

## **DATA PROCESSING AGREEMENT** **(Revised May 2022)**

This Data Processing Agreement (“**DPA**”) forms a part of the Customer Terms of Service found at <https://pandadoc.com/terms-of-service> or other written agreement between PandaDoc, Inc. and Customer for the purchase and/or use of PandaDoc, Inc.’s and/or its Affiliates (collectively, “**PandaDoc**”) products and/or services (the “**Agreement**”), and reflects the parties mutual understanding and agreement related to the Processing of Customer’s Personal Data (as defined herein) by PandaDoc on behalf of Customer.

By signing the DPA, Customer enters into this DPA on behalf of itself and, to the extent required under Applicable Privacy and Data Protection Laws, in the name and on behalf of its Controller Affiliates (defined below). For the purposes of this DPA only, and except where indicated otherwise, the term “Customer” shall include Customer and Controller Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In the event of inconsistencies between any provision of this DPA and any provision of the Agreement, the provisions of this DPA shall prevail. In the event of conflict between the Standard Contractual Clauses (SCCs) in Exhibit 2 and this DPA, the SCCs shall prevail.

### **HOW THIS DPA APPLIES TO CUSTOMER AND ITS AFFILIATES**

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In such case, the PandaDoc entity that is party to the Agreement with Customer is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with PandaDoc or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, this DPA shall be deemed to be an addendum to such Order Form and applicable renewal Order Forms, and the PandaDoc entity that is party to such Order Form is party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor an Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

If the Customer entity is signing this DPA is neither a party to an Order Form nor an Agreement directly with PandaDoc, but is instead a Customer indirectly via an authorized reseller of PandaDoc’s products and/or services, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller to discuss whether any amendments to its agreement with the reseller are necessary.

### **1. DEFINITIONS**

“**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 of or authority to direct more than 50% of the voting interests of the subject entity.

“**Applicable Privacy and Data Protection Laws**” means all applicable privacy and data protection laws and regulations, including laws and binding regulations that apply to the Processing of Personal Data under the Agreement, or to the privacy of electronic communications, including, to the extent applicable, (i) the General Data Protection Regulation (EU) 2016/679 (“GDPR”), the EU e-Privacy Directive (Directive 2002/58/EC), (ii) in respect of the United Kingdom the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom’s European Union (Withdrawal) Act 2018 (the “UK GDPR”), (iii) the State laws of California, Colorado, Virginia, Utah, Connecticut and any other U.S. states that are applicable to the Processing of Personal Data, and (iv) the Swiss Federal Data Protection Act (“Swiss Data Protection Act”), and any legislation or regulations implementing, replacing, amending or made pursuant to such laws (in each case as may be amended or superseded from time to time).

“**Controller**” shall have the meanings given to them under Applicable Privacy and Data Protection Laws.

**“Controller Affiliate”** means any of Customer's Affiliate(s) (i) that are subject to Applicable Privacy and Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (ii) permitted to use PandaDoc's products and/or services pursuant to the Agreement between Customer and PandaDoc, but have not signed their own Order Form and are not a “Customer” as defined under the Agreement.

**“Customer Data”** means (unless otherwise defined in the Agreement in which case the definition in the Agreement shall apply), all data and information provided by Customer, its Affiliates and its customers to PandaDoc in relation to PandaDoc's provision of the products and/or services including without limitation message text, files, comments, links and profile information. “Customer Data” does not include non-PandaDoc products and/or services.

**“Data Subject”** means the identified or identifiable person to whom Personal Data relates.

**“EEA”** means the European Economic Area.

**“Personal Data”** means any information that relates to an identified or identifiable natural person or to an identified or identifiable legal entity, to the extent that such information is protected as personal data or personally identifiable information under Applicable Privacy and Data Protection Laws and such data submitted is Customer Data. “Personal Data” as used herein only applies to Personal Data for which PandaDoc is a Processor.

**“Process”** or **“Processing”** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

**“Processor”** shall have the meanings given to them under Applicable Privacy and Applicable Privacy and Data Protection Laws.

**“PandaDoc Inc.”** means PandaDoc, Inc., a corporation incorporated in Delaware.

**“PandaDoc”** means, collectively, PandaDoc Inc. and its Affiliates engaged in the Processing of Personal Data.

**“Restricted Transfer”** means: (i) where the GDPR applies, a transfer of Personal Data originating from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of Personal Data originating from the United Kingdom to any other country which is not subject to adequacy regulations adopted pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) where the Swiss Data Protection Act applies, a transfer of Personal Data originating from Switzerland to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner.

**“Security Practices”** means PandaDoc's “Security Practices Datasheet”, as updated from time to time, and currently accessible at Exhibit 1.

**“Standard Contractual Clauses”** or **“SCCs”** (i) where the GDPR applies, the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 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 European Council, (the **“EU SCCs”**) and which are hereby incorporated into this DPA; (ii) where the UK GDPR applies, the International Transfer Addendum or Addendum to the EU SCCs for international data transfers issued under Section 119A of the Data Protection Act 2018 and approved by UK Parliament on 21 March 2022 (**“International Data Transfer Addendum”**) and which is hereby incorporated into this DPA; and (iii) where the Swiss Data Protection Act applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (the **“Swiss SCCs”**) For the

purposes of the EU SCCs and the International Transfer Addendum, if applicable, attached and incorporated in Exhibit 2 herein, (a) Customer shall be the 'data exporter and PandaDoc the 'data importer;' (b) Exhibit 2 incorporates the parties' selection of module 2 (controller – processor data transfer) into the EU SCCs; and (c) the parties agree that Exhibit 2, including its Appendix and attendant annexes as drafted and attached below are the SCCs for purposes of this DPA.

**“Sub-processor”** means any entity engaged by PandaDoc and/or its Affiliates to Process Personal Data in connection with PandaDoc’s products and/or services.

