**OBLIGATORY DISCLAIMER**

This document is provided “AS IS” and for informational purposes only. DocuSmart Inc. (dba Lexion) (“Lexion”) and all distributors, individuals, or other entities that have linked to this document or included a comment herein (together, “we”) do not make any warranties, express or implied, statutory or otherwise, including, but not limited to, warranties of merchantability, title, fitness for a particular purpose, or noninfringement.

You understand that each factual situation is unique and requires specific analysis from a legal professional. Therefore, we make no warranty as to the adequacy, accuracy, completeness, or currency of this document or any comments shown herein. You use this document at your own risk. This document is not a substitute for legal advice. Always consult with an attorney for your particular legal questions.

You further acknowledge and agree that we are not a law firm and do not provide legal advice. Please have a lawyer review this document or any provision you desire to use to advise you, including as to whether it is appropriate for your particular service, business, transaction, or situation.

To learn more about how to analyze, edit, and negotiate Data Processing Addendums, check out the webinar recordings in the Lexion Resource Center: <https://www.lexion.ai/resources/resource-center#Recorded-Events>

P.S. We do recommend deleting this entire section and our comments before using this document or any clauses. Also, if you find any typos or other errors, note that this document was intended for informational purposes only, meant to be edited by you or your attorney, we’re not your attorney, and it was created by humans (not AI).

**INSTRUCTIONS**

In comments (see “Note to Drafter”) and also where highlighted and in red colored font, we have included suggested areas in this document for you to analyze, tailor, and edit to your specific role, data processed, service, transaction, process, or other situation. Of course, you’re welcome to edit all parts of this document or not use this document at all.

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Data Processing Addendum**

This Data Processing Addendum, including the selected modules of the Standard Contractual Clauses and Annexes (this “**DPA**”), is dated effective as of [insert date] (“**DPA Effective Date**”) and entered into by and between [party name] (“**Vendor**”)and[other party name] (“**Customer**”).

This DPA forms a part of and is incorporated into the then-current and applicable agreement (“**Agreement**”) between Customer and Vendor that governs the provision, use, and purchase of Vendor’s products and services described in the Agreement (“**Services**”). Capitalized terms used herein and not defined will have the meanings given to such terms in the Agreement.

