

## DATA PROCESSING AGREEMENT

between

Omhu A/S  
\_\_\_\_\_  
Silkegade 8 1113 Copenhagen  
Denmark  
\_\_\_\_\_

hereinafter the “**Controller**”

and

**Unbounce Marketing Solutions, Inc.**  
400-401 West Georgia Street  
Vancouver, BC V6B 5A1  
Canada

hereinafter the “**Processor**” or “**Unbounce**”

Controller and Processor hereinafter collectively referred to as the “**Parties**”; each of them as a “**Party**”.

### RECITALS

This Data Processing Agreement (“DPA”) stipulates the legal conditions concerning the Processing of Personal Data by the Processor on behalf of the Controller, in connection with the Services provided by the Processor under the Terms of Service concluded between the Parties.

1. This DPA consists of: The main body of the DPA, Annexes 1, 2, 3 and 4, and Appendices 1 and 2 to Annex 4. All capitalized terms not defined in this DPA shall have the meanings specified in the Terms of Service.
2. This DPA has been pre-signed on behalf of Processor. The Standard Contractual Clauses in Annex 4 have been pre-signed by the Processor as the data importer.
3. To complete this DPA, Controller must:
  - a. Complete the information in the signature box and sign on page 7.
  - b. Complete the information as the data exporter on page 20.
4. Send the completed and signed DPA to Processor by e-mail, to [legal@unbounce.com](mailto:legal@unbounce.com). Upon receipt of the validly completed DPA by Processor at this e-mail-address, this DPA will become legally binding.

## 1. DEFINITIONS

For the purpose of this DPA, the terms listed in this section 1, when used in their capitalized form in this DPA, shall have the meaning set forth below. Unless expressly provided otherwise herein, all capitalized terms not specifically defined in this DPA have the meaning ascribed to them in the Agreement. The meaning shall be the same in both singular and plural form.

<b>Agreement</b>	The Terms of Services entered into between Controller and Processor.
<b>Affiliate</b>	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.
<b>Authorized Affiliate</b>	Any of Controller's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union and (b) is permitted to use the Services pursuant to the Agreement between the Parties, but has not signed up for an Account with the Processor, and is not a "Controller" as defined under the Agreement.
<b>Categories of Data Subjects</b>	Data Subjects who share the same essential characteristics and can be defined by their membership in a particular group or category.
<b>DPA</b>	This Data Processing Agreement.
<b>Controller</b>	The entity that determines the purposes and means of the processing of Personal Data alone or jointly with others (article 4 paragraph 7 GDPR), in this case Controller, acting as data controller, as stated and defined above.
<b>Data Protection Laws and Regulations</b>	Collectively, all laws and regulations applicable to the processing of Personal Data under this Agreement.
<b>Data Subject</b>	Any identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (article 4 paragraph 1 GDPR).
<b>GDPR</b>	The General Data Protection Regulation (Regulation (EU) 2016/679).
<b>Data Processing</b>	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction (article 4 paragraph 2 GDPR).

<b>Personal Data</b>	Any information relating to a Data Subject (article 4 paragraph 1 GDPR).
<b>Personal Data Breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (article 4 paragraph 12 GDPR).
<b>Processor</b>	The entity that processes personal data on behalf of the Controller (article 4 paragraph 8 GDPR), in this case Unbounce Marketing Solutions, Inc., acting as data Processor, as stated and defined above.
<b>Services</b>	All services provided by the Processor to the Controller as specified in the Agreement.
<b>Standard Contractual Clauses</b>	The agreement executed by and between the Parties and attached hereto as Annex 4, pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to Processors established in third countries which do not ensure an adequate level of data protection.
<b>Sub-Processor</b>	Any Processor engaged by the Processor.
<b>Supervisory Authority</b>	An independent public authority which is established by an EU Member State pursuant to the GDPR.
<b>Third Country</b>	State which is not a Member State of either the European Union (EU) or the European Economic Area (EEA) nor Switzerland nor the United Kingdom.
<b>TOMs</b>	Technical and organisational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.
<b>Types of Personal Data</b>	Personal Data that share the same essential characteristics and can be defined by their membership in a particular group or category.
<b>Unbounce Systems</b>	Unbounce data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within Unbounce's control and are used by Unbounce to provide the Services.