**“Supervisory Authority”** means an independent public authority which is established by an EU Member State pursuant to the GDPR for the EU; the Information Commissioner’s Office (‘ICO’) in the United Kingdom; or the Federal Data Protection and Information Commissioner (FDPIIC) in Switzerland

## **2. PROCESSING OF PERSONAL DATA**

**2.1. Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and PandaDoc is the Processor. PandaDoc may engage Sub-processors pursuant to the requirements set forth in Article 4 “Sub-processors” below to Process such Personal Data.

**2.2. Customer’s Processing of Personal Data.** Customer shall have sole responsibility for the accuracy and quality of Personal Data, the means by which Customer acquired such Personal Data and ensure compliance with laws as it relates to the foregoing. Customer acknowledges that it is responsible for properly implementing access and use controls and configuring certain features and functionalities that Customer may elect to use and that it will do so in such manner that Customer deems adequate to maintain appropriate security, protection, deletion, and backup of Personal Data. PandaDoc will be entitled to rely solely on Customer’s instructions relating to Personal Data Processed by PandaDoc.

**2.3. PandaDoc’s Processing of Personal Data.** With respect to Personal Data Processed by PandaDoc as Customer’s Processor, PandaDoc shall only Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by authorized users in their use of PandaDoc’s products and/or services; and (iii) Processing to comply with other reasonable instructions provided by Customer in writing (e.g., via email or support tickets) that are consistent with the terms of the Agreement (individually and collectively, the **“Purpose”**). PandaDoc shall not disclose Personal Data to third parties except: (i) to employees, service providers, or advisers who have a need to know the Personal Data and are under confidentiality obligations at least as restrictive as those described under this DPA, or (ii) as required to comply with valid legal process in accordance with the terms of the Agreement. If PandaDoc has reason to believe Customer’s instructions infringe the GDPR, UK GDPR or other EEA data protection provisions, then PandaDoc will promptly notify Customer. Customer acknowledges and agrees that PandaDoc collects cumulative, anonymized data and analytics pertaining to its customers including without limitation Customer (“Unidentifiable Data”), and, provided that such Unidentifiable Data Subject is and will remain unidentifiable, the data is not subject to the deletion requirement set forth in Paragraph 7 (“Return and Deletion of Client Data”) herein.

**2.4. Details of the Processing.** PandaDoc agrees that it will Process the Personal Data in relation to the Purpose and the provision of PandaDoc’s products and/or services. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in the Appendix attached hereto and incorporated herein.

## **3. RIGHTS OF DATA SUBJECTS & DATA SUBJECT REQUESTS**

**3.1.** PandaDoc shall, to the extent legally permitted, promptly notify Customer if PandaDoc receives any requests from a Data Subject to exercise the following Data Subject rights: access, rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, objection to the Processing, or to not be subject to an automated individual decision making (each, a **“Data Subject Request”**). Taking into account the nature of the Processing, PandaDoc shall assist Customer by

appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Applicable Privacy and Data Protection Laws. In addition, to the extent Customer, in its use of PandaDoc's products and/or services, does not have the ability to address a Data Subject Request, PandaDoc shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent PandaDoc is legally permitted to do so and the response to such Data Subject Request is required under Applicable Privacy and Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from PandaDoc's provision of such assistance, including without limitation any fees associated with provision of additional functionality.

#### **4. SUB-PROCESSORS**

**4.1. Appointment of Sub-processors.** Customer acknowledges and agrees that (a) PandaDoc's Affiliates may be retained as Sub-processors; and (b) PandaDoc and PandaDoc's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the products and/or services. As a condition to permitting a third-party Sub-processor to Process Personal Data, PandaDoc or a PandaDoc Affiliate will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-processor. Customer acknowledges that PandaDoc, Inc. is located in the United States and provides PandaDoc's products and/or services to Customer. Customer agrees to enter into the SCCs set out in Exhibit 2 attached hereto and acknowledges that Sub-processors may be appointed by PandaDoc in accordance with Clause 9 of Exhibit 2 attached hereto.

**4.2. List of Current Sub-processors and Notification of New Sub-processors.** The then-current list of Sub-processors PandaDoc uses to provide the products and/or services, including the identities of those Sub-processors and their country of location, is accessible at <http://www.pandadoc.com/GDPR/subprocessors> ("**Sub-processor List**") which may be updated by PandaDoc from time to time, but not less than annually when applicable, upon advance written notice to Customer.

**4.3. Objection Right for New Sub-processors.** Customer may reasonably object to PandaDoc's use of a new Sub-processor (e.g., if making Personal Data available to the Sub-processor may violate Applicable Privacy and Data Protection Laws or weaken the protections for such Personal Data) by notifying PandaDoc promptly in writing within 30 business days after Customer becomes aware of such change. Such notice shall include the date the Customer became aware of the new Sub-processor and explain the reasonable grounds for the objection. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, PandaDoc will use commercially reasonable efforts to make available to Customer a change in PandaDoc's products and/or services or recommend a commercially reasonable change to Customer's configuration or use of PandaDoc's products and/or services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If PandaDoc is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days from the date PandaDoc receives written notice from Customer, either party may terminate without penalty the applicable Order Form(s) with respect only to those PandaDoc's products and/or services which cannot be provided by PandaDoc without the use of the objected-to new Sub-processor by providing written notice to the other party advising of such termination. PandaDoc will refund to Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated PandaDoc products and/or services, without imposing a penalty for such termination on Customer.

**4.4. Liability.** PandaDoc shall be liable for the acts and omissions of its Sub-processors to the same extent PandaDoc would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

#### **5. SECURITY**

**5.1. Controls for the Protection of Customer Data.** PandaDoc shall maintain appropriate technical

and organizational measures for protection of the security, confidentiality and integrity of Customer Data, as set forth in the Security Practices located at [pandadoc.com/security](https://pandadoc.com/security).