 **1. Definitions.**In this DPA, the following terms shall have the following meanings:

* + - 1. “**Applicable Data Protection Law**” means all international, federal, national, and state privacy and data protection laws that apply to the processing of Personal Data that is the subject matter of the Agreement (including, but not limited to, where applicable, European Data Protection Law and U.S. Data Protection Law (as defined below)).
			2. “**CCPA**” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq*., as amended by the California Privacy Rights Act (“**CPRA**”), and its implementing regulations.
			3. “**Controller**” means the entity that determines the purposes and means of the processing of Personal Data.
			4. “**Data Subject**” means a natural person whose Personal Data is processed in the context of this DPA.
			5. “**European Data Protection Law**” means: (i) prior to 25 May 2018, the EU Data Protection Directive 95/46/EC, and any applicable national implementation of it; (ii) on and after 25 May 2018, the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation)(“**EU GDPR**”); (iii) 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 E.U. e-Privacy Directive (Directive 2002/58/E.C.); and (iv) the Swiss Federal Data Protection Act (“**Swiss GDPR**”).
			6. “**Personal Data**” shall have the meaning given to such term under Applicable Data Protection Law, but generally means any information relating to an identified or identifiable natural person where an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
			7. “**Processor**”means an entity that is engaged to process Personal Data on behalf of the Controller, including, as applicable, any “service provider” as that term is defined by the CCPA.
			8. “**Security Incident**” means a confirmed breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Data (as defined in Section 2.1 below) transmitted, stored, or otherwise processed by Vendor or its Sub-Processors. “Security Incident” does not include unsuccessful attempts or activities that do not compromise the security of Data, including unsuccessful login attempts, pings, port scans, denial of services attacks, and other network attacks on firewalls or networked systems.
			9. “**Standard Contractual Clauses**” means: (i) where the E.U. 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 (E.U.) 2016/679 of the European Parliament and of the Council (“**EU SCCs**”); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR (“**UK SCCs**”); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or recognized by the Swiss Federal Data Protection and Information Commissioner (“**Swiss SCCs**”).
			10. “**Sub-Processor**” means an entity engaged by the Processor to process Data on behalf of, and under the instructions of, the Controller in connection with the provision of the Service. Sub-Processors exclude employees, consultants, or independent contractors of Vendor where such individual performs services equivalent to those performed by an employee.
			11. “**U.S. Data Protection Law**” means the data protection or privacy laws and regulations applicable to the processing of Personal Data in force within the United States, including, but not limited to, (i) the CCPA, (ii) the Virginia Consumer Data Protection Act (“**VCDPA**”), (iii) once in effect, the Colorado Privacy Act, Connecticut Act Concerning Personal Data Privacy and Online Monitoring, Utah Privacy Act, and (iv) any rules or regulations implementing any of the foregoing.
1. **General Data Processing Requirements**
	1. *Relationship of the parties.* As between the parties and for the purposes of this DPA, Customer is the Controller, with respect to E.U. Data Protection Law and VCDPA, and a “business” with respect to CCPA, of the Personal Data that is included in Customer Content (“**Data**”) and appoints Vendor as a Processor, with respect to E.U. Data Protection Law and VCDPA, and a “service provider” with respect to CCPA, to process the Data on behalf of Customer.
	2. *Responsibilities of the parties.* Vendor will not sell Personal Data as the term “sell” is defined by the CCPA. Vendor will not disclose or transfer Personal Data to other parties that would constitute “selling,” as the term is defined by the CCPA. Customer shall comply with its obligations under Applicable Data Protection Law, including, but not limited to, providing notice to Data Subjects and obtaining Data Subjects’ consent for processing of Data Subjects’ Personal Data, where required. Customer represents that its use of the Service will: (i) not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data to the extent applicable under the CCPA; and (ii) not violate the rights of any Data Subject that has not opted into the processing of sensitive personal data to the extent applicable under the VCDPA. Customer, as a Controller or as a “business,” (as defined by the CCPA) is responsible for: (i) the accuracy, quality, and legality of the Data; (ii) how Customer acquired Data; (iii) the instructions Customer provides to Vendor regarding the processing of Data; (iv) providing all legally required notices to individuals and obtaining all legally required consents which may be necessary for Vendor to process Data; (v) ensuring that Customer’s processing instructions are lawful and do not violate Applicable Data Protection Laws; and (vi) ensuring that Data is provided to Vendor for a valid “Business Purpose,” as defined in the CCPA. Customer will not provide or make available to Vendor any Data in violation of the Agreement or provide any Data that is inappropriate for the nature of the Services.
	3. *Processing instructions;* *Purpose limitation.*
		1. Vendor shall process the Data as a Processor in accordance with the documented instructions of Customer (including those in this DPA and the Agreement) or with Customer’s written instructions and only for the following purposes: (i) as necessary to perform the Services for Customer under the Agreement; (ii) to perform any steps necessary for the performance of the Agreement; (iii) any processing initiated by an Authorized User in their use of the Service; and (iv) to comply with other reasonable, lawful instructions provided by Customer (e.g., via email, phone, support tickets, or online tool). Customer shall only give lawful instructions to Vendor that comply with Applicable Data Protection Law. **Annex A**, attached hereto, includes certain details of the processing of Data, as required under Applicable Data Protection Law.
		2. Vendor may process Personal Data for its own legitimate business purposes, as an independent Controller, solely when the processing is strictly necessary and proportionate, and if the processing is for one of the following purposes:
