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 out in the Agreement.

Definitions

"Adequate Jurisdiction" means any jurisdiction that the European Commission has approved as providing an adequate level of protection for Personal Data under the GDPR;
"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.

"**EU Export**" means any transfer of Customer Data from Customer located in the EEA or Switzerland to DataCamp or a DataCamp Affiliate that is not located in the EEA, Switzerland or an Adequate Jurisdiction.

"**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.

"**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.

"**UK Export**" means any transfer of Customer Data from Customer located in the UK to DataCamp or a DataCamp Affiliate that is not located in the UK or an Adequate Jurisdiction.

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 out 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 out 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, including, without limitation, the United States of America. DataCamp will at all times ensure that such transfers are made in compliance with the requirements of Data Protection Law.

   b. Cross Border Transfer Mechanism.
      i. United Kingdom: The provisions of Annex D shall apply to any UK Export.
      ii. EEA and Switzerland: The provisions of Annex E shall apply to any EU Export.
      iii. 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 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 a 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 out 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 out 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 date which is the earlier of (1) Customer's initial access to the Services through any registration or order process; or (2) the effective date of the first Order Form ("**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
Categories of Data Subjects Whose Personal Data is Transferred	● Users ● Account Administrators
Categories of Personal Data Transferred	● Personal identifiers: name, email, telephone, avatar ● Electronic identifiers: Device ID, IP address, tracking ID ● Professional data: company name, company domain ● Educational data (if applicable): school name, faculty page, teaching role ● Account information: learning history, exercise submissions
Sensitive Data Transferred	● Not applicable
Frequency of Transfer	● Continuous basis as long as the online platform located at www.datacamp.com and/or related mobile application is used by Data Exporter
Nature and Purposes of the Processing	● Providing an online platform (located at http://www.datacamp.com) and a mobile application where organizations and individuals can learn data science and analytics skills, collaborate on data analyses, certify data skills and get matched to job opportunities in data science and analytics ● Communicating with users on the DataCamp website or email (including helpdesk)
Period for which the Personal Data will be Retained	● Until deletion of all Customer Data in accordance with the DPA.
Transfers to Sub-processors	● As set out in Annex B

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 out below) to assist DataCamp, Inc. in providing the Services. The duration of the processing by such Sub-processors is on a continuous basis as long as the online platform located at www.datacamp.com and/or related mobile application is used by Customer.

Third Party Sub-processors

Name	Address	Contact person's name, position and contact details	Description of processing:	Entity HQ Location	Data Processing Location
Adyen N.V.	Simon Carmiggeltstraat 6-50, 1011 DJ, The Netherlands	dpo@adyen.com	Payment gateway for Credit Card Sales: Adyen is a payment service provider and as such Adyen provides acquiring services to its customers. Being an acquirer means that Adyen accepts payment on behalf of the relevant merchant and then transfers the funds paid by the shopper to the merchant.	EU	EU
Algolia, Inc.	301 Howard St, 3rd floor, San Francisco, CA 94105 (USA)	privacy@algolia.com	Search Engine for educational content: Algolia subscribers or subscriber's end users electronically submit (or cause to be submitted) data via the Services for hosting, indexing and related processing.	US	US
Amazon Web Services, Inc.	410 Terry Avenue North, Seattle, WA 98109-5210 (USA)	Form on the website Choose Compliance Support	Cloud hosting and data storage services: The gateway services offered by PayPal include services that provide Merchants with the software and connectivity required to allow real-time secure data transmission for processing of credit card and debit card payments and certain other available payment methods on a website or mobile application.	US	US
Braintree (PayPal)	2211 North First Street, San Jose, CA, 95131 (USA)	dpo@paypal.com	Payment gateway for Credit Card Sales	US	US
Customer.io (Peaberry Software Inc.)	921 SW Washington Street Suite 820 Portland, OR 97205 (USA)	privacy@customer.io	Marketing platform (Email Service provider). Customer.io Processes Company Data to provide the Services to Company and to perform Customer.io's obligations under the Agreement (including this DPA) or as	US	US

