Ltd. and DataCamp Belgium BV), self- employed independent contractors for customer support (Vietnam) and a range of third-party sub-processors (set forth below) to assist DataCamp, Inc. in providing the Services.

Name	Nature of processing	Entity HQ Location	Data Processing Location
Adyen N.V.	Payment gateway for Credit Card Sales	EU	EU
Algolia, Inc.	Search Engine for educational content	US	US
Amazon Web Services, Inc.	Cloud hosting and storage services	US	US
Braintree (PayPal)	Payment gateway for Credit Card Sales	US	US
Customer.io (Peaberry Software Inc.)	Marketing platform (Email Service provider)	US	US
Datadog, Inc.	Monitoring, alerting and logging of all infrastructure and client-facing applications	US	US
Google LLC	Web Analytics Cloud hosting for specific courses Google Workspace for email and general productivity tasks	US	US
Hotjar Ltd.	Usage Analytics via heatmaps	Malta	Ireland
Intercom, Inc.	Tool used for in-application user support	US	US
Microsoft Corporation	Cloud hosting for specific courses	US	US
Salesforce.com, Inc.	Customer Relationship Management for the Commercial Departments	US	US
Snowplow Analytics Limited	Web Analytics	US	US
SVMK Inc. (SurveyMonkey)	User Surveys	US	US
Wootric, Inc.	NPS score tracking	US	US
Zendesk Inc.	Support Ticket Portal for Customer Support	US	US

Zuora Inc.	Subscription Management used for invoicing and payments	US	US
Boldr LLC	Support Services	US	Philippines

Annex C - Technical and Organizational measures

DataCamp is an ISO 27001:2017 certified company, independently audited by Brand Compliance B.V. All of our security policies, measures and safeguards are subject to audit. A copy of the certificate and statement of applicability can be made available on request.

Administrative Safeguards

- All relevant employees have undergone background screening
- All employees, independent contractors and subcontractors are required to execute a confidentiality agreement.
- An asset management policy is in place including a disposal policy.
- Information assets are classified and protected according to their label
- All employees and subcontractors receive security awareness training on the Security Policy in place. Disciplinary action might occur in the event policies are neglected.
- All access to servers and hosting providers are monitored, access logs are retained for up to 6 months and internally audited on a regular basis.
- Employee access to our infrastructure is strictly limited to engineers who require such access in order to maintain the stability and efficiency of our systems. Access is based upon the principle of least privilege and requires the use of two-factor authentication.
- Annual periodic penetration testing by an external party is used to audit application and server security.
- Our organization's development and production environments are fully separated.

Technical Safeguards

- Data is logically separated based on a microservice architecture. All databases and backups are encrypted at rest with AES-256. Additionally, we backup all data on a daily basis with a 30-day retention period.
- All endpoints are centrally managed
    - Automatic device locking
    - Automatic password policy enforcement
    - Automatic software roll-out
    - Remote wiping in case of stolen or damaged equipment
    - Protected with anti-malware software and data loss protection and data is transferred securely
- All communication between users and our application are secured with 128-bit TLS 1.2 encryption and above.
- All account passwords are protected irreversibly. Employees cannot reconstruct passwords in any way or form.
- Security risks and Patch Management are dealt with based on different risk levels. For example, patches for critical, high and medium risk/vulnerabilities shall be patched within 60 calendar days after they are available to users and low risk/vulnerabilities shall be patched within a commercially reasonable time after they are available to users.
- Automatic inspection tools are used to ensure best practices related to authentication, network security, operating systems and application security are adhered to.
- Advanced user-, file- and network-activity anomaly detection monitors our infrastructure
- Our payment processors, Braintree and Adyen, are validated Level 1 PCI DSS Compliant Service Providers. They are part of Visa's Global Compliant Provider List and MasterCard's

SDP List. Additionally, they conduct regular automated vulnerability scans and have extended external penetration testing conducted by outside sources.

Physical safeguards

- All offices require badge-based access to enter. Our NY office has 24/7 security.
- Our user-facing applications are hosted on Amazon Web Services in ISO 27001 certified data centers. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state-of-the-art intrusion detection systems, biometric locks, and other electronic means. Only authorized personnel have access to the data centers.

Annex D

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: the legal entity that is a party to the Agreement with DataCamp, Inc. (the data exporter)

And

Name of the data importing organisation: DataCamp, Inc. and its affiliates
Address: 350 Fifth Avenue, Suite #7720, New York, NY 10118, USA, ATTN: General Counsel
E-mail: privacy@datacamp.com
(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 sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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.
2. 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.
3. The data subject can enforce against the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.
4. 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:

A. 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;
B. 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;

C. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
D. 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;
E. that it will ensure compliance with the security measures;
F. 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;
G. to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
H. 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 sub-processing 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;
I. that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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
J. 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;
B. 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;
C. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
D. that it will promptly notify the data exporter about:
    a. 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;

b. any accidental or unauthorised access; and
c. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

E. 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;
F. 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;
G. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, 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;
H. that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent
I. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
J. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. 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 sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. 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 sub-processor 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 of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
3. 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. 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:
    a. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
    b. to refer the dispute to the courts in the Member State in which the data exporter is established.
2. 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

1. 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.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, 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.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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.

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

Sub-processing

1. 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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing 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.
4. The data exporter shall keep a list of sub-processing 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

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor 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.
2. The data importer and the sub-processor 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 legal entity that entered into the Agreement with DataCamp, Inc. to provide training to individual persons, e.g. employees.

Data importer

DataCamp, Inc. is a provider of online education services on the DataCamp website located at http://www.datacamp.com and a mobile application.

Data subjects

The personal data transferred concern the following categories of data subjects:

- End users of the online education service
- Contacts involved with administering the training, e.g. invoicing contact, group admins

Categories of data

The personal data transferred in relation to the use of DataCamp services may include the following categories of data:

- Personal identifiers: name, email, telephone, avatar
- Electronic identifiers: Device ID, IP address, tracking ID
- Financial data (as applicable): credit card information, billing information and/or transaction information
- Professional data: company name, company domain
- Educational data (if applicable): school name, faculty page, teaching role
- Account information: learning history, exercise submissions

Special categories of data (if appropriate)

Not applicable

Processing operations

The personal data transferred will be subject to the following basic processing activities:
Any processing that is required to perform the purposes for which the data exporter entered into the Agreement with the data importer, as described in the Agreement and the DPA.

Appendix 2

to the Standard Contractual Clauses

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

Data importer will maintain appropriate technical and organizational measures to secure Customer Data designed to protect the security, confidentiality and integrity of Customer Data. The Technical and organizational measures as of the Effective Date are attached to the DPA as **Annex C**.