			1. Billing, account and customer relationship management (including marketing communications), support, and related correspondence;
			2. Complying with and resolving legal obligations, tax requirements, and in connection with any disputes;
			3. Monitoring and protecting the confidentiality, privacy, and security of the Services;
			4. Internal reporting, financial reporting, revenue planning, and forecast modeling;
			5. Receiving feedback regarding the Services and incorporating feedback into product development; and
			6. other uses permitted by Customer in the Agreement or other terms entered into between Vendor and Customer.
	4. *Confidentiality of processing.* Vendor shall ensure that any person that it authorizes to process Data (including Vendor's staff, agents, and subcontractors) shall be subject to a duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to process the Data who is not under such a duty of confidentiality.
	5. *Security standards.* Vendor shall implement appropriate technical and organizational measures intended to protect the Data from: (i) accidental or unlawful destruction; and (ii) loss, alteration, unauthorized disclosure of, or access to the Data. At a minimum, such measures shall include the security measures identified in **Annex B** (“**Security Measures**”).
2. **Sub-Processors and Subcontracting**
	1. Subject to the terms and conditions set forth in this DPA, Customer generally authorizes Vendor to continue to use and disclose Data to Sub-Processors engaged by Vendor in the context of providing the Services and processing activities. Customer approves the use of Sub-Processors described at [Insert link or reference to an attached exhibit]. Vendor shall remain fully liable for any breach of Vendor’s obligations under this DPA that is caused by an act, error, or omission of Vendor’s Sub-Processors.
	2. Vendor shall not subcontract any processing of Data to a third-party Sub-Processor unless: (i) such Sub-Processor is subject to an agreement with Vendor that contains data protection terms not less protective as those provided for by this DPA with respect to the protection of Data to the extent applicable to the nature of the service provided by such Sub-Processor, and, to the extent the CCPA applies, each written agreement with a Sub-Processor will comply with the CCPA, designate the Sub-Processor as a “service provider” or “contractor,” and prohibit the Sub-Processor from selling Customer’s Data or using Customer’s Data for any purpose not authorized by the CCPA; and (ii) Vendor provides Customer prior notice (where notice will be provided by Vendor by email to Customer’s Service account administrator or by an in-product notification within the Service) of the addition or replacement of such Sub-Processor (including the details of the processing it performs or will perform, and the location of such processing) before authorizing any new Sub-Processor(s) to process Customer’s Data in connection with the provision of the applicable Service. Notwithstanding the foregoing, in the event of an emergency concerning Service availability or security, Vendor is not required to provide prior notice but shall provide notification within seven (7) business days following the change in Sub-Processor. Customer will notify Vendor within ten (10) business days of receipt of Vendor’s notice of a new Sub-Processor if it objects to the addition or replacement of a Sub-Processor. Customer’s objection should be sent to [Insert email address(es) to be notified or method of other notification option] and explain the reasonable grounds for the objection. If Customer objects to Vendor's appointment of a third party Sub-Processor on reasonable grounds relating to the protection of Data, and Vendor is unable to adequately address the reasonable grounds (e.g., make available to Customer a reasonable change to Customer’s configuration or use of the Service to avoid the processing of Data by the objected-to new Sub-Processor without unreasonably burdening Customer), then Vendor will not engage the Sub-Processor, or Customer may elect to suspend or terminate its subscription to the impacted Service without penalty. If Customer does not object to a Sub-Processor within thirty (30) days of Vendor’s notice as described in this Section 3, then the Sub-Processor will be deemed accepted by Customer.
3. **International transfers of Data.** To perform the Services for Customer under the Agreement, Vendor may transfer Personal Data to countries other than the country in which the data were originally collected, including, without limitation, the United States. Vendor will ensure that such transfers are made in compliance with Applicable Data Protection Law and this DPA. Customer authorizes such cross-border Personal Data transfers and represents, warrants, and covenants that Customer will comply with any requirements under Applicable Data Protection Law regarding such Personal Data transfers. For such cross-border Personal Data transfers subject to Applicable Data Protection Law, Vendor and Customer agree to be bound by: (i) in the case of GDPR, the EU SCCs then-current and applicable module and terms of the Standard Contractual Clauses published by the European Commission and located as of the date of this DPA at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers\_en; (ii) in the case of UK GDPR, the UK SCCs; and (iii) in the case of Swiss GDPR, the Swiss SCCs. In connection with the Standard Contractual Clauses referred to in (i) and (ii) of this Section 4, the parties agree to the following, as applicable:
	1. With respect to Data processed by Vendor pursuant to Section 2.3.1:
		* 1. Module Two of the EU SCCs will apply;
			2. in Clause 7, the optional docking clause will apply;
			3. in Clause 9, the Option 2 will apply;
			4. in Clause 11, the optional language will not apply;
			5. in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Irish law;
			6. in Clause 18(b), disputes shall be resolved before the courts of Ireland; (vi) Annex 1 will be deemed completed with the information set out in Annex A (Details of Processing) of this DPA;
			7. Annex 2 (Security Measures) will be deemed completed with the information set out in Annex B of this DPA; and
			8. Annex 3 (Sub-Processors) will be deemed completed with the information set out in Section 3 of this DPA.
	2. With respect to Personal Data processed by Vendor pursuant to Section 2.3.2:
		* 1. Module One of the EU SCCs will apply;
			2. in Clause 7, the optional docking clause will apply;
			3. in Clause 11, the optional language will not apply;
			4. in Clause 17, the Standard Contractual Clauses will be governed by Irish law;