**5.2. Third-Party Certifications and Audits.** PandaDoc has obtained the third-party certifications and audits set forth in the Security Practices. Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, PandaDoc shall make available to Customer (or Customer's independent, third-party auditor) information regarding PandaDoc's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Security Practices. Customer may contact PandaDoc in accordance with the "Notices" Section of the Agreement to request an audit of PandaDoc's procedures relevant to the protection of Personal Data, but only to the extent required under Applicable Privacy and Data Protection Laws and Customer shall not disrupt PandaDoc's business operations during the performance of such audit. Customer shall reimburse PandaDoc for any time expended for any such audit at PandaDoc's then-current rates. Before the commencement of any such audit, Customer and PandaDoc shall mutually agree upon the scope, timing, and duration of the audit, in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by PandaDoc. Customer shall promptly notify PandaDoc with information regarding any non-compliance discovered during the course of an audit, and PandaDoc shall use commercially reasonable efforts to address any confirmed non-compliance.

## **6. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION**

PandaDoc shall maintain commercially reasonable security incident management policies and procedures specified in the Security Practices. PandaDoc shall notify Customer without undue delay of any breach relating to Personal Data (within the meaning of Applicable Privacy and Data Protection Laws ) of which PandaDoc becomes aware and which may require a notification to be made to a Supervisory Authority or Data Subject under Applicable Privacy and Data Protection Laws or which PandaDoc is required to notify to Customer under Applicable Privacy and Data Protection Laws (a "**Customer Data Incident**"). Taking into account the nature of Processing and the information available to PandaDoc and in accordance with the Agreement, PandaDoc shall provide commercially reasonable cooperation and assistance in identifying the cause of such Customer Data Incident and take commercially reasonable steps to remediate the cause to the extent the remediation is within PandaDoc's control. The obligations herein shall not apply to incidents that are caused by Customer, Customer's authorized users and/or any non-PandaDoc products and/or services.

## **7. RETURN AND DELETION OF CUSTOMER DATA**

Upon termination of the Agreement and/or Order Form pursuant to which PandaDoc is Processing Personal Data, PandaDoc shall, upon Customer's request, and subject to the limitations described in the Agreement and the Security Practices, return all Customer Data and copies of such data to Customer or securely destroy them and reasonably demonstrate to the Customer that it has taken such measures, unless applicable law prevents it from returning or destroying all or part of Customer Data. PandaDoc agrees to preserve the confidentiality of any retained Customer Data for the duration of the Agreement and only and will only actively Process such Customer Data after such date if agreed to by the parties or to otherwise comply with laws. This Section 7 shall not apply to Unidentifiable Data, as defined herein.

## **8. CONTROLLER AFFILIATES**

**8.1. Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement and/or Order Form and this DPA, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Controller Affiliates, thereby establishing a separate DPA between PandaDoc and each such Controller Affiliate subject to the provisions of the Agreement. Each Controller Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, a Controller Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the PandaDoc products and/or services by Controller Affiliates must comply with the terms and

conditions of the Agreement and any violation of the terms and conditions of the Agreement by a Controller Affiliate shall be deemed a violation by Customer and Customer shall be liable for such violation.

**8.2. Communication.** The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with PandaDoc under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Controller Affiliates.

**8.3. Rights of Controller Affiliates.** If a Controller Affiliate becomes a party to the DPA with PandaDoc, it shall, to the extent required under Applicable Privacy and Data Protection Laws, also be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

**8.3.1.** Except where Applicable Privacy and Data Protection Laws require the Controller Affiliate to exercise a right or seek any remedy under this DPA against PandaDoc directly by itself, the parties agree that (i) solely the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Controller Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Controller Affiliate individually but in a combined manner for all of its Controller Affiliates together (as set forth, for example, in Section 8.3.2, below).

**8.3.2.** The parties agree that the Customer that is the contracting party to the Agreement shall, if carrying out an audit of the PandaDoc procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on PandaDoc by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Controller Affiliates in one single audit.

## **9. PANDADOC PERSONNEL**

**9.1. Confidentiality.** PandaDoc shall use commercially reasonable efforts to 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. PandaDoc shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

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

**9.3. Limitation of Access.** PandaDoc shall ensure that PandaDoc's access to Personal Data is limited to those personnel performing services in accordance with the Agreement.

**9.4. Data Protection Officer/Responsible Party.** PandaDoc has a data protection officer or individual responsible for its data protection in the United States, EU and UK that are collectively reached at [privacyteam@pandadoc.com](mailto:privacyteam@pandadoc.com).

## **10. LIMITATION OF LIABILITY**

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Controller Affiliates and PandaDoc, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, the total liability of PandaDoc (and its Affiliates, if any) for all claims from the Customer and all of its Controller Affiliates arising out of and/or related to the Agreement and each DPA shall apply in the aggregate for all claims under the Agreement and all DPAs established under the Agreement, including by Customer and all Controller Affiliates. It is specifically understood that liability shall not apply individually and severally to Customer and to Controller Affiliates.

**11.** PandaDoc will Process Personal Data in accordance with the Applicable Privacy and Data Protection Laws requirements directly applicable to the provisioning of PandaDoc's products and services.

**11.1. Data Protection Impact Assessment.** Upon Customer's request, PandaDoc shall provide Customer with reasonable cooperation and assistance (at Customer's expense) needed to fulfill Customer's obligation under the GDPR to carry out a data protection impact assessment related to Customer's use of PandaDoc's products and/or services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to PandaDoc. PandaDoc shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority, to the extent required under the GDPR.

**11.2. Transfer Mechanisms.**

**11.2.1.** For transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, to countries which do not ensure an adequate level of data protection within the meaning of Applicable Privacy and Data Protection Laws of the foregoing territories, to the extent such transfers are subject to such Applicable Privacy and Data Protection Laws, the EU SCCs and Additional Terms for EU Personal Data Transfers set forth in Exhibits 1 and 2 (including all annexes and appendix) respectively, apply as attached and incorporated herein.