## 2. PROCESSING OF PERSONAL DATA

**2.1. Scope, Duration, Object, and Purpose of Processing.** Personal Data will be Processed during the Subscription Period. The objective of the Processing is the provision of the Services. After termination of this DPA the Processor shall, upon request of the Controller, i) **delete** or ii) return to the Controller all Personal Data processed under this DPA, and any copies thereof, unless applicable law requires further storage of the Personal Data (e.g. retention obligations). In the latter case, Processor shall ensure that Data Processing is restricted to that purpose.

Controller hereby instructs Processor to process Personal Data for the following **purposes**: (a) as part of any Processing initiated by the Controller's use and configuration of the Services; (b) Processing to comply with other documented reasonable instructions provided by the Controller (e.g., via e-mail), where such instructions are consistent with the Terms of Service and this DPA; and (c) as otherwise authorized in this DPA.

**2.2. Controller's Rights and Obligations.** The Controller shall have sole **responsibility** for the accuracy, quality, and legality of Personal Data and the means by which Controller acquired Personal Data. For the avoidance of doubt, Controller's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations.

In addition to the instructions concerning Data Processing specified in this DPA, the Controller may **instruct** the Processor as to the manner, scope, and procedure of the Data Processing, namely deletion. Such instructions shall be issued in writing or by e-mail. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes upon applicable data protection law. The Processor shall then be entitled to suspend the execution of the relevant instruction until the Controller confirms or amends it. The Processor is under no obligation to assess the legitimacy of the instructions.

**2.3. Processor's Obligations.** Processor shall, in its use of the Services, process Personal Data in accordance with Data Protection Laws and Regulations, with this DPA and, where applicable, with the instructions of the Controller, exclusively for the purposes stated in this DPA. The Processor may not process Personal Data for any other **purposes** unless required under applicable law; in the latter case, the Processor shall inform the Controller of said legal requirement prior to processing, unless the law in question prohibits the disclosure of such information.

**2.4. Technical and organizational measures.** Processor will implement and maintain TOMs aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing, as set forth in Annex 3 and in Processor's Security Factsheet (the "Factsheet") found at <https://unbounce.com/security/>. Processor agrees to regularly monitor compliance with these measures, and may amend the TOMs from time to time, as needed. Processor will not materially decrease the overall security of the Services during a subscription term, and will take into consideration the severity of risk to the rights and freedoms of Data Subjects.

**2.5. Audit Activities.** Processor shall inform the Controller without undue delay should Processor be subject to an audit or other oversight measure taken by any Supervisory Authority, insofar as such audit or measures relate to the Data Processing occurring under this DPA.

**2.6. Compliance.** Upon Controller's request, and with reasonable prior written notice to Processor, and subject to confidentiality obligations agreed to between the Parties, Processor shall make available to Controller information regarding Processor's compliance with the obligations set forth in this DPA. Controller shall be responsible for the payment of all costs incurred by the Processor related to any such audit. Controller shall promptly notify Processor should any audit reveal possible or actual non-compliance.

**2.7. Categories and Types of Data Subjects.** Controller may solicit Personal Data from Data Subjects, to be Processed by the Processor. The nature of the information collected is determined and controlled by Controller in its sole discretion, and may include, but is not limited to, **Personal Data** relating to customers of Controller, prospective customers of Controller, prospective business partners, prospective employees, prospective students, survey participants, and contest or sweepstakes entrants (who are natural persons).

The Types of Personal Data subject to and Categories of Data Subjects affected by Data Processing will be further detailed in Annex 2.