			5. in Clause 18(b), disputes shall be resolved before the courts of Ireland;
			6. Annex 1 will be deemed completed with the information set out in Annex A (Details of Processing) of this DPA; and
			7. Annex 2 (Security Measures) will be deemed completed with the information set out in Annex B of this DPA.
	3. With respect to Personal Data subject to UK GDPR, the UK SCCs will apply and:
		* 1. the EU SCCs will also apply to transfers of Personal Data; and
			2. Table 1 to 3 of the UK SCCs will be deemed completed with the relevant information from the EU SCCs completed as set forth in Sections 4.1 and 4.2 above and the option “neither party” is checked in Table 4. The start date of the UK SCCs in Table 1 will be the date of this DPA.
	4. With respect to Personal Data subject to Swiss GDPR, the Swiss SCCs will apply and:
		* 1. the EU SCCs will apply and any references in the EU SCCs to “Directive 95/46/EC” or “Regulation (EU) 2016/679” will be interpreted as references to the Swiss SCCs;
			2. references to “EU,” “Union,” “Member State,” and “Member State Law” will be interpreted as references to “Switzerland’ and ‘Swiss law,’ as the case may be; and
			3. references to the “competent supervisory authority” and “competent courts” shall be interpreted as references to the FDIPC and competent courts in Switzerland, unless the EU SCCs as implemented above cannot be used to lawfully transfer such Personal Data in compliance with the Swiss SCCs, 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 of the Swiss SCCs shall be populated using the information contained in Annex A and Annex B to this DPA.
	5. To the extent Vendor adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses adopted pursuant to Applicable Data Protection Laws) for the transfer of Personal Data (“**Alternative Transfer Mechanism**”), the Alternative Transfer Mechanism will automatically apply instead of any applicable transfer mechanism described in this DPA (but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Laws applicable to the European Economic Area and extends to territories to which Customer’s Personal Data is transferred).
4. **Cooperation and Individuals’ Rights***.* Taking into account the nature of the processing and the information available, Vendor shall provide all reasonable and timely assistance to enable Customer to respond to: (i) any request from an individual to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable); and (ii) any other correspondence, inquiry, or complaint received from a regulator or public authority, Data Subject, or another third party, in connection with the processing of the Customer’s Data. If any such communication is made directly to Vendor, Vendor shall promptly and without undue delay (and in any event, no later than within forty-eight (48) hours of receiving such communication) provide Customer full details of the same and shall not respond to the communication unless specifically required by law or authorized by Customer.
5. **Data Protection Impact Assessment.** Taking into account the nature of the processing and the information available to the Vendor, Vendor shall provide Customer with reasonable and timely assistance with any data protection impact assessments and, where necessary, consultations with data protection authorities.
6. **Security Incident.**
	1. Upon becoming aware of a Security Incident affecting the Data, Vendor shall: (a) inform Customer without undue delay and in any event, no later than the earlier of, (i) within seventy-two (72) hours after confirming a Security Incident affected the Data, and (ii) the time period required by Applicable Data Protection Laws; and (b) provide sufficient available information and cooperation to enable Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law.
	2. Vendor shall further take such measures and actions as are necessary to contain, investigate, remedy, and mitigate the Security Incident and shall keep Customer informed of all material developments in connection with the Security Incident. Vendor shall not notify any third parties of a Security Incident affecting the Data unless and to the extent that: (a) Customer has agreed to such notification, or (b) notification is required to be made by Vendor under Applicable Data Protection Laws. Customer is responsible for its secure use of the Services, including, but not limited to, securing its account authentication credentials and protecting the security of Data transmitted via the systems Customer administers and maintains (i.e., email encryption).
7. **Deletion or Return of Data**. During the Term of the Agreement, Customer may access, export, or delete Customer’s Data using the features included with the Services or by contacting Vendor for assistance as needed. Upon termination or expiry of the Agreement or upon the Customer’s request, Vendor shall (at Customer's election and in accordance with the terms of the Security Measures and the Agreement) delete or return all Data, including copies, in its possession or control. This requirement shall not apply to the extent that Vendor is required by Applicable Data Protection Laws to retain some or all the Data, in which event Vendor shall isolate and protect the Data from any further processing except to the extent required by such law.
8. **Audit Rights and Reports**
	1. Vendor will conduct an annual third-party audit to attest to the SOC 2 Type II framework (or equivalent or successor attestations or certifications). Such audit will result in the generation of a summary report, which Vendor will make available to Customer upon request, in addition to such other information regarding Vendor’s information security and privacy practices as Customer may reasonably request (together, “**Reports**”). All Reports are Vendor’s Confidential Information.