**11.2.2.** For transfers of Personal Data under this DPA from the United Kingdom, to countries which do not ensure an adequate level of data protection within the meaning of Applicable Privacy and Data Protection Laws of the foregoing territory, to the extent such transfers are subject to such Applicable Privacy and Data Protection Laws, the (i) the EU SCCs and Additional Terms for EU Personal Data Transfers set forth in Exhibits 1 and 2 (including all annexes and appendix) respectively and (ii) the International Data Transfer Addendum apply as attached and incorporated herein.

**11.2.3.** For transfers of Personal Data under this DPA protected by the Swiss Data Protection Act, to countries which do not ensure an adequate level of data protection within the meaning of Applicable Privacy and Data Protection Laws of the foregoing territory, to the extent such transfers are subject to such Applicable Privacy and Data Protection Laws, the EU SCCs will also apply to such transfers as attached and incorporated herein, with the following modifications:

- i. any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss Data Protection Act;
- ii. references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; and
- iii. references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the FDIPC and competent courts in Switzerland,
- iv. unless the EU SCCs as implemented above cannot be used to lawfully transfer such Personal Data in compliance with the FPDIC, in which event the Swiss SCCs shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the Swiss SCCs shall be populated using the information contained in Exhibits 1,2, 3 and 4 of this DPA (as applicable).

**12. LEGAL EFFECT**

This DPA shall only become legally binding between Customer and PandaDoc (and PandaDoc, Inc., if different) when executed by both parties. If Customer has previously executed a data processing addendum with PandaDoc concerning the subject matter hereof, the parties acknowledge and agree that this DPA supersedes and replaces such prior data processing addendum. For purposes of clarification, this DPA becomes legally binding on the date the last party below executes the DPA.

**13. VENUE**

This DPA and any dispute or claim arising out of and/or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by, and construed in

accordance with, the legal system of Ireland.

**14. MISCELLANEOUS**

The parties agree that this DPA and, if applicable, the Standard Contractual Clauses, shall terminate automatically upon (i) termination of the Agreement; or (ii) if applicable, the expiration or termination of all Order Forms or similar contract documents entered into by PandaDoc with Customer pursuant to the Agreement, whichever is later. Any obligation imposed on either party under this DPA in relation to the Processing of Personal Data that would reasonably be interpreted to survive any termination or expiration of this DPA, shall survive. Customer may notify PandaDoc in writing from time to time of any variations to this DPA which are required as a result of a change in Applicable Privacy and Data Protection Laws . Any such required variations shall take effect on the date falling 45 (forty-five) calendar days after the date such written notice is received and PandaDoc shall procure that, where necessary, the terms in each contract between PandaDoc or any PandaDoc Affiliate and each Sub-processor are amended to incorporate such variations within the same time period. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

**List of Exhibit(s) attached and incorporated:**

- Exhibit 1: Technical and Organizational Measures
- Exhibit 2: Data Transfer Impact Assessment with Appendix
- Exhibit 3: Additional Safeguards for Personal Data Stored in the United States
- Exhibit 4: Standard Contractual Clauses with Annexes
- Exhibit 5: UK International Data Transfer Addendum \*\*\* only applicable to UK Customers.

The parties' authorized signatories have executed this DPA as set forth below. The agreement begins on the date the Customer signs.

**On behalf of Customer:**

Print Name: \_\_\_\_\_

Position: \_\_\_\_\_

Address:

Signature: \_\_\_\_\_


Date: \_\_\_\_\_

**On behalf of PandaDoc, Inc.:**

Print Name: Kelley Boland

Position: Director of Legal and Compliance, Senior Legal Counsel.

Address: 3739 Balboa St. #1083, San Francisco, CA 94121

Signature:  \_\_\_\_\_

Date: 06 / 01 / 2022



**EXHIBIT 1 TO THE DATA PROCESSING AGREEMENT**  
**TECHNICAL AND ORGANIZATIONAL MEASURES**

This Exhibit 1 forms part of the Agreement. Capitalized terms not defined in this Exhibit 1 have the meaning set forth in the Agreement.

PandaDoc shall implement and maintain commercially reasonable administrative, technical, and physical safeguards designed to protect Customer Personal Data. Such safeguards shall include:

- IT Security Policy. PandaDoc will maintain a written information security policy applicable to all authorized personnel and systems.
- Training. PandaDoc will provide information security awareness training to all employees at least annually.
- Access Control. PandaDoc will maintain an access control policy, procedures, and controls consistent with industry standard practices. PandaDoc will limit access to Customer's Personal Data to those employees and Sub-processors with a need-to-know.
- Logical Separation. PandaDoc will ensure Customer's Personal Data is logically separated from other PandaDoc customer data.
- Networking. PandaDoc will ensure network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the systems and applications infrastructure.
- Encryption. Where appropriate, Customer's Personal Data will be encrypted in-transit and at rest using industry standard encryption technologies.
- Asset Inventory. PandaDoc will maintain an inventory of all information technology assets used in its operation of the services. .
- Password Management. PandaDoc will maintain a password management policy designed to ensure strong passwords consistent with industry standard practices.
- Incident Response Plan. PandaDoc will maintain an incident response plan that addresses Security Incident handling.
- Backups of Customer Personal Data. PandaDoc will maintain an industry standard backup system and backup of Customer's Personal Data designed to facilitate timely recovery in the event of a service interruption.
- Disaster Recovery and Business Continuity Plans. PandaDoc will maintain disaster recovery and business continuity plans consistent with industry standard practices.
- Malicious Code Protection. All PandaDoc workstations will run the current version of industry standard anti-virus software with the most recent updates available on each workstation. Virus definitions will be updated within a reasonable period following release by the anti-virus software vendor.
- Vendor Management. PandaDoc will maintain the Third Party/Vendor Management Program and oversee the risk and compliance program for vendors, partners and other third parties by assessing and managing the risks assumed by the nature of relationships with vendors, partners and other third parties. Vulnerability Management Controls. PandaDoc will maintain a vulnerability management program to identify and resolve security vulnerabilities in a timely manner.