			otherwise agreed by the parties. Those data Processing activities may include, for example, collecting email addresses of Company's customers, segmenting Company's customers by interest categories, and sending email marketing communications to individuals on Company's behalf		
Datadog, Inc.	620 8TH Ave FL 45, New York, NY, 10018-1741 (USA)	gdpr@datadoghq.com	Monitoring, alerting and logging of all infrastructure and client-facing applications	US	US
Google LLC	1600 Amphitheatre Parkway Mountain View, CA 94043 (USA)	Privacy Help Center	Web Analytics Cloud hosting for specific courses Google Workspace for email and general productivity tasks	US	US
Hotjar Ltd.	Dragonara Business Centre 5th Floor, Dragonara Road, Paceville St Julian's STJ 3141 Malta (Europe)	support@hotjar.com	Usage Analytics via heatmaps	Malta	Ireland
Intercom, Inc.	55 2ND St FL 4 San Francisco, CA, 94105-4560 (USA)	DPO legal@intercom.com	Tool used for in-application user support	US	US
Microsoft Corporation	One Microsoft Way Redmond WA 98052-6399 (USA)	Form on the website	Cloud hosting for specific courses	US	US
Salesforce.com, Inc.	415 Mission Street 3rd Floor San Francisco, CA 94105 (USA)	Form on the website	Customer Relationship Management for the Commercial Departments	US	US
Snowplow Analytics Limited	17 Bevis Marks, Floor 6, London, EC3A 7LN (UK)	info@snowplowanalytics.com	Web Analytics	UK	US
SVMK Inc / Momentive.ia (SurveyMonkey)	1 Curiosity Way, San Mateo, CA 94403 (USA)	Form on the website	User Surveys: to create and send surveys	US	US
Wootric, Inc.	220 27th Street San Francisco, CA 94131(USA)	privacy@inmoment.com	NPS score tracking: Wootric uses customizable Net Promoter Score (NPS) microsurveys in any channel to deliver real-time customer sentiment metrics and qualitative feedback across customer journey touchpoints.	US	US
Zendesk Inc.	1019 Market Street San Francisco, CA 94103 (USA)	privacy@zendesk.com	Support Ticket Portal for Customer Support	US	US
Zuora Inc.	3050 South Delaware Street, Suite 301 San Mateo, CA 94403 (USA)	support@zuora.com	Subscription Management used for invoicing and payments	US	US
Boldr LLC	1210 Pine St, Huntington Beach, CA, 92648-2738 (USA)	support@liveboldr.com	Support Services	US	Philippines

Annex C - Technical and Organizational measures

DataCamp helps organizations and individuals become data literate by building the best platform to learn, collaborate on data analyses, and certify their data skills. In doing so, protecting your data is one of our most important priorities. Accordingly, DataCamp implements reasonable, administrative, technical, and physical safeguards in an effort to secure its facilities, systems and Applications from unauthorized access and to secure the User Content (as defined in the Agreement). “Applications” means the online learning platform, Workspace coding environment, and Certification program at www.datacamp.com, and the related DataCamp mobile application.

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.

DataCamp, as data importer, has implemented the following technical and organizational measures to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons:

Measures of pseudonymization and encryption of personal data - All communication between users and our application are secured with 128-bit TLS 1.2 encryption and above. All databases and backups are encrypted at rest with AES-256. When a user deletes or requests us to delete their user account we replace personal identifiable information with a nil value. After 30 days our daily incremental backups rotate and the information is fully removed from our systems.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services - Data is logically separated based on a microservice architecture. Our organization’s development and production environments are fully separated. All relevant employees have undergone background screening**.** All employees, independent contractors and subcontractors are required to execute a confidentiality agreement. All employees and independent contractors receive security awareness training on the Security Policy in place. Disciplinary action might occur in the event policies are neglected. An asset management policy is in place including a disposal policy. Information assets are classified and protected according to their label. 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. Our networks are protected with multiple layers of controls (firewall, virus scanner, watchful monitoring, etc.).