	2. Solely to the extent required to comply with Applicable Data Protection Law, and to the extent the Reports do not satisfy Applicable Data Protection Law, Customer may audit (including by an independent third-party engaged by Customer who must enter into a non-disclosure agreement with Vendor) Vendor's compliance with this DPA. In the case of such audit, subject to the terms of this DPA, the parties agree that: (a) Vendor shall make available all such information, systems, and staff reasonably necessary to allow Customer to conduct such audit; (b) Customer shall not exercise its audit rights more than once per calendar year except following a Security Incident or following an instruction by a regulator or public authority; (c) Customer shall give Vendor at least forty-five (45) days prior written notice of its intention to audit pursuant to this DPA; (d) Customer shall conduct its audit during Vendor’s normal business hours, and take all reasonable measures to prevent unnecessary disruption to the Services, Vendor's operations, and to ensure the protection of the data (which may include Personal Data) of Vendor’s employees, contractors, suppliers, or other users or customers; (e) be limited in scope to matters reasonably required for Customer to assess Vendor’s compliance with this DPA and the parties’ compliance with Applicable Data Protection Law, and the parties shall mutually agree in advance on the date, scope, duration, and security and confidentiality controls applicable to an audit; (f) cover only facilities controlled by Vendor (unless otherwise agreed by the parties and any applicable Sub-Processors); (g) restrict findings to Customer’s Data only; and (h) Customer and its auditors must treat any audit findings and results as Confidential Information to the fullest extent permitted by Applicable Data Protection Laws.
	3. Customer understands and agrees that its right to audit a Sub-Processor’s compliance with this DPA will be subject to the audit provisions in the data processing terms between Vendor and such Sub-Processor, and that Customer may be required to execute a non-disclosure agreement and other related terms directly with such Sub-Processor to receive access to Sub-Processor’s reports and policies.
	4. Customer shall reimburse Vendor for all costs and expenses in connection with an audit carried out by Customer under this DPA, except that Vendor will provide Customer the Reports at no cost.
	5. Customer agrees that any of its audit rights set out in the Standard Contractual Clauses and other Applicable Data Protection Law shall be subject to, and carried out in accordance with, the terms of this Section 9.
9. **Compliance with Applicable Laws**
	1. Vendor will process Data in accordance with this DPA and Applicable Data Protection Laws applicable to its role under this DPA. Vendor is not responsible for complying with Applicable Data Protection Laws uniquely applicable to Customer by virtue of its business or industry. Vendor will promptly inform Customer if it becomes aware that Customer’s processing instructions infringe Applicable Data Protection Laws.
	2. With respect to the CCPA, except to the extent Section 2.3.2 applies, Vendor will: (i) comply with sections of the CCPA applicable to “service providers” as defined by the CCPA; (ii) process Data solely to provide the Services to Customer, consistent with Section 1798.140(e)(5) of the CCPA; and (iii) not sell Data, or retain, use, or disclose Data for any purposes other than to perform the Service or as otherwise permitted under Agreement or this DPA.
	3. With respect to the VCDPA, Vendor will: (i) comply with sections of the VCDPA applicable to “processors” as defined by the VCDPA; and (ii) process Data solely to provide the Services to Customer.
	4. To the extent that Section 2.3.2 applies, Vendor shall comply with the CCPA sections applicable to a “business” and the VCDPA sections applicable to a Controller.
10. **Indemnification for Third Party Claims.** Subject to the terms of the Agreement and relevant sections of this DPA, Vendor will defend and hold harmless Customer against any third-party claim brought against Customer arising from Vendor’s breach of its obligations under this DPA and indemnify Customer from the resulting costs and damages awarded against Customer to the third party raising such third-party claim by a court of competent jurisdiction or agreed to in settlement.
11. **Costs Allocation and Liability.**
	1. Each party will bear the costs of the investigation, remediation, mitigation, and other related costs to the extent a Security Incident is caused by such party.
	2. Each party will bear the costs of any fines, penalties, damages, or other related amounts imposed by an authorized regulatory body, governmental agency, or court of competent jurisdiction to the extent arising from such party’s breach of its obligations under this DPA.
	3. To the maximum extent allowed under Applicable Data Protection Law and other applicable law, each party’s liability under this DPA will be limited to actual and proven damages in an amount not to exceed three (3) times the amount paid by Customer to Vendor under the Agreement for the Services during the 12-month period immediately preceding the incident giving rise to the claim.
12. **Miscellaneous Provisions**
	1. The obligations placed upon Vendor under this DPA shall survive so long as Vendor or its Sub-Processors process Data on behalf of Customer. The parties agree that this DPA will replace any existing data processing agreement the parties may have previously entered into in connection with the Services. Any claims against Vendor or its Affiliates under this DPA may only be brought by the Customer entity that is a contracting party to the Agreement. In no event shall this DPA or any party restrict or limit the rights of any Data Subject or of any competent supervisory authority.
	2. The parties agree that this DPA applies to Provider’s Processing of Customer’s Data under the Agreement solely to the extent such processing is subject to Applicable Data Protection Laws. Other than as required by the Standard Contractual Clauses, this DPA is governed by the governing law set forth in the Agreement unless otherwise required by Applicable Data Protection Laws.
	3. Except for the changes made by this DPA, the Agreement continues to govern the provision and use of the Service and remains unchanged and in full force and effect (including, for avoidance of doubt, the limitation on liability provision in the Agreement). If there is any direct conflict between a provision in this DPA and a provision in the Agreement, the provision in this DPA shall prevail solely to the extent of that conflict only.
	4. Other than as required by the Standard Contractual Clauses, this DPA does not confer any third-party beneficiary rights; it is intended for the benefit of the parties hereto, respective permitted successors, and assigns only, and is not for the benefit of, nor may any provision hereof be enforced by, any other person.
	5. Other than as required by the Standard Contractual Clauses, the dispute mechanisms, including those related to venue and jurisdiction, set forth in the Agreement govern any dispute pertaining to this DPA.
	6. The parties will work together in good faith to negotiate an amendment to this DPA as either party reasonably considers necessary to address the requirements of Applicable Data Protection Laws from time to time.
	7. This DPA may be executed electronically and in counterparts, each of which shall be deemed to be an original and together shall constitute one and the same agreement.