### 3. RIGHTS OF DATA SUBJECTS

**3.1. Data Subject Requests.** Processor shall, to the extent legally permitted, promptly notify Controller if Processor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). The response to such a request is the sole responsibility of the Controller. The Processor is not liable if the Controller does not comply with the request. Taking into account the nature of the Processing, Processor shall assist Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Controller's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Controller, in its use of the Services, does not have the ability to address a Data Subject Request, Processor shall, upon Controller's request, provide commercially reasonable efforts to assist Controller in responding to such Data Subject Request, to the extent Processor is legally permitted to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Controller shall be responsible for any costs arising from Processor's provision of such assistance.

**3.2. Assistance** Taking into account the nature of the Data Processing and the information available, the Processor shall **assist** the Controller, as far as possible, in fulfilling its **obligations** laid down in the applicable data protection law (e.g. issuing data breach notifications to data protection supervisory authorities and Data Subjects, carrying out data protection impact assessments). In particular, the Processor shall notify the Controller without undue delay after becoming aware of a Personal Data Breach that might affect Personal Data processed on behalf of the Controller under this DPA.

### 4. UNBOUNCE PERSONNEL

**4.1. Confidentiality.** Processor shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. Processor shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

**4.2. Reliability.** Processor shall take commercially reasonable steps to ensure the reliability of any Processor personnel engaged in the Processing of Personal Data.

### 5. SUB-PROCESSORS

**5.1.** Subcontracting for the purpose of this DPA is to be understood as **meaning** services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal/transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Processor shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of Controller's Personal Data, even in the case of outsourced ancillary services.

**5.2.** The Controller hereby acknowledges and agrees that Processor does, and may continue to, engage Sub-Processors in connection with the provision of the Services. Processor shall make available to Controller the current list of Sub-Processors upon written request. Such Sub-Processor lists shall include the identities of those Sub-Processors and their location ("Sub-Processor Lists"). Any

commissioning of additional Sub-Processors requires the prior approval of the Controller, which shall not be refused without reasonable cause. The prior approval of Controller is deemed to be given, if a) Processor has notified the planned commissioning of a new Sub-Processor to the Controller in writing or in text form, b) Controller has not objected to the planned sub-processing in writing or in text form within ten business days upon receipt of the notification, and c) Processor has entered into a data processing agreement in accordance with section 5 paragraph 3 below with the respective Sub-Processor. Processor shall engage only Sub-processors that agree to protect Personal Data to the extent applicable to the nature of the Services provided by such Sub-Processor, but no less than the level of protection afforded by this Agreement.

**5.3.** The Processor shall conclude **corresponding data processing agreements** with Sub-Processors. Such data processing agreements shall afford a level of protection equivalent to this DPA. Controller may, upon written request, evaluate the implementation of Sub-Processor data protection obligations, including, where necessary, by requesting to review any DPAs between the Processor and any applicable Sub-Processor.

**5.4.** If a Sub-Processor intends to provide an agreed-upon service in or from a **Third Country**, the Processor shall ensure the legitimacy of that Third Country transfer of Personal Data pursuant to articles 44 et seq. GDPR.

**5.5.** Where a Sub-Processor fails to fulfill its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the Sub-Processor's obligations.

## **6. SECURITY BREACH NOTIFICATION**

Processor shall notify Controller without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed by the Processor or its Sub-Processors of which the Processor becomes aware (a "Data Incident").

## **7. LIABILITY AND LIMITATION OF LIABILITY**

**7.1.** Each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, generally is subject to the "Disclaimer, Exclusion, and Limitation of Liability" section of the Terms of Service.

**7.2.** For the avoidance of doubt, Processor's and any Affiliates' total liability for all claims from the Controller arising out of or related to the Agreement and DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement.

**7.3.** Additionally for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Annexes and Appendices.

## **8. EUROPEAN SPECIFIC PROVISIONS**

**8.1. GDPR.** Processor will process Personal Data in accordance with the GDPR requirements directly applicable to Processor's provision of its Services.

**8.2. Data Protection Impact Assessment.** Upon Controller's request, Processor shall provide Controller with reasonable cooperation and assistance needed to fulfill Controller's obligation under the GDPR to carry out a data protection impact assessment related to Controller's use of the Services, to the extent Controller does not otherwise have access to the relevant information, and to the extent such information is available to Processor. Processor shall provide reasonable assistance to Controller in the


cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 8.2 of this DPA, to the extent required under the GDPR.