**Additional Safeguarding Measures**

- PandaDoc conducts periodic reviews of our security policies and practices through independent third-party auditing services. Reporting on Controls at a Service Organisation (SOC 2) Audits, as well as internal auditing services and other assessments deemed appropriate.
- PandaDoc maintains annual penetration tests to identify and resolve foreseeable attack vectors and potential abuse scenarios.

**EXHIBIT 2 TO THE DATA PROCESSING AGREEMENT**  
**DATA TRANSFER IMPACT ASSEMENT**

This Exhibit 2 forms part of the Agreement. Capitalized terms not defined in this Exhibit 2 have the meaning set forth in the Agreement.

- **Requirements for Transfers of Personal Data Outside the EEA, Switzerland, and/or the UK.** As a general rule, transfers of personal data which originate in the EEA, Switzerland, and/or the UK to a country that has not been found to provide an “adequate” level of protection (each a “**Third Country**”) are only permitted where such transfers are supported by “appropriate safeguards.” The most common “appropriate safeguards” used by companies to support the transfer of EEA, Swiss, and/or UK personal data to Third Countries are the [EU Standard Contractual Clauses; the UK International Data Transfer Agreement or Addendum; or the EU Standard Contractual Clauses amended as applicable to the Swiss Federal Data Protection Act.](#)
- **Data Transfer Impact Assessments and Related European Data Protection Board (“EDPB”) Guidance.**
  - **Data Transfer Impact Assessments:** Following the decision of the Court of Justice of the European Union in the Case C-311/18: Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems (“Schrems II”), data exporters and data importers are also required to carry out an assessment of each Third Country’s laws and/or practices in force that “may impinge on the effectiveness of the appropriate safeguards of the transfer tools (the data exporter is) relying on, in the context of (the data exporter’s) specific transfer” of personal data to the Third Country.<sup>1</sup>
  - **Related EDPB Guidance:** However, under the EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 (“**EDPB Recommendations on Supplementary Measures**”), *even if the data transfer impact assessment reveals the Third Country’s legislation is “problematic,”<sup>2</sup> then the parties may still proceed with the transfer of personal data to the Third Country if the parties are able to demonstrate and document that they have no reason to believe that the Third Country’s problematic laws (if any) will be interpreted and/or applied in practice so as to cover the parties’ transfer of personal data to the Third Country.*<sup>3</sup>
  - **EU Standard Contractual Clauses:** Clause 14 requires that for all transfers of personal data (regardless of whether they originate from, or are received by, a controller or processor) the parties must warrant that they have “no reason to believe the laws and practices in the third country of destination applicable to the processing of personal data by the data importer . . . prevent the data importer from fulfilling its obligations under these Clauses.”<sup>4</sup> The data importer specifically warrants that it has “made its best efforts to provide the data exporter with the relevant information” to complete the assessment,<sup>5</sup> and the Parties jointly agree to “document the assessment . . . and make it available to the competent supervisory authority on request.”<sup>6</sup>
- **Problematic Legislation in the United States – EO 12333 and FISA Section 702.** On the record before it in Schrems II, the CJEU considered Executive Order 12333 and FISA Section 702 to be “problematic legislation.”

<sup>1</sup> European Data Protection Board, EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0, June 18, 2021, (hereinafter EDPB Recommendations on Supplementary Measures), at 14, available at [https://edpb.europa.eu/system/files/2021-06/edpb\\_recommendations\\_202001vo.2.0\\_supplementarymeasures-transfer-tools\\_en.pdf](https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasures-transfer-tools_en.pdf).

<sup>2</sup> “Problematic legislation” is understood as legislation that 1) imposes on the recipient of personal data from the European Union obligations and/or affect the data transferred in a manner that may impinge on the transfer tools’ contractual guarantee of an essentially equivalent level of protection and 2) does not respect the essence of the fundamental rights and freedoms recognized by the EU Charter of Fundamental Rights or exceeds what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognized in Union or EU Member States’ law, such as those listed in Article 23 (1) GDPR.

<sup>3</sup> EDPB Recommendations on Supplementary Measures at 17 – 18.

<sup>4</sup> EU (New) Standard Contractual Clauses (all Modules) Clause 14(a).

<sup>5</sup> EU (New) Standard Contractual Clauses (all Modules) Clause 14(c).

<sup>6</sup> EU (New) Standard Contractual Clauses (all Modules) Clause 14(d).

- **Data Transfer Impact Assessment Summary – EO 12333 and FISA Section 702 Likely Do Not Apply.** *The processing that PandaDoc (and its subprocessors) engage in under the agreement is likely not subject to Executive Order 12333 or FISA Section 702. As a result, transfers to PandaDoc and its subprocessors in the United States are likely permitted pursuant to the EDPB Recommendations on Supplementary Measures.*<sup>7</sup>
- **Executive Order 12333 Likely Does Not Apply.** Executive Order 12333 governs how United States' intelligence agencies carry out surveillance outside the United States with respect to non-U.S. persons to whom the United States Constitution and laws do not apply. Executive Order 12333 likely has limited to no relevance to transfers of EEA, Swiss, or UK personal data to the United States as it generally applies to surveillance activities that are conducted wholly outside of the United States. Accordingly, it's unlikely that Executive Order 12333 would apply to transfers of personal data to PandaDoc or its subprocessors to or within the United States.
- **FISA Section 702 Likely Does Not Apply.** FISA Section 702 (codified at 50 U.S.C. § 1881a) permits the United States government to conduct certain surveillance of non-US persons located outside of the United States through compelled assistance of electronic communication service providers. Surveillance under FISA Section 702 is restricted to specific areas of national defense, national security, and the conduct of foreign affairs, with an emphasis on international terrorism, sabotage, the proliferation of weapons of mass destruction, and other grave hostile acts.
  - **FISA Section 702's Limited Scope – Only Foreign Intelligence Information.** In specific, FISA Section 702 only permits targeting of individuals where a significant purpose is to obtain "foreign intelligence information."