This DPA is accepted and agreed to by the parties effective as of the DPA Effective Date.

|  |  |
| --- | --- |
| **Customer:** [Insert legal name]Signature: Printed Name: Title: Date Signed:  | **Vendor:** [Insert legal name]Signature: Printed Name: Title: Date Signed:  |

### ANNEX A

### DETAILS OF PROCESSING OF PERSONAL DATA

This Annex A includes certain details of the processing of Personal Data as required by the Standard Contractual Clauses and Article 28(3) GDPR. The parties agree that this Annex forms a part of the Standard Contractual Clauses.

A. List of Parties

Data exporter(s): Customer

Role: Controller or Processor (if processing contracts on behalf of an affiliate of Customer)

Contact Information: As outlined in the Agreement

Data importer(s): Vendor

Role: Processor for purposes of Section 2.3.1 and Controller for purpose of Section 2.3.2

Contact Information: As outlined in the Agreement

B. Description of Transfer

### *Subject matter and duration of the processing of Data:*

### The subject matter and duration of the processing of Customer’s Data are set out in the Agreement and this DPA.

### *The nature and purpose of the processing of Data:*

### The nature and purpose of the processing of Customer’s Data are set out in the Agreement and this DPA.

### *The types of Data to be processed:*

[Insert data processed based on the data handled and type of service provided by Vendor]

### *The categories of Data Subject to whom the Data relates:*

### [Insert data processed based on the data handled and type of service provided by Vendor]

### *The obligations and rights of Customer:*

### The obligations and rights of Customer are set out in the Agreement and this DPA.

**Data subjects**

The Personal Data transferred concern the following categories of data subjects: [Insert data that may be exchanged] that may includePersonal Data, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subjects:

[Insert data processed based on the data handled and type of service provided by Vendor]

**Categories of data**

[Insert data processed based on the data handled and type of service provided by Vendor]

**Special categories of data (if appropriate)**

The personal data transferred concerns the following special categories of data:

[Insert data processed based on the data handled and type of service provided by Vendor]

**Processing operations**

The Personal Data transferred will be subject to the following basic processing activities:

The Personal Data transferred to or accessed by the data importer will be used only for the purposes of providing the Services to the data exporter as described in further detail in the Agreement and this DPA. To this end, Personal Data may be accessed, processed, or disclosed as necessary by the data importer's duly authorised staff or Sub-Processors, strictly for the purpose of providing Services to the data exporter and in accordance with the data exporter’s instructions set out in the Agreement and this DPA.

**ANNEX B**

**VENDOR’S SECURITY MEASURES**

[Insert reference to or attach the Vendor’s current security measures and policies]