**8.3. Transfer Mechanisms for Data Transfers.** Processor makes available the following transfer mechanism, which shall apply to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom (hereinafter the "EU-EEA Countries") to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations:

- (a). The amendments in Annex 1 of this DPA apply to the application of Data Protection Laws and Regulations applicable outside the EU-EEA Countries (Third Country Data Protection Laws and Regulations).
- (b). The Standard Contractual Clauses set forth in Annex 4 to this DPA apply to the Services.

**9. LEGAL EFFECT**

This DPA shall only become legally binding between Controller and Processor when the formalities laid out in the Section 'Recitals' have been completed.

Controller Signature: 

Print Name: Christian Mulvad Sejersen

Title: CEO

Date: 10 / 13 / 2021

Unbounce Signature: 

Print Name: Carter Gilchrist

Title: President

Date: 11 / 13 / 2019

## Annex 1

### Amendment with Respect to Third Country Data Protection Laws and Regulations

In the event that Unbounce processes personal data of residents of countries outside the EU/EEA countries on behalf of the Controller, Unbounce undertakes to comply with the data protection law applicable there if the relevant law is referred to below and applies locally to this DPA, such as e.g:

- **California Consumer Privacy Act of 2018 (“CCPA”)**, which defines “personal data” as follows in the original text: “PERSONAL DATA” means any information that (i) identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, or (ii) would be considered personal information or personal data as such term/concept is defined by applicable law.

- [...]

(hereinafter jointly referred to as “**Third Country Data Protection Laws and Regulations**”)

In this context, the Parties agree in such a case:

(1) Unbounce acts exclusively as a data processor within the meaning of the relevant Third Country Data Protection Laws and Regulations with regard to personal data of residents of states outside the EU/EEA countries, i.e. residents outside the EU/EEA countries, and the Controller as the data controller within the meaning of the relevant Third Country Data Protection Laws and Regulations.

(2) Unbounce will not sell or transfer to any unauthorized third-party any personal data of persons resident outside the EU-EEA Countries (nor inside) and the Parties acknowledge and agree that the Controller will not sell any such personal data to Unbounce in connection with the Services (as defined by the relevant Third Country Data Protection Laws and Regulations).

(3) For the purpose of complying with the relevant Third Country Data Protection Laws and Regulations, Unbounce confirms that Unbounce

(a). understands and will comply with the requirements and limitations of the relevant Third Country Data Protection Laws and Regulations, and

(b). in relation to all personal data subject to the relevant Third Country Data Protection Laws and Regulations, will not process or sell or pass on the personal data to unauthorised third parties for purposes other than the provision of the Services or outside the direct business relationship between Unbounce and the Controller.

Sub-Processors shall not be deemed to be unauthorised third parties within the meaning of the above provision.



## **Annex 2**

### **Purpose/duration of data processing, types of personal data/categories of data subjects**

Data subjects: Data subjects include the data Controller's representatives and end-users, as determined by the data Controller, and may include, but are not limited to, employees, customers, and prospective customers.

Categories of data: The personal data transferred includes data in electronic form solicited by the Controller via the Services, as determined by the data Controller's use and configuration of the Services.

Processing operations: The personal data transferred will be subject to the following basic processing activities:

- a. Duration and Object of Data Processing. See section 2.1 of the DPA.
- b. Scope and Purpose of Data Processing. See section 2.1 of the DPA.
- c. Personal Data Access. See section 2.1 and 2.2 of the DPA.
- d. Personal Data Deletion or Return. See section 2.1 and 2.2 of the DPA.

## Annex 3

### TOMs – Technical and organizational measures

Processor shall maintain technical and organizational measures to protect the security of Personal Data from accidental or unlawful destruction, loss or alteration or damage, and unauthorized disclosure. Additional information on Processor's security program can be found in the Factsheet.