When acquired from a non-U.S. person, "foreign intelligence information" can generally be thought of as information which relates to the United States' foreign affairs with or national defense against a "foreign power" or "foreign territory" or the United States' ability to protect against serious attacks of a "foreign power." The full definition of "foreign intelligence information" can be found in **Addendum A to this TIA**.
  - **PandaDoc Likely Will Not Process Foreign Intelligence Information.** The transfers of EEA, Swiss, and UK personal data to PandaDoc and its subprocessors in the United States will primarily consist of First and last names, phone number, email, company name, job role, credit card information. This personal data likely will not meet the definition of "foreign intelligence information" under FISA Section 702.

A white paper published by the United States Department of Commerce, the United States Department of Justice, and the United States Office of the Director of National Security supports this view and states, "(c)ompanies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data."<sup>8</sup>

Additionally, PandaDoc provides the following safeguards for personal data stored in the United States:

1. Personal Data will be transported to the United States and stored in an encrypted fashion.
2. The keys for decrypting Personal Data concerning individuals in Europe will not be provided to a government authority absent court order unless (1) any impacted individual in Europe has been notified of the government request, or (2) the Data Importer determines that the protection of the rights and freedoms of others requires the disclosure.
3. Data Importer has, and will maintain, a written policy and procedure for responding to requests from law enforcement agencies (the "Law Enforcement Request Policy").
4. The Law Enforcement Request Policy requires the Data Importer to determine whether a government request for information is validly issued and authentic.

<sup>7</sup> EDPB Recommendations on Supplementary Measures at 17 – 18.

<sup>8</sup> United States Department of Commerce, United States Department of Justice, United States Office of the Director of National Security, *Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II White Paper*, September, 2020, at 2, available at <https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF>.

5. The Law Enforcement Request Policy requires the Data Importer to inform a government agency that requests Personal Data that such Personal Data includes information about individuals located in Europe.
6. The Law Enforcement Request Policy requires the Data Importer to attempt to narrow requests for the Personal Data of individuals in Europe to the minimum data needed by the government agency.
7. The Law Enforcement Request Policy requires the Data Importer to inform a government agency that requests the Personal Data of individuals in Europe that the GDPR, and other European data privacy laws, confer certain rights upon individuals located in Europe including, among other things, rights to transparency, access, rectification, and deletion about, and relating to, any entity, including government agencies, that process personal information.
8. The Law Enforcement Request Policy requires the Data Importer to request that the government agency permit the Data Importer to notify the Data Exporter and/or any impacted individuals in Europe of the request prior to any information being transmitted to the law enforcement agency.
9. The Law Enforcement Request Policy requires the Data Importer to request that the government domesticate any request through counterpart agencies located within the European Union.
10. The Law Enforcement Request Policy requires the Data Importer to evaluate whether the request seeks information which goes beyond what appears reasonably necessary for (a) national security, (b) defense, (c) public security, (d) the prevention, investigation, detection and prosecution of criminal offenses, or the breach of ethics for the regulated professions, (e) other important economic or other financial interests of a country, (f) the protection of individuals, or (g) the protection of the rights and freedoms of others.
11. To the extent that the request is determined to be unreasonable, the Law Enforcement Request Policy requires the Data Importer to appeal, narrow, or attempt to quash the request, to the extent permitted by law.
12. The Data Importer will work with the Data Exporter to consider, and evaluate, any additional supplemental measures recommended by the European Data Protection Board ("EDPB").

To date, PandaDoc has never received a government request under either FISA 702 or EO 12333.

In light of the above, PandaDoc likely will not process "foreign intelligence information" and therefore PandaDoc's (and its subprocessors') processing of EEA, Swiss, and/or UK personal data under the agreement likely is not subject to FISA Section 702.

- **Conclusion: Transfers of Personal Data to PandaDoc and its Subprocessors in the United States are Likely Permitted.** In light of the information provided in this document, including PandaDoc's practical experience dealing the technical, contractual, and organizational measures PandaDoc has implemented to protect customer personal data, PandaDoc considers that the risks involved in transferring and processing European personal data in/to the US do not impinge on our ability to comply with our obligations under the EU SCCs (as "data importer") or to ensure that individuals' rights remain protected. Therefore, no additional supplementary measures are necessary at this time. PandaDoc has demonstrated and documented that it has no reason to believe that these problematic laws will be interpreted and/or applied in practice so as to cover the transfer of EEA, Swiss, and/or UK personal data to the PandaDoc or its subprocessors in the United States. As a result, transfers of EEA, Swiss, and/or UK personal data to PandaDoc and its subprocessors in the United States are likely permitted pursuant to the EDPB Recommendations on Supplementary Measures.

---

<sup>9</sup> EDPB Recommendations on Supplementary Measures at 17 – 18.

**Addendum A – Definition of Foreign Intelligence Information under FISA Section 702**

**To Transfer Impact Assessment**

When acquired from a non-U.S. person, *“foreign intelligence information”* is defined as:

(1) information that relates to ... the ability of the United States to protect against –

(A) actual or potential attacks or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power by an agent of a foreign power;

or

(2) information with respect to a foreign power or foreign territory that relates to ...

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

## **EXHIBIT 3 TO DATA PROCESSING AGREEMENT**

### **ADDITIONAL SAFEGUARDS FOR PERSONAL DATA STORED IN THE UNITED STATES**

This Exhibit 3 forms part of the Agreement. Capitalized terms not defined in this Exhibit 3 have the meaning set forth in the Agreement.

