

DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) amends and forms part of the Master Subscription Agreement or other agreement (the “**Agreement**”) between Customer and Absolute governing Absolute’s provision of the Products and Services to Customer. In the event of a conflict between the terms of this DPA and the Agreement, the terms of this DPA will control.

1. **Definitions.** Capitalized terms used but not defined in this DPA will have the meanings given to those terms in the Agreement.
 - 1.1. “**Business**”, “**Business Purpose**”, “**collect**”, “**collected**”, “**collection**”, “**Consumer**”, “**Deidentified Information**”, “**Personal Information**”, “**sale**”, “**selling**”, and “**Service Provider**” have the meaning given to them in the CCPA; and “**sell**” will be interpreted accordingly;
 - 1.2. “**Controller**”, “**Data Subject**”, “**Personal Data**”, “**processing**”, “**Processor**”, and “**Supervisory Authority**” have the meaning given to them in the GDPR, and “**process**”, “**processes**” and “**processed**” will be interpreted accordingly;
 - 1.3. “**Customer Personal Data**” means any Customer Data that constitutes Personal Information or Personal Data that is collected or processed by Absolute as a Service Provider or Processor (as applicable) on behalf of Customer to provide the Products and Services, as further described in Annex I of this DPA;
 - 1.4. “**Data Protection Law**” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations (“**CCPA**”), General Data Protection Regulation (EU) 2016/679 (“**GDPR**”), and e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC), and their national implementations in the European Economic Area (“**EEA**”), the Swiss Federal Data Protection Act, the UK General Data Protection Regulation, and the UK Data Protection Act 2018, each as applicable, and as may be amended or replaced from time to time;
 - 1.5. “**Data Subject Rights**” means Consumers’ or Data Subjects’ rights to information, access, rectification, deletion, erasure, restriction, portability, objection, opt out of sale, not to be discriminated against for exercising certain rights, and not to be subject to automated individual decision-making, in accordance with and each to the extent required by Data Protection Law;
 - 1.6. “**Europe**” means the EEA and Switzerland;
 - 1.7. “**International Data Transfer**” means any transfer of Customer Personal Data from Europe or the United Kingdom to a country outside of Europe and the United Kingdom;
 - 1.8. “**Personal Data Breach**” means any breach of Absolute’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored or otherwise processed by Absolute or its Subprocessors;
 - 1.9. “**Subprocessor**” means a Processor engaged by Absolute to process Customer Personal Data; and
 - 1.10. “**Standard Contractual Clauses**” means the clauses annexed to the EU Commission Decision 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (OJ L 199, 7.6.2021, p. 31-61) as applicable and may be amended or replaced from time to time.
2. **Role of the Parties and Scope of Processing**
 - 2.1. **Scope.** This DPA and each of the provisions and obligations herein apply to the extent Absolute processes Customer Personal Data as a Service Provider or Processor (as applicable).
 - 2.2. **Role of the Parties.** Customer is a Business or Controller and appoints Absolute as a Service Provider or Processor on behalf of Customer. Each Party will collect, retain, use, disclose, and process Customer Personal Data under or in connection with the Products and Services in accordance with applicable Data Protection Law.
 - 2.3. **Customer Responsibilities.** Customer is responsible for compliance with applicable requirements to provide notice to Data Subjects of the use of Absolute as a Processor. The subject matter, nature and purpose of the processing, the types of Customer Personal Data and categories of Data Subjects are set out in **Annex I**.
 - 2.4. **Absolute Responsibilities.** Absolute will process Customer Personal Data to provide the Products and Services in accordance with Customer’s documented lawful instructions, which are deemed given, for the following purposes: (i) processing in accordance with this DPA, the Agreement, and any applicable statement of work; (ii) processing initiated by Authorized Users in their use of the Products and Services; and (iii) processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of this DPA, the Agreement, and any applicable statement of work. Unless prohibited by applicable law, Absolute will inform Customer if it becomes aware that, or in its opinion, Customer’s instructions violate Data Protection Law. For example, if Absolute receives a subpoena or court order from a law enforcement agency, it will inform Customer of the request unless legally prohibited from doing so.
 - 2.5. **Cooperation with Customer Requests.** Absolute will, taking into account the nature of the processing and the information available to Absolute, reasonably assist Customer to (a) respond to requests to exercise Data Subject Rights; (b) conduct data protection impact assessments and prior consultations with Supervisory Authorities; and (c) notify an impacted Data Subject of a Personal Data Breach when required by law. Customer will be responsible for any reasonable costs arising from Absolute’s assistance.
3. **Security and Audits**