**1. Information Security Program.** Processor maintains an information security program (including the adoption and enforcement of internal policies and procedures) designed to:

- (a). help Controller secure Personal Data against accidental or unlawful loss, access or disclosure;
- (b). identify reasonably foreseeable and internal risks to security and unauthorized access to the Unbounce Systems; and
- (c). minimize security risks, including through risk assessment and regular testing. Processor shall designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the measures described in this Annex and in the Factsheet, as amended from time to time, as needed.

**2. Network Security.** Unbounce Systems shall be electronically accessible to employees, contractors, and other persons as necessary to provide the Services. Processor shall maintain access controls, user restrictions, and acceptable use policies to manage network access per user. Such measures shall include but not be limited to firewalls and authentication controls. Processor maintains corrective action and incident response plans to respond to potential security threats.

**3. Physical Access Controls.** Physical components of the Unbounce Systems are housed in Unbounce facilities and in Amazon Web Services ("AWS") facilities (the "Facilities"). Where Processor controls access to the Facilities (e.g. Unbounce offices), physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities controlled by Processor requires either electronic access control validation (e.g., card access systems) or validation by human security personnel. Security personnel include security guard services and employees seated at or near a reception desk. Visitors must show appropriate identification and are continually escorted by authorized employees or contractors while visiting Facilities controlled by Processor. Physical security surrounding databases storing Personal Data is under the full control of AWS.

**4. Limited Employee and Contractor Access.** Processor provides access to its Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for such access privileges, the access privileges are promptly revoked.

**5. Physical Security Protections.** All access points to Processor's Facilities (other than main entry doors) are maintained in a secured (locked) state and are monitored by video surveillance cameras designed to record all individuals accessing these Facilities. Processor maintains electronic intrusion detection systems designed to detect unauthorized access to its Facilities. Physical security protections surrounding databases storing Personal Data are under the full control of AWS.

**6. Logical Server Access Control.** Processor's logical servers ("Virtual Machines", or "VMs") are protected by two types of access control: IP whitelisting, and public-key authentication. Processor's

servers accept only incoming network requests from IP addresses that Processor has approved. These IP addresses correspond to the Processor's Vancouver office. Any employee or contractor outside of the Processor's Vancouver office needing to access Processor's logical servers to provide the Services must first use a Virtual Private Network ("VPN") connection to the Processor's Vancouver office, thereby receiving an approved IP address to complete the network connection to Processor's VMs.

Upon successful network connection, the server requires Public Key Infrastructure ("PKI") for authentication. Each employee with access to logical servers has an individual key, and change control is applied to ensure that only approved keys are allowed on VMs.

**7. Physical and Logical Control.** Access to the Processor's databases where Personal Data is stored at rest is restricted to authorized personnel only, limited to those with clear need. Clear need may include but is not limited to: troubleshooting and conducting security or spam investigations on Controller's behalf. Personal Data solicited by Controller is encrypted at rest.

**8. Continued Evaluation.** Processor shall conduct periodic security reviews, as measured against industry security standards and internal policies and procedures. Processor will continually evaluate the security of Processor's systems and Services to determine whether and/or when additional or different security measures are required to respond to new security risks or vulnerabilities.

**Annex 4**  
**The Standard Contractual Clauses (Processors)**

**Transfer of Personal Data to Third Countries**

The following list contains providers in Third Countries who are directly or indirectly involved in the processing of Personal Data covered by this DPA as well as the respective justification pursuant to articles 44 et seq. GDPR.