With respect to any Personal Data transferred outside the EU, the EEA and/or the UK to a country that does not offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities, the data importer further provides the following representations and warranties:

1. Personal Data will be transported to the United States and stored in an encrypted fashion.
2. The keys for decrypting Personal Data concerning individuals in Europe will not be provided to a government authority absent court order unless (1) any impacted individual in Europe has been notified of the government request, or (2) the Data Importer determines that the protection of the rights and freedoms of others requires the disclosure.
3. Data Importer has, and will maintain, a written policy and procedure for responding to requests from law enforcement agencies (the "Law Enforcement Request Policy").
4. The Law Enforcement Request Policy requires the Data Importer to determine whether a government request for information is validly issued and authentic.
5. The Law Enforcement Request Policy requires the Data Importer to inform a government agency that requests Personal Data that such Personal Data includes information about individuals located in Europe.
6. The Law Enforcement Request Policy requires the Data Importer to attempt to narrow requests for the Personal Data of individuals in Europe to the minimum data needed by the government agency.
7. The Law Enforcement Request Policy requires the Data Importer to inform a government agency that requests the Personal Data of individuals in Europe that the GDPR, and other European data privacy laws, confer certain rights upon individuals located in Europe including, among other things, rights to transparency, access, rectification, and deletion about, and relating to, any entity, including government agencies, that process personal information.
8. The Law Enforcement Request Policy requires the Data Importer to request that the government agency permit the Data Importer to notify the Data Exporter and/or any impacted individuals in Europe of the request prior to any information being transmitted to the law enforcement agency.
9. The Law Enforcement Request Policy requires the Data Importer to request that the government domesticate any request through counterpart agencies located within the European Union.
10. The Law Enforcement Request Policy requires the Data Importer to evaluate whether the request seeks information which goes beyond what appears reasonably necessary for (a) national security, (b) defense, (c) public security, (d) the prevention, investigation, detection and prosecution of criminal offenses, or the breach of ethics for the regulated professions, (e) other important economic or other financial interests of a country, (f) the protection of individuals, or (g) the protection of the rights and freedoms of others.
11. To the extent that the request is determined to be unreasonable, the Law Enforcement Request Policy requires the Data Importer to appeal, narrow, or attempt to quash the request, to the extent permitted by law.
12. The Data Importer will work with the Data Exporter to consider, and evaluate, any additional supplemental measures recommended by the European Data Protection Board ("EDPB").

## **EXHIBIT 4 – TO DATA PROTECTION AGREEMENT**

This Exhibit 4 and Annexes hereto forms part of the Agreement.

### **EUROPEAN ECONOMIC AREA AND SWITZERLAND STANDARD CONTRACTUAL CLAUSES**

#### **SECTION I**

##### ***Clause 1***

##### **Purpose and scope**

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.
- (b) The Parties;
  - (i) The natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

##### ***Clause 2***

##### **Effect and invariability of the Clauses**

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

##### ***Clause 3***

##### **Third-party beneficiaries**

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - (iii) Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12(a), (d) and (f);

- (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18(a) and (b).
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

**Clause 4**  
**Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

**Clause 5**  
**Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

**Clause 6**  
**Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

**Clause 7 – Option Exercised to not include.**

**SECTION II – OBLIGATIONS OF THE PARTIES**

**Clause 8**  
**Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter.
- (b) The data exporter may give such instructions throughout the duration of the contract.
- (c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**



The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### **8.6 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## **8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

## **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

## **8.9 Documentation and compliance**

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

## **Clause 9 Use of sub-processors**

- (a) **SPECIFIC PRIOR AUTHORISATION** The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least thirty (30) days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.
- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### **Clause 10** **Data subject rights**

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### **Clause 11** **Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

**Clause 12**  
**Liability**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

**Clause 13**  
**Supervision**

- (a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### ***Clause 14***

#### **Local laws and practices affecting compliance with the Clauses**

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under

these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

### **Clause 15**

#### **Obligations of the data importer in case of access by public authorities**

##### **15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i). receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii). becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

##### **15.2 Review of legality and data minimization**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose

the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **SECTION IV – FINAL PROVISIONS**

### ***Clause 16***

#### **Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever the reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.



**Clause 17**  
**Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

**Clause 18**  
**Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

**Data Exporter:**

1. Name:

Address: \_\_\_\_\_

Contact person's name, position and contact details: \_\_\_\_\_

Relevant Activities: As set forth in Exhibit 2.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Role: Data Controller

**Data Importer:**

2. PandaDoc, Inc.

3739 Balboa St. #1083, San Francisco, CA 94121

Kelley Boland, Director of Legal and Compliance

Email: [privacyteam@PandaDoc.com](mailto:privacyteam@PandaDoc.com)

Relevant Activities: As set forth in Exhibit 2. Further, PandaDoc is an organization that assists other organizations in providing technical solutions to reduce administrative burden of transacting business by creating personalized documents in an automated fashion (not profiling or automated decision making under the GDPR). Such automation includes creating and approving proposals, quotes, contracts, and eSignatures.

Signature:  \_\_\_\_\_ Date: 06 / 01 / 2022

Role: Data Processor

## **B. DESCRIPTION OF TRANSFER**

### **1. Categories of data subjects whose personal data is transferred:**

The authorized representative(s) of the organization using PandaDoc and Customer's end-user, if applicable.

### **2. Categories of personal data transferred:**

- a. Customer and Customer's end-user (if applicable):
  - i. Contact details: Name (First & Last), Email Address, Phone Number, Company Name, Job Role
  - ii. Billing details: Name (First & Last), Email Address, Address, Country, State, City, Zip code, Credit Card information
- b. Customer's Employees:
  - i. Contact Details: Name (First & Last), Email Address

### **3. Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitations, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:**

Data exporter shall not disclose (and shall not permit any data subject to disclose) any special categories of personal data to data importer for processing

### **4. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).**

Personal data may be transferred one-off or continuous basis at the option of the authorized user.

### **5. Nature of the processing. Please select from the following and/or add** The following list shall act as the default in response to this, if no selection is made.

- a. Adaption or alteration
- b. Collection
- c. Consultation
- d. Destruction
- e. Disclosure by transmission
- f. Dissemination
- g. Erasure
- h. Organization
- i. Recording
- j. Retrieval
- k. Storage
- l. Structuring
- m. Use

### **6. Purpose(s) of the data transfer and further processing**

The purpose of the data transfer is to further the contract (Terms of Service) and for the person seeking to evaluate the PandaDoc service.