- 3.1. **Security Measures.** Absolute will implement technical and organizational measures, appropriate to the risk, to protect Customer Personal Data from unauthorized access, destruction, use, modification, or disclosure, as set out in the Absolute Security Standards referenced in **Annex II**. Absolute may modify the Absolute Security Standards from time to time, but will continue to provide at least the same level of security as is described in the Absolute Security Standards. Absolute will ensure that all personnel authorized to process Customer Personal Data are subject to an obligation of confidentiality.
- 3.2. **Personal Data Breach Response.** Absolute will notify Customer without undue delay after becoming aware of a Personal Data Breach. Absolute will make commercially reasonable efforts to identify the cause of the Personal Data Breach and take those steps as Absolute deems necessary and reasonable in order to remediate the cause of the Personal Data Breach to the extent the remediation is within Absolute's reasonable control. This provision will not apply to Personal Data Breaches that are caused by Customer or Customer's users.
- 3.3. **Audit.** As required by Data Protection Law, Absolute will provide Customer with a summary of Absolute's audit reports, including any information reasonably necessary to demonstrate Absolute's compliance with the obligations of this DPA; provided, that Absolute may redact any confidential or commercially sensitive information in such reports.

4. Subprocessing

- 4.1. **Authorized Subprocessors.** Customer acknowledges and agrees that Absolute may engage Subprocessors. A list of Absolute's current Subprocessors is available at www.absolute.com/company/legal/absolute-sub-processors. Absolute will enter into a written agreement with Subprocessors which imposes on the Subprocessors materially the same obligations as those imposed on Absolute under this DPA.
- 4.2. **Changes to Subprocessors.** Customer acknowledges and agrees that Absolute will notify Customer of any intended addition or replacement of Subprocessors through updating its list of Subprocessors referred to in Section 4.1. Customer may object to the addition or replacement of a Subprocessor within thirty (30) days following Absolute's update of its list of Subprocessors. If Customer's objection is based on reasonable grounds relating to a potential or actual violation of Data Protection Law, then Customer and Absolute will work together in good faith to address Customer's objection.

5. Data Transfers

- 5.1. **International Data Transfers.** Customer agrees that Absolute may perform International Data Transfers: (a) to any country deemed adequate by the EU Commission or the UK government, as applicable, including Canada; (b) on the basis of appropriate safeguards in accordance with Data Protection Law; or (c) pursuant to the Standard Contractual Clauses referred to in Section 5.2 or Section 5.3. If Absolute's compliance with Data Protection Laws applicable to International Data Transfers is affected by circumstances outside of its control, including if a legal instrument for International Data Transfers is invalidated, amended, or replaced, then Customer and Absolute will work together in good faith to reasonably resolve such non-compliance.
- 5.2. **Data Transfers from Europe.** By signing this DPA, Customer and Absolute agree to the terms of MODULE TWO of the Standard Contractual Clauses, which are hereby incorporated into this DPA by reference. The Parties hereby agree that where the Standard Contractual Clauses apply, they shall be completed as follows: (a) the optional Clause 7 is kept; (b) in Clause 9, Option 1 is struck and Option 2 is kept; (c) in Clause 11, the optional language is struck; (d) in Clause 17 and 18, the Governing law and the competent courts are those of Ireland; and (e) Annex I and II to the Standard Contractual Clauses are Annex I and II to this DPA, respectively. If Absolute transfers Customer Personal Data from Europe to a country that does not provide an adequate level of protection as determined by the EU Commission to provide the Products to Customer, then the Standard Contractual Clauses will apply.
- 5.3. **Data Transfers from the UK.** By signing this DPA, Customer and Absolute agree to the terms of MODULE TWO of the Standard Contractual Clauses and Part 2 (Mandatory Clauses) of the International Data Transfer Addendum to the Standard Contractual Clauses, available at: <https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf> (the "**UK Addendum**"), which is hereby incorporated by reference. If Absolute transfers Customer Personal Data from the United Kingdom to a country that does not provide an adequate level of protection as determined by the UK, then the UK Addendum will apply.

6. California Consumer Privacy Act

- 6.1. **Consideration.** Absolute acknowledges that the exchange of Customer Personal Data between Customer and Absolute does not form part of any monetary or valuable consideration exchanged between Customer and Absolute with respect to the Agreement or this DPA.
- 6.2. **Use of Customer Personal Data.** Except as otherwise permitted by applicable law, Absolute will not: (a) retain, use, or disclose Customer Personal Data for any purpose other than performing the Services and providing the Products specified in the Agreement; and (b) sell Customer Personal Data. Notwithstanding any provision to the contrary of the Agreement or this DPA, the terms of this DPA will not apply to Absolute's processing of Customer Personal Data that is exempt from Data Protection Law, including under Cal Civ. Code § 1798.145(a).