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident - We backup all data on a daily basis with a 30-day retention period. We have established a Business Continuity Plan to

recover the IT systems at an alternative location in case of a disruptive incident and to provide user access to them.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing - Annual periodic penetration testing by an independent external party is used to audit application and server security. For continuous feedback from the security community a bug bounty program is set up via the Intigriti platform.

Measures for user identification and authorization - All account passwords are protected irreversibly. Employees cannot reconstruct passwords in any way or form. We have set strong password requirements. 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 principles of least privilege, need to know and need to use and it requires the use of two-factor authentication. We ensure on-going management of system access.

Measures for the protection of data during transmission - All communication between users and our application are secured with 128-bit TLS 1.2 encryption and above. The organization-provided electronic messaging facilities must always be used when communicating with others on official business.

Measures for the protection of data during storage - All databases and backups are encrypted at rest with AES-256. 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. We have put in place a Cloud Computing Policy to establish rules for the selection and management of cloud computing services so that data is appropriately protected.

Measures for ensuring physical security of locations at which personal data are processed - Being a geographically distributed company with employees working in home offices or public co-working spaces, DataCamp's information security strategy is to focus on the endpoints and cloud services rather than building bastion locations. However, all our office spaces meet local building regulations and have lockable doors to prevent theft. All offices require badge-based access to enter and our NY office has 24/7 security.

Measures for ensuring events logging - Advanced user-, file- and network-activity anomaly detection monitors our infrastructure. All access to servers and hosting providers are monitored. All endpoints, servers and other equipment (such as network routers and switches) involved in hosting the storage or processing of classified information have the available audit logging facilities activated to allow the recording and monitoring of activities. Log files will be kept for a period of six months and are internally audited on a regular basis.

Measures for ensuring system configuration, including default configuration - 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.

Measures for internal IT and IT security governance and management - Automatic inspection tools are used to ensure best practices related to authentication, network security, operating systems and application security are adhered to.

Measures for certification/assurance of processes and products - For a continued optimal performance of our Information Security Management System, periodic internal audits are performed. The outcome and subsequent corrective actions are reviewed by Senior Management. An annual external audit in light of our ISO 27001:2017 certification ensures independent review of the ISMS.

Measures for ensuring data minimization - We only process data for specific purposes, which is to help you learn, practice, and apply data science skills. DataCamp does not collect any sensitive data, we only collect relevant and necessary data (e.g. name and email address) for these purposes. For more information on what personal data we collect and how we use that data, please see our Privacy Policy.

Measures for ensuring data quality - DataCamp uses the principle of master data, all data is owned and updated by the (micro)service for which the data is relevant. This service will notify other services via an event system that data has been updated, effectively creating a single source of truth. The service is responsible for when data is submitted to validate the data format, content and its correctness in relation to its usage. The data itself is protected through a combination of backups, audit logging and alerting.

Measures for ensuring limited data retention – We have set up a Records Retention and Protection Policy to ensure compliance with all relevant legal, regulatory and contractual requirements in the collection, storage, retrieval and destruction of records.

Measures for ensuring accountability - We have a data register or register of processing activities and we have all the necessary documentation available to demonstrate compliance with the GDPR.

Measures for allowing data portability and ensuring erasure – Users have the right to ask us to retrieve and/or transfer all the personal data we have about them. Users can submit a request via our privacy contact form if they wish to download their data. At any time users can cancel their subscription and delete their data permanently in their account settings. We've also implemented a Records Retention and Protection Policy and execute regular data deletion.

In regards to transfers to (sub-) processors, DataCamp implements a Supplier Due Diligence Assessment Procedure to understand the information security approach and controls the potential supplier has in place before contracting with the company. The information security

requirements of DataCamp are reflected within the written contractual agreement entered into with the supplier.

We choose our processors with care. For example, our payment processors, Braintree and Adyen, are validated Level 1 PCI DSS Compliant Service Providers. We integrated these payment processors in such a manner that DataCamp does not handle any payment data. 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.