<b>Name and address of Processor and/or the commissioned subcontractor(s) in Third Country</b>	<b>Justification of Personal Data transfer (e.g. Adequacy Decision of EU Commission, EU Model Contract Clauses, Binding Corporate Rules, EU-US Privacy Shield Certification etc.)</b>
<i>Amazon Web Services</i>	<i>EU Standard Contractual Clauses</i>

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, you (as data exporter) and Unbounce Corporation (as data importer), each a “party,” together “the parties,” have agreed on the following Contractual Clauses (the “Clauses” or “Standard Contractual Clauses”) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

**Clause 1**

**Definitions**

For the purposes of the Clauses:

**(a).** ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

**(b).** ‘the data exporter’ means the controller who transfers the personal data;

**(c).** ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

**(d).** ‘the subprocessor’ means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

**(e).** ‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of

personal data applicable to a data controller in the Member State in which the data exporter is established;

**(f).** ‘technical and organisational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## **Clause 2**

### **Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 below 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 subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

**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 subprocessor 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 subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

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

**(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:

**(i).** any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

**(ii).** any accidental or unauthorised access, and

**(iii).** any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

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

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

**(i).** that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

**(j).** to send promptly a copy of any subprocessor 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 subprocessor 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 subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has

assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities. The provisions in Section 7 of this DPA regarding limitation of liability shall remain unaffected.

**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 subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

## **Clause 7**

### **Mediation and jurisdiction**

**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 subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

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

## **Clause 9**

### **Governing Law**



The Clauses shall be governed by the law of the Member State in which the data exporter is established.

## **Clause 10**

### **Variation of the contract**

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

## **Clause 11**

### **Subprocessing**

**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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

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

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

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

## **Clause 12**

### **Obligation after the termination of personal data processing services**

**1.** The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

**2.** The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

## **Appendix 1 to the Standard Contractual Clauses:**

Data exporter: You are the data exporter. The data exporter is a user of the Services as defined in the Terms of Service.

Data importer: The data importer is **Unbounce Marketing Solutions Inc.** The data importer provides the Services as defined in the Terms of Service.

Data subjects: Data subjects include the data exporter's representatives and end-users, as determined by the data exporter, and may include, but are not limited to, employees, customers, and prospective customers.

Categories of data: The personal data transferred includes data in electronic form solicited by the data exporter via the Services, as determined by the data exporter's use and configuration of the Services.

Processing operations: The personal data transferred will be subject to the following basic processing activities:


- a. Duration and Object of Data Processing. See section 2.1 of the DPA.
- b. Scope and Purpose of Data Processing. See section 2.1 of the DPA.
- c. Personal Data Access. See section 2.1 and 2.2 of the DPA.
- d. Personal Data Deletion or Return. See section 2.1 and 2.2 of the DPA.

**Appendix 2 to the Standard Contractual Clauses**

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

The technical and organizational measures set forth in Annex 3 of the DPA are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Signing the Standard Contractual Clauses, Appendix 1 and Appendix 2 on behalf of the data importer:



Carter Gilchrist, President

Unbounce Marketing Solutions Inc.  
401 West Georgia Street, Suite 400  
Vancouver, BC V6B 5A1

Signing the Standard Contractual Clauses, Appendix 1 and Appendix 2 on behalf of the data exporter:

Controller Signature:   
Print Name: Christian Mulvad Sejersen  
Title: CEO  
Date: 10 / 13 / 2021  
Address: Silkegade 8 1113 Copenhagen  
Denmark

<b>TITLE</b>	Unbounce data processing addendum (DPA)
<b>FILE NAME</b>	191101_English_DPA_-signed.pdf
<b>DOCUMENT ID</b>	d7b1e4614d5e4750da662cdfd48c191453b535bf
<b>AUDIT TRAIL DATE FORMAT</b>	MM / DD / YYYY
<b>STATUS</b>	● Completed

---

## Document History



SENT

**10 / 12 / 2021**

22:21:26 UTC

Sent for signature to Christian Mulvad Sejersen  
 (christian.sejersen@omhu.com) from legal@unbounce.com  
 IP: 3.236.58.2



VIEWED

**10 / 12 / 2021**

22:32:23 UTC

Viewed by Christian Mulvad Sejersen  
 (christian.sejersen@omhu.com)  
 IP: 80.197.253.178



SIGNED

**10 / 12 / 2021**

22:33:47 UTC

Signed by Christian Mulvad Sejersen  
 (christian.sejersen@omhu.com)  
 IP: 80.197.253.178



COMPLETED

**10 / 12 / 2021**

22:33:47 UTC

The document has been completed.