**7. *The period for which the personal data will be retained or, if that is not possible, the criteria used to determine that period.***

For the duration of the Terms of Service and the provision of services as outlined in such Agreement or Order Form.

**8. *For transfers to (sub-) processors, also specific subject matter, nature and duration of the processing:***

As set forth at Annex III to these SCCs.

**C. COMPETENT SUPERVISORY AUTHORITY**

Data Protection Commission (Ireland)

## **ANNEX II**

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

As set forth in Exhibit 1

## ANNEX III

### LIST OF SUB-PROCESSORS

*The Controller has authorized the following list of sub-processors:*

<b>Product(s)</b>	<b>Sub-processing Activities</b>	<b>In what countries does PandaDoc store Customer Personal Data?</b>	<b>In what countries does PandaDoc process (e.g., access, transfer, or otherwise handle) Customer Personal Data?</b>
Amazon Web Services	Cloud Service Provider	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Salesforce	Cloud-based Sales Services	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
HubSpot	Software products for inbound marketing, sales, and customer service	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Google Workspace & Analytics	User, employee and applicant data is maintained in GSuite	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Recurly	Payment Subscription Management	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Amplitude	Product analytics	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Segment	Data infrastructure	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Chilipiper	Meeting scheduler	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States

Zendesk	Cloud Service Provider	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
FullStory	User data for user research	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Mailgun Technologies, Inc.	Mailgun Technologies, Inc.	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
SalesLoft	Sales engagement platform	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Imperva	WAF and DDoS Protection	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Stitch	ETL data pipeline	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Wootric	NPS Surveys	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Gainsite	Customer success management platform helps CSMs to optimise their work.	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Gong	Sales Efficiency Tool	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Netsuite	Enterprise Resource Planning	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States

Appcues	Onboarding tours, announcements and surveys	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Split Software	Feature Testing Tool	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Pusher	Hosted API Service	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Twilio	Communication API	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States



**EXHIBIT 5 – UK INTERNATIONAL DATA TRANSFER ADDENDUM**  
**THIS IS ONLY APPLICABLE TO UK CUSTOMERS**

This Exhibit 5 forms part of the Agreement.

**International Data Transfer Addendum to the EU Commission Standard  
Contractual Clauses**


**VERSION B1.0, in force 21 March 2022**

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

---

**Part 1: Tables**

**Table 1: Parties**

<b>Start date</b>		
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>	<b>Importer (who receives the Restricted Transfer)</b>
<b>Parties' details</b>	Full legal name:  Trading name (if different):  Main address (if a company registered address):  Official registration number (if any) (company number or similar identifier):	Full legal name: PandaDoc, Inc.  Trading name (if different):  Main address (if a company registered address):  Official registration number (if any) (company number or similar identifier): 3739 Balboa Street #1083, San Francisco, CA 94121, United States.
<b>Key Contact</b>	Full Name (optional):  Job Title:  Contact details including email:	Full Name (optional): Kelley Boland  Job Title: Director, Legal and Compliance  Contact details including email: privacyteam@pandadoc.com
<b>Signature (if required for the purposes of Section 2)</b>		

**Table 2: Selected SCCs, Modules and Selected Clauses**

<b>Addendum EU SCCs</b>	<p>The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date:</p> <p>Reference (if any):</p> <p>Other identifier (if any):</p>
-------------------------	--

**Table 3: Appendix Information**

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: PandaDoc and

Annex 1B: Description of Transfer: As detailed in Annex I of the SCCs, detailed in Table 2

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As detailed in Annex II of the SCCs, detailed in Table 2.

Annex III: List of Sub processors (Modules 2 and 3 only): As detailed in Exhibit 1 of the DPA and noted on Appendix III of the SCCs, detailed in Table 2.

**Table 4: Ending this Addendum when the Approved Addendum Changes**

<b>Ending this Addendum when the Approved Addendum changes</b>	<p>Which Parties may end this Addendum as set out in Section 19:</p> <p>Importer</p> <p>Exporter</p> <p>neither Party</p>
--	---

## Part 2: Mandatory Clauses

### Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

### Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

### **Hierarchy**

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

### **Incorporation of and changes to the EU SCCs**

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

- a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
- b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
- c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

- a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
- b. In Clause 2, delete the words:  
"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
- c. Clause 6 (Description of the transfer(s)) is replaced with:  
"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
- d. Clause 8.7(i) of Module 1 is replaced with:  
"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
- e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

- f. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
- g. References to Regulation (EU) 2018/1725 are removed;
- h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
- i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
- j. Clause 13(a) and Part C of Annex I are not used;
- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
- l. In Clause 16(e), subsection (i) is replaced with:  
“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;
- m. Clause 17 is replaced with:  
“These Clauses are governed by the laws of England and Wales.”;
- n. Clause 18 is replaced with:  
“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and
- o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

### **Amendments to this Addendum**

- 16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
- 17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 18. From time to time, the ICO may issue a revised Approved Addendum which:
  - a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
  - b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

- a its direct costs of performing its obligations under the Addendum; and/or
- b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.


**Alternative Part 2 Mandatory Clauses:**

<b>Mandatory Clauses</b>	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
--------------------------	---



# Signature Certificate

Reference number: BMBKY-P4854-XBDY2-GPSSU

Signer	Timestamp	Signature
<b>Kelley Boland</b> Email: kelley.boland@pandadoc.com Sent: 01 Jun 2022 15:34:16 UTC Viewed: 01 Jun 2022 17:35:36 UTC Signed: 01 Jun 2022 17:45:35 UTC		
<b>Recipient Verification:</b> ✓Email verified	01 Jun 2022 17:35:36 UTC	IP address: 97.76.177.43 Location: Bradenton, United States

Document completed by all parties on:  
01 Jun 2022 17:45:35 UTC

Page 1 of 1



Signed with PandaDoc

PandaDoc is a document workflow and certified eSignature solution trusted by 30,000+ companies worldwide.