Annex D – UK Exports

1. In the event of a UK Export under the Agreement, the Standard Contractual Clauses annexed to European Commission Decision (2010/87/EU) (available here) ("UK SCCs") shall be incorporated into and form part of this DPA.

2. The following information shall apply to the UK SCCs:

Contracting information	
Data Exporter	Customer and relevant authorized affiliates of Customer
Data Exporter Details	As set out in the Agreement
Data Exporter Signatory	As set out in the Agreement
Data Importer	DataCamp, Inc. and relevant DataCamp Affiliates
Data Importer Details	As set out in the Agreement
Data Importer Signatory	As set out in the Agreement
Main body	
Clause 9 (Governing Law)	The law of the member state in which the Data Exporter is established.
Clause 11.3 (Sub-processing Governing Law)	The law of the member state in which the Data Exporter is established.
Illustrative Indemnity Clause	Shall not apply
Appendix 1 (Details of Transfer)	
Data Subjects	As set out in Annex A
Categories of Data	As set out in Annex A
Special Categories of Data	As set out in Annex A

Processing Operations	As set out in Annex A
Appendix 2 (Security Measures)	
Description of the technical and organizational security measures	As set out in Annex C

3. In the event that the EU SCCs are recognized as a valid transfer mechanism for UK Exports, effective as of the date of such recognition, the reference to UK SCCs in paragraph 1 above shall be replaced with reference to the EU SCCs and any additional terms or addendum required in order to validate the EU SCCs shall be deemed incorporated and shall form part of this DPA.

4. To the extent that any additional measures are required to ensure the compliance of UK Exports with relevant Data Protection Law, the Parties shall work together to promptly put in place such measures.

5. In the event of a conflict between (i) the UK SCCs (or, if replaced pursuant to paragraph 3 above, the EU SCCs); and (ii) the terms of this DPA or the Agreement, the terms of the UK SCCs (or, if replaced pursuant to paragraph 3 above, the EU SCCs) shall apply.

Annex E – EU Exports

1. In the event of an EU Export under the Agreement, Module 2 (Controller to Processor) of the Standard Contractual Clauses annexed to European Commission Decision (2021/914/EU) (available here) ("EU SCCs") shall be incorporated into and form part of this DPA.

2. The following information shall apply to the EU SCCs:

Main body	
Clause 7 (Docking Clause)	Shall be deemed incorporated
Clause 9(a) (Use of Sub-processors)	Option 2 shall apply and the time period for prior notice of Sub-processor changes will be as set out in Section 2 (Sub-processing) of this DPA.
Clause 11 (Redress)	The optional language will not apply.
Clause 17 (Governing Law)	Option 1 shall apply and the governing law shall be the law of Belgium.
Clause 18 (Choice of Forum and Jurisdiction)	The courts of Belgium.
Annex I	
A. List of Parties	
Data Exporter	Customer and relevant authorized affiliates of Customer
Data Exporter Details	As set out in the Agreement
Data Exporter Signatory	As set out in the Agreement
Data Exporter Role	Controller
Data Importer	DataCamp, Inc. and relevant DataCamp Affiliates
Data Importer Details	As set out in the Agreement
Data Importer Signatory	As set out in the Agreement

Data Importer Role	Processor
B. Description of transfer	As set out in Annex A
C. Competent Supervisory Authority	Belgian Data Protection Authority
<u>Annex II (Security Measures)</u>	
Description of the technical and organizational security measures	As set out in Annex C
<u>Annex III (List of Sub-processors)</u>	
Authorized Sub-processors	As of the date of this DPA, as set out in Annex B or as amended from time to time in accordance with the notice provisions set forth in Section 2 of this DPA

3. To the extent that any additional measures are required to ensure the compliance of EU Exports with relevant Data Protection Law, the Parties shall work together to promptly put in place such measures.

4. In the event of a conflict between (i) the EU SCCs; and (ii) the terms of this DPA or the Agreement, the terms of the EU SCCs shall apply.