7. Termination and Return or Deletion of Customer Personal Data

- 7.1. This DPA is terminated upon the termination of the Agreement. Customer may obtain the return of Customer Personal Data using the features or functionality accessible in Customer's account for the applicable Products, or if no such features or functionality are available, Customer may request the return of Customer Personal Data up to ninety (90) days after termination of the Agreement. Unless required or permitted by applicable law, Absolute will delete or anonymize all remaining copies of Customer Personal Data following termination of the Agreement.

8. Limitation of Liability

- 8.1. Each party's liability arising out of or related to this DPA, including the Standard Contractual Clauses, if applicable, whether in contract, tort or under any other theory of liability, is subject to the Limitation of Liability section of the Agreement.

9. Invalidity and Severability

- 9.1. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

ANNEX I

A. LIST OF PARTIES (MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR)

Data exporter(s): Customer

Customer, as Controller, may elect to transfer data to Absolute in connection with the receipt of Products and Services identified in the applicable Order Form. Customer's name, contact information and signature are set forth in the applicable Order Form or in the Customer's account for the Products and Services.

Data importer(s): Absolute

Absolute, as Processor, processes data received from Customer in connection with the provision of Products and Services identified in the applicable Order Form.

Address: Suite 1400, Four Bentall Centre, 1055 Dunsmuir Street, Vancouver, B.C. Canada, V7X 1K8

Contact: privacy@absolute.com

B. DESCRIPTION OF TRANSFER (MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR)

Categories of Data Subjects whose personal data is transferred in connection with the Products and Services:

#	Category
1	Customer's users of end point devices
2	Customer's administrative personnel responsible for maintenance of Customer's account via the Hosted Service

Categories of Personal Data transferred in connection with the Absolute Services:

#	Category
1	As applicable, end point device information, including computer make and model, computer serial number, system bios version, computer name, OS information, HDD serial number, HDD model, HDD firmware revision, battery device ID, computer UUID, gateway strings, RAM serial number, MAC address, NIC adapter name, IP address, device location, and device usage information.
	Hosted Service account information, including name, contact information and login credentials.

Categories of sensitive data transferred in connection with the Products and Services:

#	Category
1	None.

Frequency and Nature of the Processing:

The data is transferred on a continuous basis. The personal data transferred will be subject to the following processing operations.

- to provide the Products and Services, including storage of data for the Products and Services;
- to resolve technical or administrative issues, billing and invoicing, and otherwise comply with its own legal obligations; and
- to optimize and improve the Products and Services and other business purposes as described in the DPA.

Purpose(s) of the Data Transfer and Further Processing

The purpose of the data transfer is to provide the Products and Services.

Retention Period.

Different data retention periods apply depending on the applicable service. When determining the specific retention period, Absolute considers various factors, such as the type of service provided to the Customer, the nature and length of our relationship with the Customer, and mandatory retention periods provided by law and the statute of limitations.

Transfers to (sub-) processors

The descriptions set forth above in this Section B apply to data transferred to Subprocessors.

C. COMPETENT SUPERVISORY AUTHORITY (MODULE TWO: TRANSFER CONTROLLER TO PROCESSOR)

The competent supervisory authority as defined by Customer.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Domain	Practices
Organization of Information Security	<ul style="list-style-type: none"> • Absolute has a team dedicated to Information Security • The Information Security program is supported by the Absolute executive team • Absolute publishes a management approved information security policy
Human Resources Security	<ul style="list-style-type: none"> • Performs pre-hiring background check on personnel • Performs regular information security training
Physical and Environmental Security	<ul style="list-style-type: none"> • Only authorized users are permitted physical access to customer data processing centers • Uses datacenter and hosting providers with physical and environmental controls
Communications and Operations Management	<ul style="list-style-type: none"> • Encrypt customer data in transit and at rest • Implement network protections including firewalls, VPNs, IDS, and where possible IPS
Access Control	<ul style="list-style-type: none"> • Least principal access to networks and systems • Require MFA for remote access
Information Security Incident Management	<ul style="list-style-type: none"> • Implement a formalized Security and Privacy Incident Response program
Security Operations	<ul style="list-style-type: none"> • Annual penetration testing • Ongoing vulnerability management • Controls to detect and prevent malware • Generate and monitoring event log information
Business Continuity Management	<ul style="list-style-type: none"> • Maintains BCP and DR plans to support continued operations • Tests plans at least annually
Third-party Supplier Management	<ul style="list-style-type: none"> • Maintain a third-party supplier program to review and assess and monitor the security and privacy controls of third-party vendors.
System Development	<ul style="list-style-type: none"> • Provide secure coding training to developers • Implement security testing as a component of the SDLC • Segregated development, testing, and production environments